Contribuições no Documento Opine - Aqui

Número: OP-711928

Data: 19/06/2024 - 14:35

Resumo: :"Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, existem outras questões que demandam orientação ou regulamentação específicas pela ANPD. Primeiramente, é essencial que sejam estabelecidos parâmetros claros e objetivos para a avaliação do melhor interesse em diferentes contextos de tratamento de dados. Isso incluiria diretrizes detalhadas que ajudem os controladores a considerar a idade, maturidade e contexto social da criança, garantindo assim uma aplicação consistente e padronizada do princípio. Além disso, a educação digital e a conscientização são fundamentais para a proteção de dados pessoais de crianças e adolescentes. A ANPD poderia desenvolver programas educativos voltados tanto para as crianças e adolescentes quanto para os pais e responsáveis, informando-os sobre os riscos e benefícios do uso da internet e ensinando boas práticas de proteção de dados. Tais programas podem incluir guias práticos e recursos didáticos que facilitem a compreensão das normas e ajudem a criar um ambiente digital mais seguro. O processo de obtenção e verificação do consentimento parental também necessita de regulamentação específica. A ANPD deve estabelecer normas detalhadas sobre como obter e verificar o consentimento de pais ou responsáveis de forma que seja realmente informado e adequado. Isso inclui a criação de processos que assegurem que os responsáveis compreendam plenamente as implicações do tratamento de dados pessoais de seus filhos e que possam dar ou recusar consentimento de maneira fundamentada. A transparência e a comunicação clara são outras áreas que precisam de orientação específica. É crucial que as informações sobre a coleta e uso de dados pessoais sejam apresentadas de maneira compreensível para as crianças, utilizando linguagem simples e recursos visuais adequados. A ANPD pode estabelecer padrões para a criação de políticas de privacidade e termos de uso que sejam acessíveis para crianças, assegurando que elas compreendam como seus dados estão sendo utilizados e os seus direitos. Por fim, a proteção contra o uso abusivo ou exploratório de dados pessoais de crianças e adolescentes é uma questão urgente que requer regulamentação rigorosa. A ANPD deve definir mecanismos de monitoramento e estabelecer penalidades severas para práticas abusivas, como marketing direcionado ou manipulação psicológica. Além disso, deve promover a adoção de boas práticas de design e privacidade desde a concepção (privacy by design), incentivando desenvolvedores a incorporar medidas de proteção de dados desde o início do desenvolvimento de produtos e serviços destinados a este público. A implementação de um sistema contínuo de monitoramento e avaliação dessas práticas garantirá que as políticas de proteção de dados estejam sempre atualizadas e eficazes.","708725":"Nesse sentido, além dos

aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, existem outras questões que demandam orientação ou regulamentação específicas pela ANPD. A seguir, destacam-se sete situações ou contextos específicos que requerem maior atenção e detalhamento sobre o princípio do melhor interesse, bem como as principais questões a serem abordadas. Plataformas de Educação Digital: No contexto de plataformas digitais de ensino, é crucial garantir que os dados pessoais das crianças sejam utilizados exclusivamente para fins educacionais. A ANPD deve orientar sobre a limitação da coleta de dados apenas ao essencial para o aprendizado, além de assegurar que as informações não sejam compartilhadas com terceiros sem o consentimento explícito dos pais ou responsáveis. Redes Sociais: O uso de redes sociais por crianças e adolescentes apresenta riscos significativos de exposição a conteúdos inapropriados e exploração de dados. A ANPD precisa estabelecer regulamentações que imponham restrições rigorosas à coleta e ao compartilhamento de dados pessoais nesse ambiente, além de exigir mecanismos robustos de verificação de idade e consentimento parental. Aplicativos de Jogos e Entretenimento: Nos aplicativos de jogos e entretenimento, há uma tendência de coleta excessiva de dados pessoais para personalização de conteúdo e publicidade direcionada. A ANPD deve orientar sobre a implementação de práticas de minimização de dados, garantindo que apenas informações estritamente necessárias sejam coletadas e que os pais ou responsáveis sejam plenamente informados sobre os tipos de dados coletados e suas finalidades. Serviços de Saúde Digital: No caso de serviços de saúde digital voltados para crianças e adolescentes, como aplicativos de monitoramento de saúde e bem-estar, é fundamental proteger dados sensíveis e garantir a confidencialidade. A ANPD deve desenvolver diretrizes específicas para assegurar que esses dados sejam tratados com o mais alto nível de segurança e apenas para finalidades legítimas e benéficas para a saúde das crianças. Marketing e Publicidade Online: A exposição de crianças e adolescentes a práticas de marketing e publicidade online deve ser rigorosamente controlada. A ANPD deve proibir práticas de manipulação psicológica e marketing direcionado que explorem a vulnerabilidade das crianças, garantindo que qualquer publicidade seja transparente e apropriada para a idade. Dispositivos Conectados e Internet das Coisas (IoT): Com o aumento do uso de dispositivos conectados, como smartwatches e brinquedos inteligentes, que coletam dados pessoais de crianças, a ANPD deve criar regulamentos específicos para assegurar que esses dispositivos tenham configurações de privacidade padrão que protejam os dados das crianças e permitam o controle parental sobre a coleta e uso das informações. Ambientes Públicos e Instituições Educacionais: A coleta de dados pessoais de crianças em ambientes públicos, como escolas e bibliotecas, exige atenção especial. A ANPD deve orientar sobre as melhores práticas para a coleta e armazenamento seguro desses dados, assegurando que sejam usados exclusivamente para fins educacionais ou administrativos e que os pais ou responsáveis sejam informados e consintam claramente para tais práticas. Em resumo, a proteção de dados pessoais de crianças e adolescentes em diversos contextos exige uma abordagem detalhada e específica por parte da ANPD. A implementação de regulamentos claros e a promoção de boas práticas são essenciais para garantir que o princípio do melhor interesse seja sempre observado, protegendo a privacidade e o bem-estar dos jovens em todos os ambientes digitais.","705523":"1. Clareza e Transparência das Informações: o As informações

fornecidas aos pais ou responsáveis devem ser claras, acessíveis e compreensíveis, explicando de maneira detalhada quais dados serão coletados, para que finalidade, como serão utilizados e armazenados. o Utilizar linguagem simples e direta, evitando termos técnicos complexos, para garantir que os responsáveis entendam plenamente o que estão consentindo. 2. Destaque do Consentimento: o O pedido de consentimento deve ser apresentado de forma destacada, não podendo estar embutido em termos de uso ou políticas de privacidade longas. Deve ser um processo separado e visível. o Utilizar técnicas de design, como caixas de seleção destacadas, pop-ups ou modais, que chamem a atenção dos pais ou responsáveis para a necessidade de fornecer consentimento explícito. 3. Especificidade do Consentimento: o O consentimento deve ser específico para cada finalidade de tratamento de dados. Não é suficiente um consentimento genérico; cada uso dos dados deve ser claramente descrito e consentido individualmente. o Detalhar todas as atividades de tratamento de dados previstas, incluindo eventuais compartilhamentos com terceiros. 4. Verificação da Identidade dos Pais ou Responsáveis: o Implementar mecanismos razoáveis para verificar que o consentimento está realmente sendo dado pelos pais ou responsáveis legais. o Utilizar tecnologias disponíveis para garantir a autenticidade do consentimento, como autenticação multifator. 5. Facilidade de Revogação do Consentimento: o Garantir que os pais ou responsáveis possam revogar o consentimento a qualquer momento de maneira simples e direta, sem burocracia excessiva. o Incluir instruções claras sobre como revogar o consentimento nas mesmas plataformas onde ele foi inicialmente dado. 6. Registro e Documentação do Consentimento: o Manter registros detalhados de todos os consentimentos obtidos, incluindo informações sobre como e quando foram dados. o Armazenar esses registros de forma segura, de modo que possam ser apresentados em auditorias ou em caso de disputas legais. 7. Educação e Conscientização dos Pais ou Responsáveis: o Promover a educação dos pais ou responsáveis sobre a importância da proteção de dados pessoais e as implicações do consentimento. o Disponibilizar materiais educativos, como guias e tutoriais, que expliquem os direitos dos titulares de dados e as responsabilidades dos controladores. Esses critérios e parâmetros são essenciais para garantir que o consentimento "específico e em destaque" seja obtido de maneira adequada, respeitando os direitos das crianças e adolescentes e cumprindo com as exigências da LGPD. A implementação desses passos contribui para uma prática de tratamento de dados mais ética e transparente, fortalecendo a confiança entre controladores e titulares de dados. ","708742":"Design Intuitivo e Informações Claras: Implementar interfaces de usuário que apresentem de forma destacada e intuitiva o pedido de consentimento, utilizando linguagem clara e acessível. Fornecer descrições detalhadas sobre quais dados serão coletados, como serão utilizados, por quanto tempo serão armazenados e com quem serão compartilhados, sempre de maneira compreensível. Verificação de Identidade: Utilizar métodos robustos de verificação de identidade, como a solicitação de documentos pessoais (RG, CPF) ou a autenticação multifator (MFA) para garantir que o consentimento está sendo dado pelos pais ou responsáveis legais. Integrar tecnologias de verificação de identidade eletrônica que autentiquem de maneira segura e eficaz a identidade dos responsáveis. Processo de Consentimento Destacado: Garantir que o processo de consentimento seja um procedimento

separado, destacado dos termos de uso gerais ou políticas de privacidade, para evitar confusão. Utilizar caixas de seleção ou botões específicos que necessitem de uma ação afirmativa clara, indicando o consentimento para cada finalidade de tratamento de dados. Documentação e Armazenamento Seguros: Manter registros detalhados e seguros de todos os consentimentos obtidos, incluindo o contexto, data e hora em que o consentimento foi dado. Utilizar sistemas de gerenciamento de consentimento que permitam fácil acesso e auditoria dos registros, assegurando a conformidade com a LGPD. Facilidade para Revogação do Consentimento: Proporcionar um meio fácil e direto para que os pais ou responsáveis possam revogar o consentimento a qualquer momento, sem burocracia. Incluir informações claras sobre o processo de revogação nas comunicações iniciais e em todas as interações subsequentes com os dados. Uso de Tecnologias Disponíveis: Adotar tecnologias como inteligência artificial para monitorar e detectar inconsistências no processo de consentimento, ajudando a identificar possíveis fraudes ou consentimentos não autorizados. Implementar ferramentas de blockchain para criar registros imutáveis dos consentimentos, garantindo a transparência e a confiabilidade das informações armazenadas. Educação e Conscientização: Desenvolver e disponibilizar materiais educativos para pais e responsáveis sobre a importância da proteção de dados e as implicações do consentimento, promovendo uma cultura de privacidade e segurança. Realizar campanhas de conscientização digital sobre a privacidade dos dados das crianças, utilizando recursos multimídia e plataformas de fácil acesso. Auditorias e Revisões Regulares: Realizar auditorias periódicas para verificar a conformidade com as políticas de consentimento e ajustar processos conforme necessário. Atualizar regularmente as práticas de consentimento em resposta a mudanças tecnológicas e regulatórias, assegurando que todos os esforços razoáveis estejam sendo empregados continuamente. Essas medidas e mecanismos, quando implementados de forma integrada e contínua, asseguram que o consentimento dos pais ou responsáveis legais para o tratamento de dados pessoais de crianças seja obtido e verificado de maneira eficaz e conforme os princípios da LGPD, especialmente os da finalidade, necessidade e adequação.","708745":"Capacidades Civis e Regra Geral de Representação: De acordo com o direito civil brasileiro, adolescentes menores de 18 anos são considerados relativamente incapazes para certos atos, incluindo a celebração de contratos e o fornecimento de consentimento. Assim, em regra geral, é necessária a representação ou assistência dos pais ou responsáveis legais para consentir o tratamento de dados pessoais. A obtenção do consentimento deve observar rigorosamente essas disposições legais, garantindo que qualquer coleta de dados de adolescentes seja autorizada por seus pais ou responsáveis. Autonomia Progressiva e Princípio do Melhor Interesse: O princípio do melhor interesse da criança e do adolescente, conforme previsto no Estatuto da Criança e do Adolescente (ECA) e em consonância com a Convenção sobre os Direitos da Criança, reconhece a autonomia progressiva dos adolescentes. Isto implica que, conforme crescem e se desenvolvem, os adolescentes adquirem capacidade crescente para tomar decisões informadas. Em determinados contextos, pode ser apropriado considerar a capacidade dos adolescentes para fornecer consentimento, especialmente quando tais decisões envolvem seu cotidiano digital e interações rotineiras. Contextos Específicos para Consentimento Autônomo: Em situações onde o tratamento de dados é diretamente relacionado a atividades educacionais, sociais ou

culturais que envolvem o desenvolvimento pessoal do adolescente, pode ser razoável permitir que eles forneçam consentimento de forma autônoma. Exemplos incluem plataformas de aprendizagem online, redes sociais restritas por idade e aplicativos que promovam a participação em comunidades juvenis. Critérios para Avaliar a Autonomia: A autonomia do adolescente para fornecer consentimento deve ser avaliada com base em critérios como a maturidade do adolescente, a natureza dos dados coletados, o potencial impacto da coleta e a complexidade das informações envolvidas. Medidas de verificação, como testes de compreensão ou consentimento guiado, podem ser implementadas para assegurar que o adolescente entende plenamente as implicações de suas decisões. Políticas de Proteção e Salvaguardas: Independentemente da autonomia progressiva, devem ser implementadas políticas robustas de proteção de dados que incluam salvaguardas adicionais para adolescentes. Isso inclui a minimização da coleta de dados, a restrição de compartilhamento de dados e a implementação de controles de privacidade rigorosos. As plataformas devem fornecer ferramentas de fácil acesso para que adolescentes e seus responsáveis possam revisar e revogar consentimentos quando necessário. Educação e Conscientização: Promover programas educativos direcionados tanto aos adolescentes quanto aos pais ou responsáveis sobre os direitos e responsabilidades no ambiente digital. Oferecer recursos informativos que expliquem claramente as práticas de coleta e uso de dados, ajudando os adolescentes a tomar decisões informadas. Monitoramento e Ajuste Contínuo: Estabelecer mecanismos de monitoramento contínuo para avaliar a eficácia e a conformidade das práticas de consentimento autônomo, ajustando as políticas conforme necessário para responder a novas realidades e desafios tecnológicos. Garantir que as plataformas se mantenham atualizadas com as melhores práticas de privacidade e proteção de dados, refletindo o equilíbrio entre a proteção legal e a autonomia dos adolescentes. Essas abordagens equilibram a necessidade de proteção jurídica com o reconhecimento da autonomia progressiva dos adolescentes, em consonância com o princípio do melhor interesse. Adaptar as práticas de consentimento ao contexto específico e ao desenvolvimento individual dos adolescentes pode promover um ambiente digital mais seguro e adequado às suas necessidades e capacidades.","705539":"Princípio da Finalidade: Coletar e tratar dados pessoais de crianças e adolescentes apenas para finalidades específicas, explícitas e legítimas. Garantir que os dados não sejam utilizados para outros fins além dos informados e consentidos pelos pais ou responsáveis. Princípio da Necessidade: Limitar a coleta de dados ao mínimo necessário para atingir a finalidade específica. Evitar a coleta de dados excessivos ou irrelevantes que não contribuam diretamente para a finalidade informada. Princípio da Adequação: Assegurar que o tratamento de dados seja adequado, pertinente e proporcional às finalidades para as quais os dados foram coletados. Implementar práticas que sejam condizentes com a idade e o nível de maturidade das crianças e adolescentes. Princípio da Transparência: Fornecer informações claras, precisas e acessíveis sobre a coleta e uso de dados pessoais. Utilizar linguagem simples e recursos audiovisuais adequados para que tanto os pais quanto as crianças entendam como seus dados estão sendo tratados. Consentimento Específico e Destacado: Obter consentimento específico e destacado dos pais ou responsáveis legais, garantindo que eles estejam plenamente informados sobre as finalidades e os meios de tratamento dos dados. Implementar mecanismos para verificar a autenticidade desse consentimento. Privacidade

como Padrão (Privacy by Design): Integrar a privacidade desde a concepção dos produtos e serviços digitais. Utilizar medidas técnicas e organizacionais que garantam a proteção de dados por padrão, sem a necessidade de configurações adicionais pelos usuários. Verificação de Idade: Implementar técnicas robustas para a verificação da idade dos usuários, assegurando que apenas crianças autorizadas acessem conteúdos e serviços apropriados. Utilizar métodos seguros e eficientes para confirmar a identidade e a idade dos usuários. Minimização da Coleta de Dados: Reduzir a coleta de dados pessoais ao estritamente necessário para a funcionalidade do serviço. Evitar a criação de perfis comportamentais que possam expor crianças a riscos adicionais, como publicidade direcionada ou manipulação psicológica. Controle Parental: Fornecer ferramentas e funcionalidades que permitam aos pais ou responsáveis monitorar e controlar o tratamento de dados pessoais das crianças. Incluir opções para revisar, modificar ou revogar consentimentos a qualquer momento. Segurança dos Dados: Adotar medidas de segurança apropriadas para proteger os dados pessoais contra acesso não autorizado, vazamento, alteração ou destruição. Implementar criptografia, controle de acesso e outras técnicas de segurança da informação. Educação e Conscientização: Desenvolver programas educativos para crianças e adolescentes sobre privacidade e segurança digital. Informar pais e responsáveis sobre os riscos e melhores práticas para proteger os dados pessoais no ambiente digital. Monitoramento e Auditoria: Realizar auditorias regulares para garantir a conformidade com as políticas de privacidade e proteção de dados. Monitorar continuamente as práticas de tratamento de dados e ajustar as medidas de proteção conforme necessário. Responsabilidade e Prestação de Contas: Estabelecer mecanismos claros de responsabilidade e prestação de contas. Assegurar que os controladores e operadores de dados cumpram rigorosamente as normas de proteção de dados e sejam transparentes sobre suas práticas de tratamento. Esses princípios, parâmetros e salvaguardas, quando implementados de maneira integrada e contínua, garantem que o tratamento de dados pessoais de crianças e adolescentes em plataformas digitais seja realizado de forma ética, segura e em consonância com o seu melhor interesse.","708762":"Formulários de Autodeclaração de Idade: Implementar formulários simples onde os usuários declaram sua idade. Apesar de ser a técnica mais básica, deve ser combinada com outras medidas para maior eficácia. Verificação por Documentos de Identidade: Solicitar o upload de documentos oficiais (como RG ou CPF) para verificar a idade do usuário. Utilizar tecnologias de reconhecimento óptico de caracteres (OCR) para automatizar a validação. Autenticação Multifator (MFA): Combinar a verificação de idade com autenticação multifator, onde os usuários precisam confirmar sua identidade por meio de dois ou mais métodos, como SMS, e-mail ou aplicativos de autenticação. Serviços de Verificação de Idade de Terceiros: Integrar serviços de verificação de idade oferecidos por terceiros que utilizam bases de dados públicas e privadas para confirmar a idade dos usuários. Biometria Facial: Utilizar tecnologias de biometria facial para estimar a idade dos usuários. Ferramentas de inteligência artificial podem analisar características faciais para verificar se o usuário está dentro da faixa etária permitida. Questionários de Conhecimento: Implementar questionários que incluam perguntas relacionadas à cultura e eventos históricos específicos de certas faixas etárias. Essas perguntas podem ajudar a determinar se o usuário está mentindo sobre sua idade. Verificação de Pagamento: Utilizar métodos de pagamento que

exigem verificação de idade, como cartões de crédito que possuem informações sobre a idade do titular. Consentimento Parental: Enviar uma solicitação de consentimento aos pais ou responsáveis, que devem confirmar a idade da criança e fornecer o consentimento necessário para a criação da conta. Tecnologias de Geolocalização: Usar geolocalização para identificar a jurisdição legal e aplicar as leis de verificação de idade pertinentes ao local onde o usuário está. Análise de Comportamento: Monitorar o comportamento do usuário na plataforma para detectar inconsistências que possam indicar falsificação de idade, como horários de uso incomuns para crianças em idade escolar. Capacitação e Educação: Educar os pais e os próprios usuários sobre a importância de fornecer informações precisas e verdadeiras ao criar contas em plataformas digitais. Alertas de Segurança: Implementar alertas de segurança que avisam os pais quando uma tentativa de criar uma conta é feita por um menor sem a devida verificação de idade. Revisões Regulares: Realizar revisões periódicas dos métodos de verificação de idade para assegurar que estão atualizados com as melhores práticas e as novas tecnologias disponíveis. Feedback e Melhorias Contínuas: Coletar feedback dos usuários e responsáveis sobre o processo de verificação de idade e utilizar essas informações para melhorar continuamente as práticas e técnicas empregadas. Essas boas práticas e técnicas ajudam a garantir que as plataformas digitais verifiquem a idade dos usuários de maneira eficaz, protegendo crianças e adolescentes e assegurando a conformidade com os requisitos legais e os princípios da LGPD.","708764":"Dados Estritamente Necessários: Coletar apenas os dados pessoais estritamente necessários para a finalidade específica da plataforma. Evitar a coleta de dados excessivos ou irrelevantes que não contribuam diretamente para a atividade ou serviço oferecido. Proibição de Coleta para Formação de Perfis: Não coletar dados pessoais para a formação de perfis comportamentais que possam ser usados para manipular, influenciar ou direcionar publicidade de maneira abusiva ou inadequada para crianças e adolescentes. Consentimento Específico e Informado: Obter consentimento específico e destacado dos pais ou responsáveis legais para qualquer coleta de dados, assegurando que eles estejam plenamente informados sobre quais dados serão coletados e para que finalidade. Finalidade Clara e Legítima: Definir e comunicar claramente a finalidade da coleta de dados, garantindo que os dados não sejam utilizados para fins secundários ou diferentes dos informados no momento da coleta. Limitação de Compartilhamento de Dados: Restringir o compartilhamento de dados pessoais de crianças e adolescentes com terceiros. Quando necessário, garantir que os terceiros adotem as mesmas práticas de proteção de dados e obtenham consentimento apropriado. Anonimização e Pseudonimização: Sempre que possível, anonimizar ou pseudonimizar os dados pessoais coletados para minimizar os riscos de identificação direta dos menores e proteger sua privacidade. Transparência e Acessibilidade das Informações: Fornecer informações claras e acessíveis sobre a coleta e uso de dados pessoais, utilizando linguagem simples e recursos audiovisuais para garantir que tanto os pais quanto as crianças compreendam as práticas de coleta de dados. Revisões e Atualizações Regulares: Revisar e atualizar regularmente as práticas de coleta de dados para garantir que continuem alinhadas com as melhores práticas de proteção de dados e com as exigências legais em constante evolução. Minimização de Dados Sensíveis: Evitar a coleta de dados sensíveis (como informações de saúde, localização precisa, ou dados financeiros) a menos que seja absolutamente necessário e com consentimento explícito e específico dos pais

ou responsáveis. Armazenamento Seguro e Restrito: Garantir que os dados pessoais coletados sejam armazenados de maneira segura e acessível apenas para aqueles que necessitam desses dados para cumprir com a finalidade informada, implementando controles de acesso rigorosos. Exclusão de Dados Após a Finalidade: Implementar políticas de retenção de dados que assegurem a exclusão dos dados pessoais assim que a finalidade para a qual foram coletados for alcançada, salvo obrigações legais de retenção. Proibição de Condicionar o Acesso a Dados: Conforme disposto no art. 14, § 4º, da LGPD, não impor o fornecimento de informações pessoais como condição para a participação em jogos, aplicações de internet e outras atividades, exceto para as informações estritamente necessárias para a atividade. Controle Parental: Fornecer mecanismos que permitam aos pais ou responsáveis monitorar e controlar a coleta e uso de dados pessoais de seus filhos, incluindo a possibilidade de revisar, modificar ou revogar consentimentos previamente dados. Educação e Conscientização: Promover a educação de pais, responsáveis e crianças sobre as práticas de coleta de dados, seus direitos e como proteger suas informações pessoais no ambiente digital.","708768":"Painéis de Controle Parental: Implementar painéis de controle dedicados onde os pais ou responsáveis possam visualizar, gerenciar e controlar todas as informações coletadas sobre seus filhos. Esses painéis devem ser intuitivos e de fácil acesso. Notificações e Alertas: Enviar notificações regulares aos pais ou responsáveis sobre as atividades de coleta e uso de dados. Isso pode incluir alertas sobre novas atividades, consentimentos pendentes ou alterações nas políticas de privacidade. Ferramentas de Consentimento: Desenvolver ferramentas que permitam aos pais ou responsáveis fornecer e revogar consentimento de maneira simples e rápida. Essas ferramentas devem possibilitar a atualização das permissões de coleta de dados conforme necessário. Relatórios de Atividade: Fornecer relatórios periódicos que detalhem as atividades de tratamento de dados dos filhos, incluindo quais dados foram coletados, como estão sendo usados e com quem foram compartilhados. Configurações de Privacidade Personalizáveis: Oferecer opções de configuração de privacidade que permitam aos pais ou responsáveis definir níveis de privacidade específicos, ajustando quais dados podem ser coletados e utilizados. Recursos Educativos: Disponibilizar materiais educativos e tutoriais para pais e responsáveis sobre a importância da privacidade de dados e como utilizar as ferramentas de controle oferecidas pela plataforma. Autenticação Parental: Implementar sistemas de autenticação robustos para assegurar que somente os pais ou responsáveis legais possam acessar e alterar as configurações de privacidade e consentimento. Opção de Anonimização: Permitir que os pais ou responsáveis solicitem a anonimização dos dados pessoais dos seus filhos, quando possível, para proteger a identidade das crianças e adolescentes. Revisão de Políticas: Facilitar a revisão das políticas de privacidade e termos de uso por parte dos pais ou responsáveis, garantindo que estejam atualizados e compreendam todas as práticas de coleta e tratamento de dados. Interfaces Simples e Intuitivas: Desenvolver interfaces amigáveis e intuitivas que facilitam a navegação e a gestão das configurações de privacidade e consentimento, reduzindo a complexidade do processo para os pais. Feedback e Suporte: Criar canais de suporte dedicados onde os pais ou responsáveis possam obter ajuda e fornecer feedback sobre as práticas de tratamento de dados, permitindo a melhoria contínua dos sistemas de controle. Controles de Acesso Granulares: Implementar controles de acesso

granulares que permitam aos pais especificar exatamente quais tipos de dados podem ser coletados e para quais finalidades, com a possibilidade de ajustes em tempo real. Sessões de Treinamento: Oferecer sessões de treinamento online ou presenciais para pais e responsáveis, explicando como funcionam as ferramentas de controle parental e a importância de monitorar as atividades digitais dos filhos. Segurança de Dados: Assegurar que todas as ferramentas e mecanismos de controle implementados sejam acompanhados de medidas de segurança robustas para proteger os dados contra acessos não autorizados e vazamentos. Esses mecanismos e boas práticas podem efetivamente ampliar o controle dos pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes, promovendo um ambiente digital mais seguro e transparente. ","708772":"Políticas de Privacidade Simplificadas: Redigir políticas de privacidade em linguagem simples e clara, evitando jargões técnicos. Utilizar um formato de perguntas e respostas para tornar as informações mais acessíveis e compreensíveis para pais e crianças. Recursos Visuais e Audiovisuais: Utilizar infográficos, vídeos explicativos e animações para ilustrar como os dados pessoais são coletados, utilizados e protegidos. Esses recursos ajudam a transmitir informações complexas de maneira mais intuitiva. Sumários Executivos: Fornecer resumos executivos das políticas de privacidade, destacando os pontos mais importantes de forma concisa e direta. Incluir seções como “O que coletamos?”, “Como usamos seus dados?” e “Seus direitos”. Avisos e Consentimento Granulares: Apresentar avisos contextuais e solicitações de consentimento granulares que aparecem no momento em que os dados estão prestes a ser coletados ou usados, explicando claramente a finalidade e solicitando consentimento específico. Acessibilidade Digital: Garantir que todas as informações sejam acessíveis a pessoas com deficiências, utilizando ferramentas de leitura de tela, contraste de cores adequado, e suporte a diversas línguas. Perguntas Frequentes (FAQ): Manter uma seção de perguntas frequentes (FAQ) que aborda as dúvidas mais comuns sobre o tratamento de dados pessoais. Atualizar regularmente com base no feedback dos usuários. Interface de Usuário Amigável: Desenvolver interfaces de usuário intuitivas que facilitem a navegação e a compreensão das informações sobre privacidade e coleta de dados. Incluir botões de ajuda e dicas em cada seção relevante. Sessões Educativas Interativas: Oferecer módulos educativos interativos que expliquem a importância da privacidade de dados e como as informações pessoais são tratadas. Esses módulos podem incluir quizzes e atividades para reforçar o aprendizado. Notificações Proativas: Enviar notificações regulares aos pais e responsáveis sobre atualizações na política de privacidade, novos tipos de dados coletados ou mudanças significativas no tratamento de dados. Garantir que essas notificações sejam claras e acionáveis. Feedback de Usuários: Estabelecer canais para receber e responder a feedback dos usuários sobre a clareza e a compreensão das informações fornecidas. Usar esse feedback para melhorar continuamente as práticas de transparência. Consultas e Workshops: Realizar consultas públicas e workshops com pais, responsáveis e especialistas para discutir e revisar práticas de transparência e fornecer informações de maneira clara. Incorporar sugestões e melhorias baseadas nesses encontros. Documentação Detalhada de Consentimento: Manter registros detalhados dos consentimentos obtidos, incluindo a data, a finalidade e os dados específicos coletados. Permitir que os pais acessem e revisem esses registros facilmente. Opções de Revisão e Revogação de Dados: Proporcionar ferramentas fáceis de usar para que

os pais e responsáveis possam revisar e, se necessário, revogar o consentimento dado anteriormente, além de solicitar a exclusão de dados pessoais. Treinamento Contínuo de Funcionários: Treinar regularmente os funcionários sobre a importância da transparência e as melhores práticas para comunicar informações de maneira simples e acessível, garantindo que estejam preparados para interagir de forma eficaz com os usuários. Implementando essas boas práticas, as plataformas digitais podem garantir que as informações sobre o tratamento de dados pessoais de crianças e adolescentes sejam transmitidas de forma transparente, simples, clara e acessível, promovendo maior confiança e segurança entre os usuários.","708775":"Limitações no Uso de Inteligência Artificial: Esclarecer e regulamentar o uso de algoritmos de inteligência artificial e aprendizado de máquina no tratamento de dados pessoais de crianças e adolescentes, garantindo que não sejam utilizados de maneira prejudicial ou exploratória. Publicidade e Marketing Direcionado: Estabelecer regras mais rígidas sobre publicidade e marketing direcionado a crianças e adolescentes, incluindo restrições específicas sobre como e quando essas práticas podem ser utilizadas, para evitar manipulação e exploração. Proteção de Dados em Aplicativos Educacionais: Regulamentar de maneira específica os aplicativos e plataformas educacionais, assegurando que a coleta e o uso de dados pessoais sejam estritamente para fins educacionais e com consentimento apropriado. Transferência Internacional de Dados: Definir critérios claros para a transferência internacional de dados pessoais de crianças e adolescentes, garantindo que os países receptores ofereçam um nível adequado de proteção de dados conforme os padrões da LGPD. Dados Gerados por Dispositivos IoT: Regulamentar o tratamento de dados pessoais gerados por dispositivos de Internet das Coisas (IoT) voltados para crianças, como smartwatches e brinquedos inteligentes, assegurando a privacidade e segurança desses dados. Direitos dos Titulares Menores: Esclarecer os direitos dos titulares menores de idade, incluindo como esses direitos podem ser exercidos diretamente por adolescentes ou por meio de seus pais ou responsáveis, dependendo da idade e maturidade. Adoção de Medidas Proativas de Segurança: Exigir que plataformas digitais adotem medidas proativas de segurança, como auditorias regulares de segurança de dados e protocolos de resposta a incidentes, especialmente focados na proteção de dados de crianças e adolescentes. Responsabilidade dos Controladores e Operadores: Detalhar a responsabilidade dos controladores e operadores de dados em casos de violação de dados pessoais de crianças e adolescentes, incluindo penalidades específicas e obrigações de notificação. Consentimento em Contextos Específicos: Fornecer orientações detalhadas sobre como obter consentimento em contextos específicos, como em ambientes de saúde digital ou em plataformas de mídia social, garantindo que o consentimento seja sempre informado e adequado. Educação e Conscientização Digital: Implementar programas obrigatórios de educação e conscientização digital para pais, responsáveis e crianças sobre os riscos e melhores práticas de proteção de dados pessoais, promovendo um uso mais seguro e consciente das tecnologias. Revisão e Atualização de Regulamentos: Estabelecer mecanismos para a revisão e atualização periódica dos regulamentos de proteção de dados, garantindo que acompanhem as mudanças tecnológicas e sociais, e continuem relevantes e eficazes. Participação de Crianças e Adolescentes: Incentivar a participação ativa de crianças e adolescentes na formulação de políticas e regulamentos sobre proteção de dados, assegurando que suas perspectivas e

necessidades sejam consideradas. Tratamento de Dados Sensíveis: Regulamentar com maior detalhe o tratamento de dados sensíveis de crianças e adolescentes, como dados biométricos e de saúde, assegurando que sejam tratados com um nível de proteção ainda mais elevado. Obrigações de Transparência Aumentada: Exigir níveis adicionais de transparência para plataformas que tratam dados de crianças e adolescentes, incluindo relatórios públicos sobre práticas de coleta, uso e proteção de dados. Essas questões adicionais merecem esclarecimentos e regulamentações específicas para assegurar que o tratamento de dados pessoais de crianças e adolescentes seja realizado de maneira ética, segura e em conformidade com os princípios da LGPD.

Contribuinte: FERNANDO RODRIGUES PERES

Número: OP-713088

Data: 22/06/2024 - 14:43

Resumo: :"No contexto escolar, na questão do uso de dispositivos de conexão digital, para garantir o desenvolvimento da criança é necessário um encarregado que cuide de oferecer os acessos, segurança digital, educação digital, definir regras de utilização e não utilização em momentos de estudo, assim toda instituição de ensino deve ter um profissional para apoiar os alunos, professores e funcionários no uso do ambiente digital da escola. ","708725":"No ambiente escolar, o uso responsável dos dispositivos eletrônicos com apoio de um profissional capacitado para definir esse uso. ","705523":"Alguns ambientes como as escolas devem buscar esse consentimento em uma reunião onde será explicado para todos quais os benefícios oriundos do mesmo, bem como para a organização para se chegar a um acordo de consenso ","708742":"A criação do encarregado de dados pessoais dentro da escola com o papel de administrar e controlar os acessos para atender às regras de consentimento definidas com os pais.","708745":"É possível dar autonomia para os jovens a partir dos 14 ou 16 anos num perímetro de acesso definido pela comunidade.","705539":"Todo o conteúdo produzido e acessado no ambiente escolar deve ser livre de censura, mas deve definir as regras de responsabilidade definidas pela comunidade, escola, pais e responsáveis, funcionários dentro das regras legais e normas das instituições da educação do país. ","708762":"O acesso numa rede delimitada na escola deve oferecer conteúdo conforme as idades que devem também ser reguladas pelos acordos com a comunidade.","708764":"Toda coleta deve ter uma finalidade que deve ser negociada com os pais, professores e a comunidade.","708768":"A liberação de uma rede digital que possa ter um administrador que consiga acompanhar e apoiar as regras definidas pela comunidade. ","708772":"O uso da anonimização é uma opção para fornecer dados para pesquisas sem impactar as crianças e adolescentes. ","708775":"Minha sugestão é todo ambiente escolar ter um encarregado digital que possa cuidar dos acessos, dos registros, com foco na segurança e educação digital de todo o público, alunos, professores e funcionários.

Contribuinte: JOSE GERALDO LEITE COURA

Número: OP-713659

Data: 25/06/2024 - 08:27

Resumo: :"No caso de crianças e adolescentes é necessário aprofundar e descrever o uso indevido de dados nas plataformas sociais e jogos eletrônicos. É crescente denúncias sobre extorsão golpes sexuais e de adultos fingindo ser criança ou adolescente para convencer a vítima a ceder seus dados. Os jogos e plataformas sociais devem incluir mecanismos de denúncias para estes casos e violações que obrigam comunicação também em cópia imediata a ANPD, ao ministério público, a base de dados do disque denuncia. Além de provar investigação bem conduzida para identificar autores. Sancionar especialmente em valores máximos pois é defesa de incapaz. Os responsáveis devem ser notificados imediatamente. É possível desenvolver mecanismos automáticos para detecção destas fraudes eletrônicas e golpes aplicados a crianças e adolescentes. ","708725":"Golpes de sexestorsian. ","705523":"Tem que ser renovado trimestralmente. Não pode ser de longo prazo. Deve fornecer relatório de atividades no período para tutor responsável poder avaliar atividades. Qualquer suspeita de contato com adultos deve ser relatada. ","708742":"Verificar a renovação trimestral obrigatória.","708745":"Progressiva somente se os pais autorizarem, fiscalizarem renovando autorização trimestralmente após estudo do relatório de atividades do período. Deve apontar qualquer suspeita de contatos maliciosos, ataques de pedofilia, sexestorsian, etc...","705539":"Idem descrição anterior.","708762":"Mesmo mecanismo de prova de vida do INSS. Confiável e fornecido pelo governo brasileiro. ","708764":"Mínimo, minimizar, pseudonimizar, encriptado para dados sigilosos. Proibido estatísticas. São dados sensíveis demais. Anonimizacao para divulgação. ","708768":"Vide acima","708772":"Evitar totalmente. Só divulgar dados anônimos. ","708775":"Devem ser auditados regularmente se estão cumprindo as determinações. Punir exemplarmente.

Contribuinte: SERGIO TOLOMEI

Número: OP-719808

Data: 04/07/2024 - 15:07

Resumo:
:"teste","708725":"teste","705523":"teste","708742":"teste","708745":"teste","705539":"teste","708762":"testeteste","708764":"teste","708768":"teste","708772":"teste","708775":"teste

Contribuinte: GUILHERME FERREIRA FOLHA

Número: OP-728477

Data: 15/07/2024 - 10:35

Resumo: :"No comment.","708725":"No comment.","705523":"No comment.","708742":"No comment.","708745":"No comment.","705539":"There are

multiple different ways digital platforms can verify users' ages, and each of these methods comes with different strengths and weaknesses. Some are more accurate but more invasive, whereas others are less invasive but also less accurate. First, many digital platforms already require users to either check a box indicating they are over a certain age or input their date of birth to confirm they are over a certain age. This form of self-verification is the least invasive, because it only requires users to disclose, at most, one piece of personal information: their date of birth. Because many people share the same birthday, this piece of information cannot uniquely identify an individual. However, this method is also the least reliable, as underage users can and often do lie about their age in order to gain access to certain digital platforms. On the other end of the spectrum when it comes to accuracy and invasiveness is the ID check. This form of age verification is common in physical spaces, where customers must provide a valid government-issued ID in order to prove they are above the minimum age required to enter an age-gated space or purchase an age-gated product. It is also highly accurate, as government-issued IDs are more difficult to falsify than checking a box or entering one's date of birth. However, because most in-person ID checks do not involve making a copy of each customer's ID, these encounters pose lower privacy risks than online ID checks, where a digital platform may store the information from users' IDs. Additionally, as many as three million Brazilians do not have necessary identity documents, complicating the process of online ID checks for those individuals. Digital forms of government-issued identification could solve some of the privacy concerns associated with ID checks for age verification, as well as make the process more efficient. Currently, online ID checks typically require users to upload a photo of their physical ID as well as sometimes additional steps to prove the ID belongs to them, such as uploading a current image of their face to compare to the photograph on the ID. If designed right, digital IDs would streamline this process and allow users to only share necessary information. For example, individuals trying to access an age-restricted digital platform could verify that they are over a certain age without providing their exact date of birth, let alone all the other information a physical ID would reveal. Brazil's digital ID system has 153 million registered users, and while these IDs currently allow users to prove their identity to access government services, the system could potentially allow for easier and more privacy-protective age verification in the future. Finally, in between self-verification and ID checks, there is a third potential method of age verification using artificial intelligence (AI) to estimate users' ages from an image of their face. Combined with privacy protections requiring online services to delete users' images after the age estimation process is complete, this would minimize the amount of personal information users have to give up in order to verify their age. Of course, age estimation technology is not perfectly accurate and likely never will be, but it is constantly improving.","708762":"No comment.","708764":"No comment.","708768":"In order to increase parental control, and as an alternative to age verification, device operating systems could create a "trustworthy child flag" for user accounts that signals to apps and websites that a user is underage and apps and websites that serve age-restricted content could check for this signal from their users and block underage users from this content. Rather than using ID checks to determine whether to activate this child flag option, this would be an opt-in process built in to existing parental controls on devices. Parents could activate or disable the child flag option depending on their own values

and the maturity of their children. Additionally, devices could default to certain parental controls recommended for children. Because this approach does not require anyone to disclose or verify their identity, it does not create privacy risks by forcing users to share their government IDs or allowing online services to link their online activity to their offline identities. It is also a low-impact approach, allowing adults to continue using the Internet as they do today. Similarly, the vast majority of websites and apps that are meant for the general public would not have to take any action. Third, it would be entirely voluntary for users. Parents who want to control what their children see on the Internet could choose to use this feature and other parents could choose not to.","708772":"Requiring digital platforms to provide certain information would enable children and parents to make better-informed safety and privacy decisions. With the necessary information at their fingertips, parents could more effectively tailor their child's online safety and privacy protections to their parenting style and the child's developmental needs, allowing for an individualized approach to children's online safety and privacy instead of a one-size-fits-all mandate. Information that would be useful to children and their parents includes information about a digital platform's safety and privacy safeguards, potential risks facing children on the platform, personalized recommendation systems the platform uses, and advertising on the platform that targets children.","708775":"No comment.

Contribuinte: Ash Johnson

Número: OP-728823

Data: 15/07/2024 - 13:51

Resumo: :"Sem contribuições","708725":"Sem contribuições","705523":".Sem contribuições","708742":"Sem contribuições","708745":"É essencial equilibrar a necessidade de proteção dos adolescentes com o reconhecimento de sua capacidade crescente de tomar decisões informadas. Em muitos casos, a melhor prática é adotar uma abordagem híbrida, onde o consentimento seja obtido com a participação dos pais ou responsáveis, mas considerando a possibilidade de autonomia progressiva dos adolescentes em contextos apropriados. Essa abordagem deve sempre ser guiada pelo princípio do melhor interesse da criança e do adolescente.","705539":".Sem contribuições","708762":"Sem contribuições","708764":"Sem contribuições","708768":"Sem contribuições","708772":"Sem contribuições","708775":"Sem contribuições

Contribuinte: GIOVANA LOPES AZEVEDO DA SILVA NEVES

Número: OP-728844

Data: 15/07/2024 - 14:10

Resumo: :" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-

BR.docx.pdf","708725":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","705523":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708742":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708745":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","705539":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708762":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708764":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708768":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708772":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf","708775":" Por favor, veja nossos comentários em anexo: https://progresschamber.org/wp-content/uploads/2024/07/Brazil-Proceeding-on-Processing-of-Personal-Data-of-Children_PT-BR.docx.pdf

Contribuinte: Todd O'Boyle

Número: OP-728851

Data: 15/07/2024 - 14:17

Resumo: :"A ANPD deve atuar conjuntamente com o Ministério dos Direitos Humanos e da Cidadania/Secretaria Nacional dos Direitos da Criança e do Adolescente (SNDCA) em iniciativas visando a proteção desse grupo, bem como eventual alteração legislativa do ECA.","708725":"Redes sociais, jogos/videogame, publicidade direcionada, setor de saúde, processo judicial, quando envolver tratamento de dados pessoais de crianças e adolescentes.","705523":"Deve-se seguir os mesmos parâmetros previstos no art. 8º da LGPD, especialmente §1º que determina que se em contrato, em cláusula destacada das demais. Descata-se também, por analogia, o art. 54, §3º do CDC, que determina a utilização de termos claros e com caracteres ostensivos e legíveis, cujo tamanho da fonte não será inferior ao corpo doze.","708742":"Sugere-se a coleta do consentimento seja acompanhado de documento anexo que comprove o poder parental, mediante confirmação de identidade, como medida de segurança e prevenção à fraudes.","708745":"A obtenção do consentimento deve estar em consonância com o Código Civil, segundo o qual são absolutamente incapazes

para os atos da vida civil os menores de dezesseis anos e relativamente incapazes os maiores de dezesseis e menores de dezoito anos. Assim, tão somente poderia ser aplicável a autonomia progressiva para esse segundo grupo e desde que não importe em contração de obrigações.","705539":"Devem ser observados os princípios contidos no art. 6º da LGPD, bem como os princípios que regem a aplicação de medidas específicas de proteção contidas no art. 100 do ECA.","708762":"Confirmação de cadastro com documentos comprobatórios, antes da liberação de acesso à plataformas digitais.","708764":"Devem ser observadas as mesma limitações impostas pela tríade dos princípios da necessidade, finalidade e adequação. O ideal seria restrições nas configurações de algoritmos de coleta automática de interações do usuário, a fim de impossibilitar a formação de perfis comportamentais desse grupo vulnerável.","708768":"É necessário ampla participação dos pais, escolas, sociedade em geral na proteção dos interesses da criança e adolescente, inclusive com a disponibilização de cartilhas educativas sobre privacidade e proteção de dados (a exemplo da iniciativa entre Google e Turma da Mônica.","708772":"Como medidas de design, observar o citado §6º do art. 14 segundo o qual as informações deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado.","708775":"O conceito de melhor interesse permanece como um conceito jurídico indeterminado, o que pode gerar insegurança jurídica. Sugere-se a disponibilização de modelo pela ANPD de teste de balanceamento similar ao do legítimo interesse. Por fim, o tratamento de dados de crianças e adolescente deve ser critério para a necessidade de confecção de relatório de impacto.

Contribuinte: HORTENCIA RICARTE DE OLIVEIRA PAIZANTE

Número: OP-729102

Data: 15/07/2024 - 16:28

Resumo: :"Identificamos duas questões relevantes para atuação orientativa da Autoridade: (a) como exercitar o legítimo interesse atrelado a contextos que dizem respeito ao melhor interesse do menor; e (b) apresentação de diretrizes para mitigação de riscos e sopesamento de interesses dos menores. Antes de adentrar na motivação para as questões suscitadas acima, espera-se que a ANPD foque na orientação para quem ativamente direciona serviços para esta categoria de titulares intencionalmente e de modo recorrente – como em casos de soluções educacionais, plataformas de jogos online, coleta de dados em ações destinadas a crianças –, em oposição aos casos em que o tratamento ocorre de forma incidental – como serviços não destinados a crianças e adolescentes, mas que venham a ser acessados por este público. A) Legítimo interesse e melhor interesse da criança e do adolescente: Entendemos ser necessário obter da ANPD parâmetros mais claros sobre como exercitar o legítimo interesse atrelado à contextos que dizem respeito ao melhor interesse do menor, por meio de novos exemplos mais complexos em seus Guias, visando superar interpretações contraditórias. O direcionamento pela Autoridade auxiliará a mensurar corretamente e reconhecer o que pode ser flexibilizado quando em conflito com determinados outros interesses, e ainda assim continuar protegendo os menores atrelados a esse interesse. Nesse aspecto, sugerimos que a

Autoridade leve em consideração a razão de ser do legítimo interesse e a sua complementariedade com o melhor interesse da criança, de forma a não propor parâmetros que sejam excessivamente onerosos ao controlador, tornando inviável a aplicação da base legal nesse contexto. Por exemplo, entendemos que exigir um teste de balanceamento específico para respaldar os direitos da criança caracterizaria uma onerosidade excessiva e desnecessária aos controladores, além de ser uma medida não necessariamente eficiente no resguardo do princípio do melhor interesse. B) Orientação para mitigação de riscos inerentes a atividades de tratamento, inclusive quando necessários para buscar o melhor interesse do menor: Partindo do posicionamento da ANPD no Enunciado CD/ANPD nº 01/2022 sobre o condicionamento de aplicação de quaisquer bases legais dispostas na LGPD ao atendimento de seus requisitos legais somado à observância do melhor interesse, é necessário pensar em circunstâncias de mitigação de riscos inerentes nos casos em que os dados precisam ser tratados. Ou seja, é relevante que a ANPD apresente critérios para o sopesamento de riscos identificados em casos de tratamentos que se mostram necessários (por exemplo, para execução de um contrato, ou ainda cumprimento de uma obrigação legal à qual o controlador esteja sujeito) e riscos inerentes da atividade que não conseguirão ser afastados em prol do melhor interesse do menor.Como exemplo cita-se eventual tratamento de dados biométricos como mecanismo para prevenção à fraude em aplicações, partindo do pressuposto que já tenha sido avaliada sua proporcionalidade. Nesse caso, ao fazer o sopesamento de interesses, é possível enxergar que a proteção à segurança e à identidade da criança estão em linha com o resguardo de seu melhor interesse. Contudo, há riscos inerentes ao tratamento de dados biométricos de crianças, por exemplo em relação às suas mudanças enquanto indivíduo em desenvolvimento e a fragilização da acurácia a longo prazo. Assim, questiona-se o que a ANPD poderia orientar aos agentes de tratamento em relação aos riscos residuais inerentes à atividade. Orientações neste sentido são necessárias pois o tratamento de dados pessoais de menores por diversas vezes é imprescindível e detém papel relevante nas atividades de tratamento de um controlador. Assim, ao invés de vedar essa utilização ou inserir restrições excessivas, a contribuição maior da ANPD é no sentido de indicar caminhos e fornecer insumos sobre como viabilizar esse tipo de operação. Por fim, pontuamos que não há necessidade, a priori, de uma regulamentação específica sobre o melhor interesse, na medida em que o ECA (Estatuto da Criança e do Adolescente) já fornece base sólida para a proteção dos direitos da criança no Brasil.","708725":"Consideramos que as seguintes situações demandam maior detalhamento orientativo pela ANPD acerca do princípio do melhor interesse: (a) indicativos do melhor interesse a serem avaliados pelos controladores; (b) cenários que demonstrem e comparem a observância e a violação ao melhor interesse; e (c) flexibilização ou presunção de melhor interesse em contextos determinados.A) Orientação sobre indicativos para cumprimento do princípio do melhor interesse: Da perspectiva do princípio de responsabilização e prestação de contas, é relevante que o controlador possua orientações sobre como documentar e gerar evidências sobre o cumprimento do princípio do melhor interesse da criança e do adolescente. Assim, a Autoridade poderá fornecer indicativos práticos, exemplificativos e não taxativos sobre seu entendimento acerca dos aspectos englobados pelo princípio do melhor interesse da criança, inclusive considerando o ambiente digital. Conforme trazido pela ONU no Comentário Geral nº 25 de 2021 (do

Comitê dos Direitos da Criança), o melhor interesse é um conceito dinâmico e que depende de análise contextual. Assim, é importante que a ANPD considere a natureza adaptável do princípio ao estabelecer estes indicativos não vinculantes para mensurar se o princípio está sendo cumprido ou não. A título de exemplo, a ANPD poderá demonstrar quais elementos poderão ser contemplados em uma avaliação sobre o melhor interesse, como: a opinião da criança; qual(is) direito(s) são promovidos, resguardados ou ao menos não impactados; adoção de meios menos intrusivos; entre outros, ponderados conforme caso concreto. De toda forma, em que pese seja necessária a orientação sobre indicativos para avaliar e documentar o melhor interesse, não entendemos ser uma medida razoável a exigência de um novo documento não previsto em lei para este fim, como testes de balanceamento específicos que onerem os controladores. Porém, a ANPD poderá indicar sobre o cabimento de incluir tal evidência em instrumentos já existentes como registro de atividades de tratamento ou relatório de impacto à proteção de dados pessoais, bem como quais elementos espera que sejam registrados. B) Orientação sobre situações de observância ou violação ao princípio do melhor interesse: Assim como tem sido a abordagem da Autoridade em outros materiais orientativos, reforçamos a importância de se apresentar vários exemplos de situações detalhadas sobre tratamentos de dados envolvendo o melhor interesse e que afetem a liberdade fundamental do menor enquanto ser em desenvolvimento. Essa é uma ideia relativamente subjetiva e que carece de interpretações práticas até o presente momento. A partir de exemplos concretos, abordando tanto situações simples quanto casos mais complexos, se torna mais factível para os controladores entenderem tanto situações em que o melhor interesse é atendido, quanto os limites para que seja interpretado pela ANPD como uma violação ao princípio. Estas orientações se complementam ao item (a) anterior, demonstrando a aplicação dos indicativos para alcançar o atendimento ao princípio do melhor interesse. C) Flexibilização ou presunção de melhor interesse: É relevante que a ANPD se posicione quanto à necessidade de comprovação do melhor interesse do menor por determinados agentes específicos ou situações inerentemente vinculadas à promoção do melhor interesse. É o caso, por exemplo, de entidades, fundações e ONGs voltadas especificamente para os direitos das crianças, como instituições de assistência social, centros de adoção, fundações de apoio à educação, entre outros. Nessas circunstâncias, especialmente quando a missão institucional estiver atrelada a aspectos de promoção de interesses de crianças e adolescentes, é relevante questionar até que ponto é razoável e proporcional onerar o agente de tratamento na demonstração do melhor interesse. Assim, como sugestão visando proporcionalidade e efetividade nas ações reguladoras da Autoridade, seria relevante se a ANPD considerasse eventual legitimidade presumida que permitisse uma flexibilização aos agentes de tratamento para as obrigações relativas às demonstrações de cumprimento ao princípio do melhor interesse.","705523":"Preliminarmente, entendemos que a ANPD deve evitar a adição de critérios exaustivos para a validade do consentimento, além do que a LGPD já apresenta, para não tornar sua aplicação prática algo de difícil operacionalização. Para tanto, poderá observar diretrizes que também se apliquem para especificidades exigidas ao consentimento para tratamento de dados pessoais sensíveis, sem causar ônus adicionais aos controladores. A) Parâmetros acerca do consentimento “específico” • Consentimento para finalidades determinadas A LGPD (artigo 8º, § 4º) determina que as autorizações genéricas

para o tratamento de dados pessoais serão nulas e que o consentimento deverá referir-se a finalidades determinadas. Assim, a ANPD poderá guiar-se por esta disposição, considerando a especificidade vinculada a finalidades determinadas. Nesse sentido, o European Data Protection Board, nas Diretrizes 05/2020 relativas ao consentimento na acepção do Regulamento 2016/679 de 2020, indica que o consentimento "específico" se dá em função da finalidade e granularidade. Sobre a limitação de finalidade, a autoridade francesa CNIL, na publicação "Conformité RGPD: comment recueillir le consentement des personnes?" reforça o entendimento do EDPB ao pontuar que a autorização deve corresponder a uma única operação de tratamento, para uma finalidade específica e que os indivíduos devem ser capazes de consentir de forma independente quando o tratamento tiver diversas finalidades. Já a autoridade britânica ICO, na publicação "What is valid consent?", complementa o posicionamento do EDPB ao indicar que o controlador deve oferecer opções granulares para consentir separadamente a finalidades distintas, a menos que isso seja excessivamente disruptivo ou confuso. • Consentimento específico como oposição ao consentimento genérico A ANPD poderá orientar aos controladores exemplos de situações que configurariam o consentimento genérico e, portanto, inválido. Assim, os controladores identificariam os elementos que tornam o consentimento inválido para garantir que nenhum desses elementos é preenchido em suas atividades. B) Parâmetros acerca do consentimento "em destaque" • Facilidade de identificação do consentimento Um dos objetivos do consentimento "em destaque" é assegurar que seja identificado facilmente, conforme avaliação contextual e o meio de obtenção deste consentimento. Assim a Autoridade poderá orientar sobre práticas de destaque, com exemplos de aplicações proporcionais ao caso concreto e contextual. Como referência, o EDPB indica, nas Diretrizes 05/2020 mencionadas previamente, sobre a necessidade de separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões. Outros exemplos contextuais: a criação de uma seção específica para "consentimento para o tratamento de dados de criança" poderá ser razoável em meio a um documento extenso que tenha um sumário facilitado e em camadas, mas poderá ser desproporcional para um formulário simplificado. Ainda, há casos em que recursos visuais poderão ser efetivos, ou ainda pop-ups em aplicativos e plataformas poderão ser utilizados. • Ausência de técnicas enganosas ou obscuras A ANPD poderá ilustrar seu entendimento sobre consentimentos mascarados, escondidos ou ofuscados, por exemplo, pelo uso de recursos obscuros que desviem a atenção do pai ou responsável, como práticas que tornam o consentimento inválido. O material do EDPB "Diretrizes 3/2022 sobre padrões obscuros em interfaces de plataformas de mídia social: Como reconhecê-los e evitá-los" elucida essas práticas que retiram o "destaque" do consentimento, por exemplo, quando este está diluído em meio a outras informações, como termos de uso ou avisos de privacidade extensos e pouco claros, ou, ainda, em seções descontextualizadas. Da mesma maneira, recursos visuais que deixem o consentimento em letras miúdas ou em cores que dificultem sua leitura também representam um consentimento inválido. ","708742":"Primeiramente, destacamos que as medidas e mecanismos encontrados como boas práticas de mercado e entre as orientações de reguladores internacionais são sempre acompanhados de uma perspectiva de proporcionalidade e razoabilidade, a depender do risco do tratamento de dados

pessoais para o qual o consentimento é solicitado. Este é o posicionamento de autoridades estrangeiras como CNIL, na França (“Recommendation 7”) e DPC, na Irlanda (“Fundamentals for a child-oriented approach to data processing”), que indicam que a coleta de dados dos pais e responsáveis ou das crianças e adolescentes para verificação do consentimento parental e de seu vínculo enquanto pai ou responsável não deve exceder o tratamento para o qual será obtido o consentimento, considerando a minimização de dados e a adequação. Com relação aos mecanismos sugeridos, o Federal Trade Commission dos Estados Unidos, em material intitulado “A guide for businness and parentes and small entity compliance guide”, traz uma lista não exaustiva de exemplos interessantes que podem servir como boas diretrizes para a ANPD ao estipular maneiras de validar o consentimento fornecido pelos responsáveis no ambiente digital, a serem avaliadas de acordo com o contexto do tratamento: • Exigir que o pai, em conexão com uma transação monetária, use um cartão de crédito, cartão de débito ou outro sistema de pagamento on-line que forneça notificação de cada transação discreta ao titular da conta principal; • Exigir que os pais liguem para um número de telefone gratuito, ou se conectem via videoconferência, com pessoal treinado para identificar a relação deste adulto com a criança; • Verificar a identidade de um dos pais por meio de um formulário de identificação emitido pelo governo a partir de bancos de dados com tais informações; • Exigir que um dos pais responda a uma série de perguntas de desafio baseadas em conhecimentos que seriam difíceis de responder a alguém que não o progenitor; • Verificar a identidade do adulto a partir da comparação entre a foto de algum documento de identificação enviado pelo responsável com uma segunda foto enviada por este mesmo responsável, usando tecnologia de reconhecimento facial. Cada medida deverá ser avaliada conforme o risco do tratamento, para não configurar um tratamento excessivo, inclusive sob uma perspectiva de custos e tecnologias disponíveis à época. Nesta perspectiva de proporcionalidade ao risco, cita-se o exemplo apresentado pelo EDPB em nas Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 de 2020: (1) em casos de baixo risco, a verificação da responsabilidade parental por e-mail pode ser suficiente, pela qual o controlador informa a criança de que um dos pais ou responsáveis deve consentir, solicitando que forneça o e-mail do responsável e posteriormente o controlador o contata para obter o consentimento; (2) e em casos de alto risco, pode ser adequado solicitar mais provas como: solicitar ao responsável o pagamento de R$0,01 através de transferência bancária, incluindo uma breve confirmação no espaço para observações da transação que o titular da conta é o titular da responsabilidade parental em relação ao utilizador; ou contratar serviços de verificação para tanto, mas evitando soluções que por si só representem uma coleta excessiva de dados. Em conclusão, a verificação do consentimento parental no ambiente digital exige uma abordagem multifacetada, sendo necessário garantir o equilíbrio entre a adequação e proporcionalidade das medidas adotadas, minimizando os riscos e maximizando a proteção dos direitos das crianças, sem onerar excessivamente os controladores. ","708745":"Exigir um consentimento assistido ou a representação dos representantes legais de um adolescente a cada coleta de autorização para tratamento de dados pessoais seria uma medida que, em muitos casos, poderia contrariar o melhor interesse do menor e representar um ônus excessivo aos controladores. Assim, o caminho a ser adotado é coerente com o conceito de autonomia progressiva dos adolescentes.

Já temos exemplos na legislação pátria de que a capacidade civil não é absoluta, com exceções no código civil e em esferas onde a manifestação de vontade autônoma de adolescente é fomentada – como o direito ao voto facultativo aos 16 anos. Considerando que a capacidade de discernimento varia entre adolescentes de 12 e 17 anos, a depender do contexto, é relevante buscar da ANPD quais elementos os controladores deverão observar para avaliar este discernimento em sua realidade, viabilizando mecanismos de consentimento "autônomo", ou assistido, caso necessário. Dito isso, apresentamos posicionamentos de autoridades estrangeiras convergentes com o consentimento seguindo a autonomia progressiva: • ICO, Reino Unido (ICO'S Age-Appropriate Design Code): adolescentes podem consentir para tratamentos de dados que não apresentem grandes riscos. O ICO se baseou em um estudo sobre o desenvolvimento cognitivo por faixa etária, e entendeu que a autonomia deve estar atrelada aos riscos, porque na adolescência é comum superestimarem sua capacidade de lidar com riscos e desafios derivados de comportamentos e relacionamentos online. Portanto, ainda que a eles seja garantida certa autonomia, são jovens que ainda podem se beneficiar de orientações e, em certos casos, apoio parental. • DPC, Irlanda ("Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing"): adolescentes poderão consentir a partir dos 16 anos, mas isso não afasta as demais proteções visto que a infância ainda é considerado espaço protegido até os 18 anos. Ou seja, a autonomia concedida para fornecimento do consentimento do adolescente não significa tratar adolescentes como adultos. • CNIL, na França ("8 recommendations to enhance the protection of children online"): por um lado, adolescentes acima de 15 anos podem dar seu próprio consentimento quando isto não implicar em efeito contratual, podendo aceitar cookies ao visitar um site, definir seu perfil de rede social como público ou privado ou ativar um recurso opcional de geolocalização em um aplicativo. Já para consentimentos "contratuais", a análise deve ser contextual, considerando se: a) os serviços são adequados para um público infantil; b) o tratamento estiver em conformidade com as regras de proteção de dados; c) a criança recebe informações claras e adequadas sobre o tratamento e sobre seus direitos; e nos casos de contas online, d) os pais têm o direito de solicitar a exclusão da conta se necessário para proteger os interesses de seus filhos. Com relação a crianças com menos de 15 anos de idade, existe o instituto do "consentimento conjunto", baseado em um acordo conjunto entre a criança e os pais para casos não contratuais. Nesses casos, os pais não podem ir contra a vontade do filho e o filho não pode anular a objeção dos pais, garantindo a qualidade do consentimento dado e o incentivo para buscar e levar em conta as opiniões do filho. Entendemos necessário obter da ANPD um posicionamento que considere elementos contextuais no conceito de autonomia progressiva, como: tipo de serviço a ser contratado, riscos do tratamento, efeitos do consentimento solicitado, e o discernimento e a opinião do adolescente. Ainda, é relevante que a ANPD aborde as consequências do consentimento – ou revogação deste - pelo adolescente em relação a eventual consentimento parental prévio. O tema já conta com posicionamento do EDPB, como referência, nas "Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, ao pontuar que o consentimento parental pode ser confirmado, modificado ou retirado assim que o titular dos dados atinja a idade para dar consentimento digital, e o controlador deverá informar a criança acerca dessa possibilidade.","705539":"Identificamos os seguintes parâmetros principais: (a)

minimização de dados; e (b) privacidade desde a concepção. A) Minimização de dados A autoridade britânica ICO no Children's Code - Age Appropriate Design: a code of practice for online service discorre sobre a minimização e a coleta mínima, que devem estar atreladas à finalidade específica do serviço online prestado, de modo que sejam coletados apenas os dados essenciais. Por exemplo, durante a criação de contas dos menores para jogos online, seria razoável coletar dados como nome de usuário e senha, mas devem ser evitadas informações como nome completo, endereço ou dados escolares. Já no caso de plataformas educacionais, por exemplo, estes últimos dados poderiam ser considerados como necessários. Ainda, a coleta de dados de localização de menores deve ser limitada a situações estritamente necessárias para o funcionamento do serviço, assim como cookies ou quaisquer outras tecnologias de rastreamento que coletam dados pessoais desnecessários. Por exemplo: uma ferramenta de controle parental que disponibilize funções de segurança para que pais localizem onde está o celular da criança e saibam onde ela está representaria uma situação em que a coleta de dados de localização é aceita; já a coleta deste mesmo dado para desbloquear customização de recursos de jogos (como "skins" de personagens), excederia a necessidade. Neste material, o ICO ainda orienta que a coleta de dados pessoais ocorra apenas quando o menor estiver usando ativamente e conscientemente aquele elemento do serviço. Deve, também, ser ressaltado para os controladores a importância de revisar regularmente a necessidade de armazenamento de dados e excluir qualquer informação desnecessária, minimizando a retenção de dados pessoais, para além da coleta. Por fim, a autoridade britânica também sugere a desidentificação de dados pessoais de menores antes de utilizações para fins secundários, como pesquisa e desenvolvimento de produtos. B) Privacidade desde a concepção Quanto a medidas de design a serem levadas em conta durante o desenvolvimento de ferramentas, como em plataformas de jogos online, indicamos as diretrizes previstas pela autoridade norueguesa de proteção de dados pessoais no guia "Datatilsynet Principles on Children & Online Gaming": • As configurações que interferem na privacidade e na proteção de dados das crianças devem ser desabilitadas por padrão. Isso inclui evitar o rastreamento de localização geográfica, acesso a contatos, gravação de voz, sincronização com mídias sociais, a menos que sejam fundamentalmente necessários para o funcionamento do jogo; • A natureza dos jogos online pode levar à coleta de uma grande quantidade de dados pessoais sobre as crianças. No entanto, sugere-se que as plataformas devam evitar a coleta automática e análise de dados para fins como a criação de perfis de jogadores, a derivação de dados sobre a personalidade da criança ou suas habilidades cognitivas. • Por fim, no lugar de coletar dados detalhados sobre as crianças, plataformas devem oferecer opções de personalização que permitam que as crianças escolham o gênero de jogo, o nível de dificuldade, sem a necessidade de coletar dados adicionais.","708762":"A) Técnicas sugeridas para verificação de idade em ambientes digitais.Com base no ICO no Children's Code e em práticas de mercado, conforme relatório da Fundação 5Rights "But how do they know it is a child? Age assurance in the digital world", indicamos as seguintes técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais:Autodeclaração com mecanismos de dissuasão: permitir que o usuário declare sua idade, mas utilize mecanismos de dissuasão, como questionários sobre cultura popular ou eventos recentes, para desencorajar declarações falsas.Provas de idade digitais: como

carteiras de identidade digitais para verificar a idade do usuário.Verificação de idade por proxy: solicitar a confirmação de idade por um adulto responsável, como um pai ou responsável legal. Esse método pode ser eficaz para crianças mais novas, mas exige mecanismos seguros para garantir a identidade do adulto e o consentimento informado.Ainda, o FTC também divulgou em sua página, os métodos de verificação que não foram aprovados para fins de cumprimento com os requisitos da lei estadunidense Children's Online Privacy Protection Act.Assim, a ANPD poderá orientar que as abordagens a seguir sejam evitadas:Análise de características biométricas: por meio de tecnologias que analisam imagens do rosto ou da voz para estimar a idade do usuário são imprecisas, invasivas e podem perpetuar vieses existentes.Rastreamento comportamental: coletar dados sobre o comportamento online do usuário para deduzir sua idade, já que caracteriza prática obscura, imprecisa e levanta sérias preocupações éticas.B) Tópicos complementares sobre verificação de idade. Proporcionalidade: Nos materiais de autoridades estrangeiras mencionados neste tópico houve convergência para a necessidade de que as técnicas empregadas para verificação de idade sejam minimamente invasivas e protejam a privacidade, sendo proporcionais em relação ao risco do tratamento de dados pessoais.A CNIL, nas “Recommendation 7”, ressalta a importância de se buscar mecanismos simplificados, ou seja, soluções simples e fáceis de usar, que consigam, por exemplo, cumular verificação de idade com consentimento parental, quando aplicável. O objetivo é não gerar diretrizes de operacionalização dificultada para os usuários e para o controlador, considerando os custos e a tecnologia disponível.Com base no relatório da Fundação 5Rights previamente mencionado, é relevante que a ANPD forneça exemplos de situações em que a verificação de idade provavelmente não será necessária. Por exemplo: quando os produtos e serviços já tenham sido concebidos com a implementação de mecanismos de design específicos para atender ao público de crianças e adolescentes, então a idade não influenciaria na definição do design; ou, quando o produto ou serviço requerer a identificação de um usuário único pelo qual já se tenha atribuído sua idade, tornando desnecessário verificá-la novamente (como usuários de plataformas educacionais com cadastro). E, pensando no melhor interesse do menor e da oportunidade de estimular sua autonomia, a ANPD poderá sugerir métodos de como envolver as crianças e adolescentes na implementação de sistemas de verificação de idade, oferecendo opções de controle sobre seus dados.Adequação do tratamento de dados pessoais para verificação de idade. A verificação de idade implicará em um tratamento de dados pessoais – para o qual já se reconhece uma finalidade legítima, conforme indicado na AVMSD. Assim, o tratamento relativo à verificação de idade não deverá implicar em usos secundários, sendo recomendável a exclusão dos dados coletados durante este processo assim que o nível adequado de confiança quanto à idade do usuário for atingido.Sobretudo, neste momento de verificação, independentemente do método escolhido, é importante reforçar a necessidade de ser transparente com o usuário sobre como sua idade está sendo verificada. ","708764":"O art. 14, § 4º da LGPD prevê que controladores não deverão condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Nesse sentido, entendemos que a ANPD deve ter cuidado especial ao abordar a questão de formação de perfis comportamentais. Esse tem sido um tema bastante discutido internacionalmente e, dada

a sensibilidade das informações que engloba, merece atenção especial da Autoridade.O objetivo não é que a ANPD determine uma proibição quanto à formação de perfis comportamentais, mas oriente os controladores sobre que circunstâncias consistiriam em riscos a esta categoria, desafiando inclusive o princípio do melhor interesse. Assim, o balizamento para determinar as orientações sobre o tema não precisa fugir do que já se debate acerca do tema de melhor interesse, mas acomodar exemplos claros envolvendo casos de perfilização.Por exemplo, no cenário internacional, o EDPB pontua nas Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 que a tomada de decisões automatizada, incluindo profiling, não deve ser usada em relação aos dados de crianças, exceto em circunstâncias necessárias para proteger seu bem-estar e integridade. No mesmo contexto, o Conselho da Europa e o Comitê das Nações Unidas sobre os Direitos da Criança, por meio do Comentário Geral nº 25 do Comitê das Nações Unidas sobre os Direitos da Criança no Ambiente Digital (2021), também indicam exceções apenas quando estritas para o bem da criança ou para o interesse público, e, enfatizando os riscos de dados imprecisos e a interferência na capacidade das crianças de formar suas próprias opiniões. Ainda, o EDPB exemplifica nos Guidelines mencionados anteriormente que, em determinadas circunstâncias, a publicidade direcionada a crianças com base em profiling não deve ser realizada, considerando que este grupo de indivíduos pode ser particularmente suscetível no ambiente online e mais facilmente influenciado pela publicidade comportamental. Para o cenário brasileiro, a ANPD poderá atrelar estas situações às disposições já existentes sobre publicidade infantil, contribuindo com exemplos de tratamentos ilegítimos quando estes corresponderem a práticas abusivas proibidas, conforme Código do Consumidor. Nessa mesma linha, no guia “Fundamentals for a Child-Oriented Approach to Data Processing”, o Data Protection Commission (DPC), a autoridade irlandesa de proteção de dados, entendeu que não se deve deve perfilar crianças, nem as envolver em tomada de decisões automatizadas ou usar seus dados pessoais para fins de publicidade/marketing, a menos que o controlador possa demonstrar como e por qual motivo esse tratamento de dados seria do interesse do menor. Assim como o DPC, a ANPD pode apresentar exemplos do que interpretar como uma finalidade alinhada aos interesses das crianças no âmbito de publicidade. Por fim, como um contraponto a também ser levado em consideração pela ANPD, trazemos a opinião do ICO em orientação publicada “Automated decision-making and profiling”, que destacou que o profiling pode ser adequado, citando como exemplo quando for utilizada uma ferramenta de verificação de idade, desde que os controladores (1) informem os usuários antecipadamente sobre isso, (2) coletem apenas a quantidade mínima de dados pessoais que precisam para esse fim e (3) não usem nenhum dado pessoal que coletem para esse fim para outros fins. ","708768":"A) Mecanismos sugeridos para controle parental no ambiente digital É pertinente que a ANPD leve em conta as diferentes idades desses jovens e sua autonomia progressiva. As recomendações de métodos abaixo levam em consideração as faixas etárias definidas pelo ICO no “Children’s Code - Annex B: Age and developmental stages” acerca do desenvolvimento cognitivo em cada etapa: Para crianças mais novas, em idade pré-escolar e primeiro ciclo do ensino fundamental, sugerimos: • Restrição de conteúdo: bloquear o acesso a conteúdo impróprio, como violência, pornografia e linguagem inapropriada. • Limitação de tempo de tela: definir

limites de tempo para o uso de dispositivos, incentivando atividades offline e interação social. • Bloqueio de compras: impedir compras acidentais ou não autorizadas dentro de aplicativos e jogos. Já para crianças mais velhas, no segundo ciclo do ensino fundamental e adolescentes, sugerimos: • Gerenciamento de redes sociais: supervisionar o uso de redes sociais, orientando sobre privacidade, cyberbullying e contato com estranhos. • Controle de localização: permitir o compartilhamento de localização apenas com contatos confiáveis e em situações específicas. • Monitoramento de atividades: acompanhar o histórico de navegação, downloads e interações online, sempre com diálogo e respeito à privacidade. B) Tópicos complementares sobre controle parental • Proporcionalidade Embora a ANPD busque mecanismos para ampliar o controle parental, é relevante considerar que implementação efetiva dos controles varia de acordo com a dinâmica familiar e o discernimento da criança, bem como o tipo de tratamento de dados e os riscos atrelados. Com base em diretrizes do ICO no "Children's Code - 11. Parental controls", o diálogo aberto e constante, a construção de uma relação de confiança e o acompanhamento atento às necessidades de cada criança são fundamentais para garantir uma experiência online segura e positiva. Neste sentido, a CNIL pontua em seu material "Recommendation 5: Promote parental controls that respect the child's privacy and best interests" que mecanismos intrusivos podem causar um sentimento de constante monitoramento prejudicial aos melhores interesses da criança, sendo importante buscar as oportunidade de intervenção ou supervisão dos pais e responsáveis com limites claros orientados para resguardar sua segurança. • Transparência sobre o controle parental A orientação às crianças e adolescentes deve ser transparente, informando que controles parentais estão em vigor, de forma contextualizada e quais são os limites de como podem exercer controle sobre seus dados. Nesse sentido, as informações a serem fornecidas e formatos adequados poderão variar conforme cada faixa etária em relação ao desenvolvimento cognitivo de crianças e adolescentes, conforme os seguintes exemplos do ICO no Children's Code - 11. Parental controls: para crianças em idade pré-escolar até primeiro ciclo do ensino fundamental, pode ser adequado o fornecimento de materiais de áudio ou vídeo para a criança explicar que seus pais estão sendo informados sobre o que ela faz on-line para ajudar a mantê-la segura; já para adolescentes até estágios próximos da fase adulta, é razoável fornecer materiais escritos descrevendo como seu serviço funciona e o equilíbrio entre os direitos de privacidade dos pais e do adolescente. • Orientações aos pais e responsáveis pela ANPD Por fim, a efetividade de uma experiência online segura e positiva nos ambientes digitais não se esgota apenas na atuação de controladores de dados, sendo uma tarefa compartilhada com os pais e responsáveis. Assim, a ANPD poderá contribuir com orientações destinadas aos pais e responsáveis abordando, por exemplo, os seguintes aspectos: • Diálogo e confiança: priorizar a conversa sobre os riscos online, incentivando a responsabilidade e o uso consciente da tecnologia. • Acordos familiares: estabelecer regras claras em conjunto sobre o uso de internet, mídias sociais e jogos, definindo limites e consequências. • Ferramentas de segurança: orientar sobre o uso de senhas fortes, softwares de segurança e como identificar e evitar golpes online.","708772":"Considerando o artigo 14 § 6º da LGPD, o pilar de qualquer comunicação com crianças e adolescentes deve ser a transparência clara, acessível e compreensível, considerando as particularidades deste público-alvo. Assim, entendemos que a ANPD poderá

promover orientações não exaustivas que explorem o atendimento ou não dessa adequação de linguagem, para que controladores possam aplicá-las conforme sua própria realidade. A Data Protection Commission (DPC), autoridade irlandesa de proteção de dados, apresenta no guia "Fundamentals for a Child-Oriented Approach to Data Processing" a importância da transparência como um direito independente para as crianças, no sentido de que têm direito a receber informações sobre o tratamento de seus dados pessoais, mesmo que um pai ou responsável tenha consentido em seu nome. Contudo, o DPC não propõe que as organizações necessariamente forneçam dois conjuntos separados de informações para adultos e crianças quando tiverem um público misto de usuários infantis e adultos, mas indica que se a informação for clara e simples o suficiente para uma criança entender, ela também atenderá ao requisito de transparência para adolescentes e adultos. Assim, os controladores devem garantir que o vocabulário, tom e estilo da linguagem usada para transmitir as informações sobre o tratamento de dados pessoais sejam apropriados e ressoem com as crianças para que reconheçam que a mensagem está sendo direcionada a ela. Nesse sentido, entendemos que podem ser eficientes para o fornecimento de informações de maneira simples, clara e acessível quanto ao tratamento de dados pessoais de crianças e adolescentes: • Uso de métodos não textuais, como desenhos animados, vídeos, imagens, ícones ou gamificação, para transmitir informações sobre proteção de dados de forma mais eficaz. Esses métodos são mais propensos a ressoar com as crianças do que blocos de texto. • Uso de formatos que sejam mais aplicáveis e relevantes ao serviço que oferecem. Por exemplo, se operam uma plataforma de serviços educacionais, o conteúdo mais lúdico e interativo provavelmente será um meio mais apropriado para transmitir informações de transparência para crianças do que uma imagem ou um texto. • Apresentação de informações de forma atraente, por exemplo, usando tamanhos de fonte grandes, listas de marcadores fáceis de ler, cores. Considerar apresentar trechos breves, de modo a facilitar a compreensão. • Disponibilizar as informações essenciais sobre proteção de dados no início e incentivar as crianças ativamente pelos controladores a descobrir mais sobre como seus próprios dados pessoais serão usados e como esse uso as afetará, por exemplo, por meio de botões clicáveis. • Uso de notificações oportunas e contextuais ao longo das interações para informar crianças e adolescentes sobre o tratamento de dados pessoais. Exemplos de momentos oportunos incluem: antes de postar ou compartilhar algo online, antes de alterar as configurações de privacidade padrão. • Fornecer explicações às crianças sobre o motivo pelo qual determinadas configurações são automaticamente desativadas ou negadas a elas por padrão. Caixas de aviso devem ser exibidas se as crianças usuárias tentarem ativar essas configurações e informações fornecidas explicando por que determinadas configurações de controle de usuário se aplicam a elas. • Incentivo, por meio de pop-ups ou prompts, por exemplo, para que crianças perguntem aos pais/adultos de confiança se tiverem alguma dúvida sobre as informações de transparência que receberam. ","708775":"Destacamos dois temas principais: (a) direitos dos titulares; e (b) tratamento de dados de geolocalização. A) Direitos dos titulares Como tópico complementar à discussão de consentimento de adolescente e consentimento parental, bem como sobre controle parental, é relevante que a ANPD considere direcionar orientações no que tange ao exercício de direitos de crianças e adolescentes enquanto titulares detentores destes direitos. É razoável que determinados

direitos possam ser exercidos livremente por menores (como confirmação de tratamento, solicitação de informações sobre entidades com as quais houver compartilhamento etc.), e que pais e responsáveis desempenhem seu controle apenas para gestão ou acompanhamento. Já para exercício de direitos que possam gerar consequências aos menores, pais e responsáveis poderiam ser aproximados para ratificar ou intervir nas requisições, como em requisições para correção ou eliminação de dados. Nesse sentido, o ICO indica no material "What rights do children have?" elementos para que o controlador verifique se no caso concreto a criança pode entender seus direitos e suas implicações, levando em conta: o nível de maturidade da criança para tomar decisões como essa; a natureza dos dados pessoais; se há ordens judiciais relacionadas ao acesso ou responsabilidade dos pais; se há dever de sigilo devido ao menor; as consequências de permitir acesso aos responsáveis para exercer os direitos da criança – se houver alegações de abuso ou maus-tratos; qualquer prejuízo para a criança ou o adolescente se os responsáveis não puderem acessar os dados; e a opinião do menor sobre se seus pais devem ter acesso às informações sobre eles. Discutir limites para atuação parental em relação a direitos dos titulares já foi objeto de posicionamento do EDPB nas Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 de 2020, ao ressaltar que o consentimento parental poderá ser alterado quando for alcançada a autonomia necessária pelo titular, por exemplo caso seja atingida sua maioridade. Assim, é relevante que a ANPD suscite este tema a fim de orientar controladores de que precisarão se preparar para um cenário mutável e viabilizar meios para recebimento e atendimento de requisições neste contexto. B) Tratamento de dados de geolocalização Entendemos que o tratamento de dados de geolocalização de crianças e adolescentes é um tema relevante e sobre o qual a ANPD poderia prestar maiores esclarecimentos. Por ser um tipo de dado particularmente crítico, já que pode colocar a segurança física da criança em risco, seria relevante que a Autoridade estabelecesse maiores diretrizes sobre como os controladores devem se portar frente a este tratamento e como garantir que ele está acontecendo da melhor forma. A Autoridade de Proteção de Dados de Singapura, Personal Data Protection Commission Singapore (PDPA), na publicação "Advisory Guidelines on the PDPA for Children Personal Data in the Digital Environment" traz como recomendação relevante aos controladores que desativem a geolocalização por padrão nos serviços prestados a esse público. Caso a geolocalização seja imprescindível para o fornecimento do serviço, sugerimos como salvaguarda a coleta da localização aproximada dos usuários em vez da localização exata, reduzindo o risco de uso indevido dos dados. A Data Protection Commission (DPC), autoridade irlandesa de proteção de dados, reitera as recomendações acima descritas no guia "Fundamentals for a Child-Oriented Approach to Data Processing", sugerindo que os controladores desativem a geolocalização por padrão para usuários infantis, a menos que o serviço prestado dependa necessariamente dela; se esse for o caso, deixe claro para a criança (por exemplo, por meio do uso de símbolos/ícones) que sua localização está disponível para o serviço ou pode ser vista por outros usuários. Ainda, é prevista a recomendação de que o controlador forneça controles visíveis para permitir que a criança interrompa o fornecimento da geolocalização a qualquer momento ou após cada sessão, após um curto período ou quando o evento ou recurso que exige localização for concluído.

Contribuinte: Adrielle campos da silva

Número: OP-729125

Data: 15/07/2024 - 16:36

Resumo: :"N/A","708725":"N/A","705523":"No contexto das plataformas e serviços digitais, o processo de consentimento relacionado aos termos e condições de privacidade online muitas vezes não é uma ação mútua. Em nosso estudo “Termômetro do Acesso Adequado à Idade: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais”, especialistas entrevistados ressaltaram que, frequentemente, as plataformas adotam um modelo unilateral que permite o monitoramento do usuário, o qual não tem outra opção senão aceitar os termos ou perder o acesso aos serviços. No que diz respeito ao consentimento sobre termos de uso e políticas de privacidade, é crucial destacar o risco de relações unilaterais que são apenas instrumentais, sem um processo de negociação, comprometendo a autonomia dos usuários e facilitando a invasão comercial e institucional da privacidade. Deve existir uma escolha granular e facilitada, apresentada de maneira acessível ao nível de desenvolvimento do usuário, assim como a garantia do consentimento informado antes da coleta de dados, explicitando claramente quais dados serão coletados e para quais finalidades. Por exemplo, um aplicativo que, antes de acessar a localização do usuário, explica de forma clara e compreensível por que precisa dessa informação, como será usada e se será compartilhada com terceiros. Ademais, consideramos importante que tais informações sejam apresentadas e adaptadas conforme a idade do usuário, seguindo o princípio da autonomia progressiva na usabilidade do serviço. No entanto, muitas vezes, a oportunidade de escolha não é suficiente para garantir a proteção do indivíduo. Além disso, delegar o ônus e a responsabilidade por certas decisões à criança, ao adolescente, ou mesmo ao responsável, não é adequado, uma vez que eles representam as partes mais vulneráveis da relação. Também, vai de encontro ao princípio da responsabilidade compartilhada, disposto no artigo 227 da Constituição Federal, no qual assegura que a defesa dos direitos de crianças e adolescentes é dever de todos os setores, inclusive empresarial. Assim, recomenda-se como uma das formas de proteção de crianças e adolescentes a adoção de princípios de privacidade por design. Exemplos da aplicação desse princípio incluem a definição de configurações de privacidade mais restritivas como padrão, permitindo que os usuários optem por compartilhar mais informações se desejarem; técnicas que tornam os dados pessoais anônimos para reduzir os riscos de identificação; e medidas robustas de segurança desde o início do desenvolvimento do serviço ou plataforma, visando proteger os dados contra acessos não autorizados e violações.","708742":"N/A","708745":"N/A","705539":"Como é sabido, o modelo de negócio das principais plataformas digitais é baseado na mercantilização de dados pessoais a partir da perfilização algorítmica dos usuários. Especialistas, como Shoshana Zuboff, Sonia Livingstone, Deivison Faustino e Walter Lippold, para citar alguns, apontam que esse modelo tem trazido impactos negativos para o exercício de direitos fundamentais, especialmente no que diz respeito à privacidade. Quando se trata de crianças e adolescentes, essa questão adquire contornos ainda mais problemáticos, uma vez que esses indivíduos estão ainda em processo de desenvolvimento, tornando-se dessa forma mais vulneráveis aos efeitos da superexposição online, dos vieses algorítmicos e de análises preditivas discriminatórias.

Para mitigar esses problemas, é fundamental a regulação do ambiente online, principalmente para proteção de crianças e adolescentes. Nesse sentido, conforme apontado no relatório "Termômetro do Acesso Adequado à Idade: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais", produzido pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), algumas medidas se fazem necessárias para salvaguardar os direitos desses indivíduos, sem que isso represente o afastamento total dos jovens desses espaços, já que também é preciso reconhecer o potencial desses espaços para trocas interpessoais, mobilização sociais, denúncias de abusos e para a formação da identidade de crianças e adolescentes. Entre as medidas apontadas no relatório, convém destacar a importância de: (1) Introduzir interfaces/funcionalidades adaptativas por faixas etárias e que levem em consideração o desenvolvimento progressivo na construção do serviço e/ou funcionalidade. (2) Adequar os serviços a partir da classificação indicativa dos conteúdos, definidos com base na faixa etária, ajustando os algoritmos de recomendação para trabalhar com base em métricas apropriadas para a idade, além das configurações alternativas estabelecidas pelos próprios usuários e/ou em conjunto com seus pais e responsáveis; (3)Utilizar design participativo com crianças e adolescentes, que conte com a presença de pais e responsáveis, além de um sistema garantidor de direitos na concepção dos produtos; (4) Tornar os termos de uso e privacidade acessíveis, diretos e compreensíveis, possibilitando a escolha granular e facilitada das configurações de maneira apropriada ao nível de desenvolvimento do indivíduo; (5) Estabelecer avisos lembrando crianças e adolescentes do alto tempo de uso, encorajando os jovens a sair do serviço para descansar; (6) Não adotar padrões obscuros/padrões enganosos na plataformas (7) Realizar periodicamente avaliações de riscos e de impacto, com testes periódicos, auditorias externas e internas, além da atualização dos algoritmos para coibir possíveis falhas e formas de burlar a segurança, bem como eventuais adaptações do produto/serviço; (8) Produzirem relatórios de transparência semestrais, com informações detalhadas sobre os critérios, métricas, metodologias e parâmetros usados nos algoritmos; (9) Minimizar a coleta de dados, a qual só pode ser realizada tendo em vista o seu melhor interesse; (10) Utilizar criptografia de ponta-a-ponta em base de dados e em plataformas e serviços; e (11) Definir configurações de privacidade e segurança mais restritivas como padrão, limitando a coleta de dados e interação dos jovens com pessoas desconhecidas. (12) Apresentar termos de uso e políticas de privacidade que possibilitem uma escolha granular e facilitada de maneira apropriada ao nível de desenvolvimento do indivíduo. ","708762":"N/A","708764":"Em que pese a Lei Geral de Proteção de Dados ter assegurado proteções adicionais aos dados pessoais de crianças e adolescentes em seu art. 14, o Enunciado CD/ANPD Nº 1, de 22 de maio de 2023, estabelece que o tratamento de dados tanto de crianças quanto de adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7° e 11° da LGPD, ampliando as possibilidades de tratamento e, consequentemente, fragilizando as proteções estabelecidas no dispositivos em questão. Antes disso, já havia divergências doutrinárias quanto à idade mínima para o consentir com tratamento de dados pessoais. Isso porque, sem mencionar adolescentes, o §1º do art. 14 determina que o tratamento de dados pessoais de crianças deve ser realizado com consentimento específico e destacado dos pais e responsáveis. Considerando o que dispõe o art. 2º do Estatuto da Crianças e do Adolescente (ECA), indivíduos a partir de 12 anos

completos teriam aptidão para dispor sobre o uso dos seus dados, contrariando o que estabelece o Código Civil sobre capacidade. A própria General Data Protection Regulation (GDPR) inclusive, apesar de admitir que os países membros disciplinem de forma diversa, adota como base a idade mínima de 16 anos para o consentimento quanto ao uso de dados. Com a consagração da doutrina da proteção integral a partir da promulgação da Constituição Federal de 1988 e, posteriormente, com o ECA, crianças e adolescentes foram reconhecidos como sujeitos de direitos. Dessa forma, reconheceu-se que é dever do Estado, da família e da sociedade assegurar, com absoluta prioridade, a efetivação dos seus direitos. Nesse sentido, é necessário estabelecer critérios mais rígidos para o tratamento de dados pessoais de crianças e adolescentes, os quais devem ser considerados dados sensíveis nos termos da lei. À luz desse contexto, é importante limitar as bases legais de tratamento, de modo a torná-las compatíveis, em todos os casos, com o melhor interesse desses indivíduos, bem como ampliar a idade mínima necessária para consentimento em conformidade com a legislação nacional em vigor. No que diz respeito especificamente ao §4º do art. 14, além de não condicionar a participação ao fornecimento de informações pessoais estritamente necessárias, é fundamental vedar o perfilamento de crianças e adolescentes para fins de publicidade comercial, anonimizar os dados sensíveis coletados desses indivíduos e também utilizar criptografia de ponta-a-ponta em base de dados e em plataformas e serviços.","708768":"A transparência e a instrução para a tomada de decisões informadas são as principais condições para que pais e responsáveis possam tomar decisões sobre a coleta e tratamento de dados que garantam o melhor interesse das crianças e adolescentes. Os dados de crianças e adolescentes, especialmente dados sensíveis, são protegidos por lei. É das organizações que coletam e tratam essas informações, portanto, a obrigação primordial de protegê-las com todo o rigor técnico e jurídico. Pais e responsáveis não podem ser os únicos responsáveis pelo cuidado com os dados digitais das crianças e adolescentes, sobretudo num país ainda tão marcado por desigualdades no acesso à educação e à tecnologia, o que significaria uma violação ao princípio da responsabilidade compartilhada, disposto no artigo 227 da Constituição Federal. (1) Uma boa prática inicial das empresas e organizações deve ser o levantamento sobre os dados que são efetivamente necessários coletar. A partir dessa definição, uma análise de risco deve apontar os impactos que o tratamento dessas informações podem ocasionar aos titulares dos dados. Pais, responsáveis e jovens devem ter acesso aos resultados do relatório de impacto de forma simplificada e em linguagem acessível. (2) Pais, responsáveis, crianças e adolescentes devem ter acesso às informações sobre a coleta e tratamento de dados desde o primeiro acesso à plataforma e no início do processo de cadastramento. Deve-se comunicar de forma clara e direta como e quais dados estão sendo coletados, para quê, como são tratados e com quem estão sendo compartilhados. Ademais, deve-se levar em consideração durante a comunicação o princípio da autonomia progressiva, adaptando para faixas etárias distintas a linguagem e a interface para o grau de maturidade da criança, adolescente e responsáveis. (3) Cada etapa do uso que requeira o processamento de dados precisa ser informada e consentida através de janelas pop-up, devendo haver a opção de negar a coleta e tratamento sem penalização para os usuários. (4) A retirada do consentimento sobre a coleta e tratamento de dados deve estar disponível de forma simples a qualquer momento. (5) Tanto os pais e responsáveis quanto às crianças e adolescentes devem ser instruídos sobre as melhores práticas para a proteção de

dados e sobre as ferramentas disponíveis nas plataformas para tal fim. Esse processo deve levar em consideração a diversidade sociocultural do Brasil, especialmente o grande percentual da população não alfabetizado adequadamente, a desigualdade no letramento digital, dificuldade de acesso a dispositivos digitais e à conexão com a Internet e a sobrecarga de atividades de trabalho e cuidado familiar. (6) Orientar-se pelos parâmetros do "privacy by design" é uma boa maneira de garantir a proteção das informações de crianças e adolescentes até que elas ou seus pais e responsáveis sintam-se seguros para adotar medidas menos protetivas. A prática inclui, por exemplo, a mínima coleta de dados por padrão, contas de crianças e adolescentes fechadas, e a desativação do chat e comentários para usuários desconhecidos. (7) É crucial que as plataformas digitais levem em conta a diversidade das formas familiares e dos contextos sociais dos usuários ao criar e aplicar suas políticas e ferramentas de mediação parental. Para garantir um ambiente digital realmente inclusivo, essas plataformas devem priorizar o desenvolvimento de interfaces acessíveis que atendam às necessidades de todas as famílias, independentemente de sua configuração ou situação socioeconômica.","708772":"Informações claras sobre tratamento de dados pessoais são fundamentais para que os direitos de crianças e adolescentes sejam efetivados. Atualmente, plataformas vêm utilizando estratégias de design e escrita para dificultar o acesso e a leitura dos termos de privacidade dos serviços. Pode-se identificar práticas de dificultar o acesso aos termos, como por exemplo dispor em locais poucos visíveis da interface, dando prioridade visual ao botão de aceite, assim como textos de difícil compreensão do público em geral. Como resultado, pesquisas nacionais e internacionais apontam que a maioria dos usuários não leem os termos com os quais supostamente estão consentindo. Nesse sentido, cabe haver um redirecionamento nas práticas nas formas como plataformas digitais apresentam termos de uso e privacidade são apresentados para os usuários. Boas práticas identificadas no nosso estudo "Termômetro do Acesso Adequado à Idade: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais" foram, por exemplo, a utilização de linguagem simples, clara, direta e sem jargões técnicos sobre como os dados pessoais estão sendo tratados. Uma das referências atuais é o Children's Code, do Reino Unido, no qual orienta que textos muito longos devem ser evitados, optando por versões curtas de como o dado será utilizado e para qual fim, nunca omitindo o real uso do que está sendo coletado. Aliado a isso, o Children's Code aponta como boa prática a adaptação da informação segundo a idade e grau de maturidade do leitor. Uma das formas de se atingir isso é por meio de interfaces adaptativas, que se modificam segundo a faixa etária do usuário, oferecendo a mesma informação de formas diferentes. Além disso, é entendido como boa prática, dependendo da faixa etária, envolver os responsáveis durante a interação da criança e adolescente com a informação. Outro ponto significativo para alcançar uma transparência no uso de dados é saber quando apresentar tais informações. Esse destaque, também feito pelo Código inglês, aponta para a importância de fazer com que etapas de aceite de termos, notificações e outras interações que envolvam dados pessoais dos usuários sejam realizadas em momentos que façam sentido lógico, como, por exemplo, criar e deletar contas.","708775":"A criptografia é a ferramenta mais poderosa para a garantia da privacidade e integridade dos dados eletrônicos. Ela deve ser encarada como uma aliada das crianças e adolescentes usuárias das plataformas e dispositivos digitais. Ela protege esses

jovens não apenas nos aplicativos de mensagens com criptografia de ponta-a-ponta, mas também nos dispositivos inteligentes, nas transações financeiras, nos bancos de dados onde guardam seus arquivos e numa ampla gama de experiências atravessadas pela informática e pela conexão à rede. Por isso, como forma de difundir esse conhecimento, o IP.rec traduziu o relatório produzido pela Child Rights International Network (CRIN) e defend digital me "Privacidade e Proteção: Uma abordagem dos direitos da criança à criptografia". Esforços para garantir a segurança e privacidade das crianças e adolescentes, como o uso de ferramentas de controle parental, caso apresentem vulnerabilidades, podem converter-se num mecanismo para o cometimento de crimes nas mãos de agentes mal-intencionados. É por isso que a adoção de sistemas robustos com criptografia forte deve ser uma condição essencial para o desenvolvimento de qualquer tecnologia que opere dados de crianças e adolescentes, especialmente dados sensíveis. Pais, responsáveis e jovens, a partir de esforços das empresas e do poder público, devem ser conscientizados sobre o papel fundamental que a criptografia pode desempenhar na proteção de suas famílias. Todos devem ser estimulados a adotar ativamente as ferramentas criptográficas em seu cotidiano e a exigirem que elas sejam implementadas nos ambientes e tecnologias onde ainda não estão disponíveis. Por fim, a criptografia pode garantir que crianças e adolescentes em condição de vulnerabilidade e exploração tenham acesso à justiça. Canais de denúncia sigilosos com criptografia de ponta-a-ponta são meios eficazes de interrupção de ciclos de violência física, psicológica e sexual, que muitas vezes ocorrem nas próprias casas desses jovens e são perpetrados por parentes que podem monitorá-los através do monitoramento de suas atividades nos ambientes e dispositivos digitais.

Contribuinte: MARCOS CESAR MARTINS PEREIRA

Número: OP-730313

Data: 16/07/2024 - 10:55

Resumo: :"I am including my comments in both English and Portuguese below: ","708725":"On behalf of the International Center for Law & Economics (ICLE), I am writing to offer our expertise and insights regarding the protection of children's personal data and online safety, particularly in the context of your current Call for Subsidies on this crucial topic. ICLE is a nonprofit, nonpartisan research center that has extensively studied and contributed to discussions on online safety, privacy legislation, and platform regulation, with a particular focus on balancing the protection of vulnerable groups like children with the preservation of free expression and access to information. Our work is grounded in rigorous economic analysis and a deep understanding of the legal frameworks that govern digital spaces, including principles akin to those outlined in Article 19 of the United Nations' International Covenant on Civil and Political Rights (ICCPR). We believe our expertise is particularly relevant to your efforts, given the complex interplay between children's safety, data protection, and the broader societal benefits of open internet access. Our research and policy recommendations consistently emphasize that protecting children's interests online is not simply a matter of passing stringent laws, but rather requires a nuanced approach that

carefully weighs the costs and benefits of regulation. Key Considerations for Laws that Effectively Protect Childrens' Interests 1. Balancing Protection and Access: While it's crucial to protect children from online harms, it's equally important to ensure that vital educational and entertainment opportunities remain accessible. There is a certain level of online access that is broadly recognized as beneficial for children's development and education. Regulations must be crafted with care to avoid inadvertently limiting these positive experiences. 2. Unintended Consequences of Regulations: Overly restrictive policies can have a chilling effect on digital platforms. In an attempt to minimize legal exposure, platforms may opt to completely remove children from their services. This approach, while seemingly protective, can ultimately deprive children of valuable online resources and experiences. 3. Economic Realities of Platform Operation: It's important to recognize that most digital platforms do not derive significant direct revenue from children, as this demographic typically lacks independent purchasing power. This economic reality means that burdensome child-specific regulations may incentivize platforms to exclude children entirely rather than navigate complex compliance requirements. 4.

Intermediary Liability and its Implications: Our work, particularly as outlined in our document "Who Moderates the Moderators?", delves into the delicate balance required in platform regulation. Imposing excessive liability on intermediaries for user-generated content can lead to over-censorship and reduced innovation, potentially limiting the development of child-friendly online spaces. 5. Cost-Benefit Analysis in Regulation: We strongly advocate for a thorough cost-benefit analysis of any proposed regulation. This approach helps ensure that the protective measures implemented do not inadvertently cause more harm than good by restricting children's access to beneficial online resources and experiences. ","705523":"Our Relevant Work and Resources To provide further context and depth to these considerations, we invite you to explore our extensive body of work on these topics. The following resources offer detailed analyses and recommendations that may be valuable to your regulatory efforts: 1. TL;DR: Children's Online Safety and Privacy Legislation https://laweconcenter.org/resources/childrens-online-safety-and-privacy-legislation/ 2. A Law & Economics Approach to Social Media Regulation https://laweconcenter.org/resources/a-law-economics-approach-to-social-media-regulation/ 3.

A Coasean Analysis of Online Age Verification and Parental Consent Regimeshttps://laweconcenter.org/resources/a-coasean-analysis-of-online-age-verification-and-parental-consent-regimes/ 4. Who Moderates the Moderators? A Law & Economics Approach to Holding Online Platforms Accountable Without Destroying the Internet https://laweconcenter.org/resources/who-moderates-the-moderators-a-law-economics-approach-to-holding-online-platforms-accountable-without-destroying-the-internet/ 5.

ICLE Comments to FTC on Children's Online Privacy Protection Rule NPRMhttps://laweconcenter.org/resources/icle-comments-to-ftc-on-childrens-online-privacy-protection-rule-nprm/ 6. ICLE Amicus to the 9th Circuit in NetChoice v. Bonta https://laweconcenter.org/resources/icle-amicus-to-the-9th-circuit-in-netchoice-v-bonta/ These resources provide in-depth analyses of various aspects of online child protection, platform regulation, and the economic implications of different policy approaches. They reflect our commitment to evidence-based policymaking and our expertise in navigating the

complex landscape of digital regulation. Conclusion We believe that effective protection of children's interests online requires a multifaceted approach that goes beyond simple prohibitions or restrictions. It demands a careful balance between safeguarding children and preserving the immense educational and social benefits that the internet can provide. We would be honored to contribute our expertise to your important work. Our team is available to provide more detailed insights, participate in discussions, or offer any other form of assistance that you might find valuable in your regulatory process. Thank you for your consideration. We look forward to the possibility of collaborating with you to develop effective, balanced policies that truly serve the best interests of children in the digital age. ","708742":" Em nome do International Center for Law & Economics (ICLE), escrevo para oferecer nossos conhecimentos e percepções sobre a proteção de dados pessoais de crianças e segurança on-line, especialmente no contexto de sua atual Solicitação de Subsídios sobre esse tópico crucial. O ICLE é um centro de pesquisa apartidário e sem fins lucrativos que tem estudado e contribuído amplamente para discussões sobre segurança on-line, legislação sobre privacidade e regulamentação de plataformas, com foco especial no equilíbrio entre a proteção de grupos vulneráveis, como crianças, e a preservação da liberdade de expressão e do acesso à informação. Nosso trabalho é baseado em uma análise econômica rigorosa e em um profundo entendimento das estruturas jurídicas que regem os espaços digitais, incluindo princípios semelhantes aos descritos no Artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos (ICCPR) das Nações Unidas. Acreditamos que nossa experiência é especialmente relevante para seus esforços, dada a complexa interação entre a segurança das crianças, a proteção de dados e os benefícios sociais mais amplos do acesso aberto à Internet. Nossas pesquisas e recomendações de políticas enfatizam consistentemente que proteger os interesses das crianças no ambiente on-line não é simplesmente uma questão de aprovar leis rigorosas, mas requer uma abordagem diferenciada que pese cuidadosamente os custos e benefícios da regulamentação. Principais considerações sobre as leis que protegem de forma efetiva os interesses das crianças 1. Equilíbrio entre proteção e acesso: Embora seja fundamental proteger as crianças contra os danos on-line, é igualmente importante garantir que as oportunidades vitais de educação e entretenimento permaneçam acessíveis. Há um certo nível de acesso on-line que é amplamente reconhecido como benéfico para o desenvolvimento e a educação das crianças. Os regulamentos devem ser elaborados com cuidado para evitar a limitação inadvertida dessas experiências positivas. 2.

Consequências não intencionais das regulamentações: Políticas excessivamente restritivas podem ter um efeito inibidor nas plataformas digitais. Em uma tentativa de minimizar a exposição legal, as plataformas podem optar por remover completamente as crianças de seus serviços. Essa abordagem, embora pareça protetora, pode acabar privando as crianças de valiosos recursos e experiências on-line. 3. Realidades econômicas da operação da plataforma: É importante reconhecer que a maioria das plataformas digitais não obtém receita direta significativa de crianças, pois esse grupo demográfico normalmente não tem poder de compra independente. Essa realidade econômica significa que regulamentações onerosas específicas para crianças podem incentivar as plataformas a excluir totalmente as crianças em vez de navegar por requisitos de conformidade mais complexos. 4.

Responsabilidade do intermediário e suas implicações: Nosso trabalho, especialmente

conforme descrito em nosso documento "Who Moderates the Moderators?" (Quem modera os moderadores?), investiga o delicado equilíbrio necessário na regulamentação de plataformas. A imposição de uma responsabilidade excessiva aos intermediários pelo conteúdo gerado pelo usuário pode levar à censura excessiva e à redução da inovação, limitando potencialmente o desenvolvimento de espaços on-line adequados às crianças. 5.

Análise de custo-benefício na regulamentação: Defendemos enfaticamente uma análise completa de custo-benefício de qualquer regulamentação proposta. Essa abordagem ajuda a garantir que as medidas de proteção implementadas não causem, inadvertidamente, mais danos do que benefícios, restringindo o acesso das crianças a recursos e experiências on-line benéficos. ","708745":"Nosso trabalho e recursos relevantes Para fornecer mais contexto e profundidade a essas considerações, convidamos você a explorar nosso extenso conjunto de trabalhos sobre esses tópicos. Os recursos a seguir oferecem análises e recomendações detalhadas que podem ser valiosas para seus esforços regulatórios: 1.

TL;DR: Legislação sobre segurança e privacidade on-line para crianças https://laweconcenter.org/resources/childrens-online-safety-and-privacy-legislation/ 2. Uma abordagem jurídica e econômica da regulamentação da mídia social https://laweconcenter.org/resources/a-law-economics-approach-to-social-media-regulation/ 3.

Uma análise coaseana dos regimes de verificação de idade on-line e de consentimento dos paishttps://laweconcenter.org/resources/a-coasean-analysis-of-online-age-verification-and-parental-consent-regimes/ 4. Quem modera os moderadores? Uma abordagem jurídica e econômica para responsabilizar as plataformas on-line sem destruir a Internet https://laweconcenter.org/resources/who-moderates-the-moderators-a-law-economics-approach-to-holding-online-platforms-accountable-without-destroying-the-internet/ 5.

Comentários da ICLE à FTC sobre a regra de proteção da privacidade on-line de crianças NPRMhttps://laweconcenter.org/resources/icle-comments-to-ftc-on-childrens-online-privacy-protection-rule-nprm/ 6. ICLE Amicus para o 9º Circuito em NetChoice v. Bonta https://laweconcenter.org/resources/icle-amicus-to-the-9th-circuit-in-netchoice-v-bonta/ Esses recursos oferecem análises aprofundadas de vários aspectos da proteção infantil on-line, regulamentação de plataformas e implicações econômicas de diferentes abordagens de políticas. Elas refletem nosso compromisso com a elaboração de políticas baseadas em evidências e nossa experiência em navegar no complexo cenário da regulamentação digital. Conclusão Acreditamos que a proteção eficaz dos interesses das crianças on-line requer uma abordagem multifacetada que vá além de simples proibições ou restrições. Isso exige um equilíbrio cuidadoso entre a proteção das crianças e a preservação dos imensos benefícios educacionais e sociais que a Internet pode oferecer. Ficaríamos honrados em contribuir com nossa experiência para seu importante trabalho. Nossa equipe está disponível para fornecer ideias mais detalhadas, participar de discussões ou oferecer qualquer outra forma de assistência que possa ser útil em seu processo regulatório. Obrigado por sua consideração. Aguardamos ansiosamente a possibilidade de colaborar com você para desenvolver políticas eficazes e equilibradas que realmente atendam aos melhores interesses das crianças na era digital. ","705539":"Kristian Stout Director of Innovation Policy International Center for Law & Economics ","708762":".","708764":".","708768":".","708772":".","708775":".

Contribuinte: Kristian Stout

Número: OP-730848

Data: 16/07/2024 - 14:37

Resumo: :"Identificamos duas questões nas quais a atuação orientativa da Autoridade se mostra relevante: (a) como exercitar o legítimo interesse atrelado à contextos que dizem respeito ao melhor interesse da criança; e (b) apresentação de diretrizes para mitigação de riscos e sopesamento de interesses dos menores. a) Legítimo interesse e melhor interesse da criança e do adolescente: Entendemos ser necessário obter da ANPD parâmetros mais claros sobre como exercitar o legítimo interesse atrelado à contextos que dizem respeito ao melhor interesse da criança, por meio de novos exemplos mais complexos, visando superar interpretações contraditórias. O direcionamento pela Autoridade auxiliará a mensurar corretamente e reconhecer o que pode ser flexibilizado quando em conflito de determinados outros interesses, e ainda assim continuar protegendo os menores que dele dependem. Nesse aspecto, sugerimos que a Autoridade leve em consideração a razão de ser do legítimo interesse e a sua complementariedade com o melhor interesse da criança, de forma a não propor parâmetros que sejam excessivamente onerosos ao controlador, tornando inviável a aplicação da base legal nesse contexto. Por exemplo, entendemos que exigir um teste de balanceamento específico para respaldar os direitos da criança caracterizaria uma onerosidade excessiva e desnecessária aos controladores, além de ser uma medida não necessariamente eficiente no resguardo do princípio do melhor interesse.b)Orientação para mitigação de riscos inerentes a atividades de tratamento, inclusive quando necessários para buscar o melhor interesse do menorÉ relevante que a ANPD apresente critérios para o sopesamento de riscos identificados em casos de tratamentos que se mostram necessários (por exemplo, para execução de um contrato, ou ainda cumprimento de uma obrigação legal à qual o controlador esteja sujeito) e riscos inerentes da atividade que não conseguirão ser afastados em prol do melhor interesse do menor.Como exemplo, cita-se eventual tratamento de dados biométricos como mecanismo para prevenção à fraude em aplicações, partindo do pressuposto que já tenha sido avaliado sua proporcionalidade. Nesse caso, ao fazer o sopesamento de interesses, é possível enxergar que a proteção à segurança e à identidade da criança está em linha com o resguardo de seu melhor interesse. Contudo, há riscos inerentes ao tratamento de dados biométricos de crianças, por exemplo em relação às suas mudanças enquanto indivíduo em desenvolvimento e a fragilização da acuraria a longo prazo. Assim, questiona-se o que a ANPD poderia orientar os agentes de tratamento em relação aos riscos residuais inerentes à atividade. Orientações neste sentido são necessárias pois o tratamento de dados pessoais de crianças por diversas vezes é imprescindível e detém papel relevante nas atividades de tratamento de um controlador. Assim, ao invés de vedar essa utilização ou inserir restrições excessivas, a contribuição maior da ANPD é no sentido de indicar caminhos e fornecer insumos sobre como viabilizar esse tipo de operação.","708725":"Consideramos que as seguintes situações demandam maior detalhamento orientativo pela ANPD acerca do princípio do melhor interesse: (a) indicativos do melhor interesse a serem avaliados pelos controladores; (b) cenários que demonstrem e comparem a observância e a violação ao melhor interesse; e (c) flexibilização ou presunção de melhor interesse em contextos

determinados. a) Orientação sobre indicativos para cumprimento do princípio do melhor interesse Da perspectiva do princípio de responsabilização e prestação de contas, é relevante que o controlador possua orientações sobre como documentar e gerar evidências sobre o cumprimento do princípio do melhor interesse da criança e do adolescente. Assim, a Autoridade poderá fornecer indicativos práticos, exemplificativos e não taxativos sobre seu entendimento acerca dos aspectos englobados pelo princípio do melhor interesse da criança, inclusive considerando o ambiente digital. A título de exemplo, a ANPD poderá demonstrar quais elementos poderão ser contemplados em uma avaliação sobre o melhor interesse, como: a opinião da criança; qual(is) direito(s) são promovidos, resguardados ou ao menos não impactados; adoção de meios menos intrusivos; entre outros, ponderados conforme caso concreto. De toda forma, em que pese seja necessária a orientação sobre indicativos para avaliar e documentar o melhor interesse, não entendemos ser uma medida razoável a exigência de um novo documento não previsto em lei para este fim, como testes de balanceamento específicos que onerem os controladores. Porém, a ANPD poderá indicar sobre o cabimento de incluir tal evidência em instrumentos já existentes como registro de atividades de tratamento ou relatório de impacto à proteção de dados, bem como quais elementos espera que sejam registrados.b)Orientação sobre situações de observância ou violação ao princípio do melhor interesse.Reforçamos a importância de apresentar vários exemplos de situações detalhadas sobre tratamentos de dados envolvendo o melhor interesse e que afetem a liberdade fundamental do menor enquanto ser em desenvolvimento. A partir de exemplos concretos, abordando tanto situações simples quanto casos mais complexos, se torna mais factível para os controladores entenderem tanto situações em que o melhor interesse é atendido, quanto os limites para que seja interpretado pela ANPD como uma violação ao princípio. c)Flexibilização ou presunção de melhor interesse É relevante que a ANPD se posicione quanto à necessidade de comprovação do melhor interesse da criança por determinados agentes específicos ou situações inerentemente vinculadas à promoção do melhor interesse. É o caso, por exemplo, de entidades e ONGs voltadas especificamente para os direitos das crianças, como instituições de assistência social, centros de adoção, entre outros. Nessas circunstâncias, especialmente quando a missão institucional estiver atrelada a aspectos de promoção de interesses de crianças e adolescentes, é relevante questionar até que ponto é razoável e proporcional onerar o agente de tratamento na demonstração do melhor interesse. Seria relevante a ANPD considerasse eventual legitimidade presumida que permitisse uma flexibilização aos agentes de tratamento para as obrigações relativas às demonstrações de cumprimento ao princípio do melhor interesse.","705523":"Preliminarmente, entendemos que a ANPD deve evitar a adição de critérios exaustivos para a validade do consentimento, além do que a LGPD já apresenta, para não tornar sua aplicação prática algo de difícil operacionalização. Para tanto, poderá observar diretrizes que também se apliquem para especificidades exigidas ao consentimento para tratamento de dados pessoais sensíveis, sem causar ônus adicionais aos controladores. a) Parâmetros acerca do consentimento “específico” • Consentimento para finalidades determinadas A LGPD (artigo 8º, § 4º) determina que as autorizações genéricas para o tratamento de dados pessoais serão nulas e que o consentimento deverá referir-se a finalidades determinadas. Assim, a ANPD poderá guiar-se por esta disposição, considerando

a especificidade vinculada a finalidades determinadas. • Consentimento específico como oposição ao consentimento genérico A ANPD poderá fornecer aos controladores exemplos de situações que configurariam o consentimento genérico e, portanto, inválido. Assim, os controladores identificariam os elementos que tornam o consentimento inválido para garantir que nenhum desses elementos é preenchido em suas atividades.b) Parâmetros acerca do consentimento “em destaque” • Facilidade de identificação do consentimento Um dos objetivos do consentimento “em destaque” é assegurar que seja identificado facilmente, conforme avaliação contextual e o meio de obtenção deste consentimento. Assim a Autoridade poderá orientar sobre práticas de destaque, com exemplos de aplicações proporcionais ao caso concreto e contextual. Exemplos contextuais: a criação de uma seção específica para “consentimento para o tratamento de dados de criança” poderá ser razoável em meio a um documento extenso que tenha um sumário facilitado e em camadas, mas poderá ser desproporcional para um formulário simplificado. Ainda, há casos em que recursos visuais poderão ser efetivos, ou ainda pop-ups em aplicativos e plataformas poderão ser utilizados. • Ausência de técnicas enganosas ou obscuras A ANPD poderá ilustrar seu entendimento sobre consentimentos mascarados, escondidos ou ofuscados, por exemplo pelo uso de recursos obscuros que desviem a atenção do pai ou responsável, como práticas que tornam o consentimento inválido.","708742":"Primeiramente, destacamos que as medidas e mecanismos encontrados como boas práticas de mercado e entre as orientações de reguladores internacionais são sempre acompanhadas de uma perspectiva de proporcionalidade e razoabilidade, a depender do risco do tratamento de dados pessoais para o qual o consentimento é solicitado. O Federal Trade Commission dos Estados Unidos, em material intitulado “A guide for businness and parentes and small entity compliance guide”, traz uma lista não exaustiva de exemplos interessantes que podem servir como boas diretrizes para a ANPD ao estipular maneiras de validar o consentimento fornecido pelos responsáveis no ambiente digital, a serem avaliadas de acordo com o contexto do tratamento: • Exigir que o pai, em conexão com uma transação monetária, use um cartão de crédito, cartão de débito ou outro sistema de pagamento on-line que forneça notificação de cada transação discreta ao titular da conta principal; • Exigir que os pais liguem para um número de telefone gratuito, ou se conecte via videoconferência, com pessoal treinado para identificar a relação deste adulto com a criança; • Verificar a identidade de um dos pais por meio de um formulário de identificação emitido pelo governo a partir de bancos de dados com tais informações; • Exigir que um dos pais responda a uma série de perguntas de desafio baseadas em conhecimentos que seriam difíceis de responder a alguém que não o progenitor; • Verificar a identidade do adulto a partir da comparação entre a foto de algum documento de identificação enviado pelo responsável com uma segunda foto enviada por este mesmo responsável, usando tecnologia de reconhecimento facial; Cada medida deverá ser avaliada conforme o risco do tratamento, para não configurar um tratamento excessivo, bem como de uma perspectiva de custos e tecnologias disponíveis à época. Em conclusão, a verificação do consentimento parental no ambiente digital exige uma abordagem multifacetada, sendo necessário garantir o equilíbrio entre a adequação e proporcionalidade das medidas adotadas, minimizando os riscos e maximizando a proteção dos direitos das crianças, sem onerar excessivamente os controladores.","708745":"Exigir um consentimento assistido ou a representação dos

representantes legais de um adolescente a cada coleta desta autorização para tratamento de dados pessoais seria uma medida que, em muitos casos, poderia contrariar o melhor interesse do menor e representar um ônus excessivo aos controladores. Assim, o caminho a ser adotado é coerente com o conceito de autonomia progressiva dos adolescentes. Já temos exemplos na legislação pátria de que a capacidade civil não é absoluta, com exceções no código civil e em esferas onde a manifestação de vontade autônoma de adolescente é fomentada – como o direito ao voto facultativo aos 16 anos. Considerando que a capacidade de discernimento varia entre adolescentes de 12 e 17 anos, a depender do contexto, é relevante buscar da ANPD quais elementos os controladores deverão observar para avaliar este discernimento em sua realidade, viabilizando mecanismos de consentimento "autônomo", ou assistido, caso necessário. Entendemos necessário obter da ANPD um posicionamento que considere no conceito de autonomia progressiva elementos contextuais, como: tipo de serviço a ser contratado, riscos do tratamento, efeitos do consentimento solicitado, e o discernimento e a opinião do adolescente. Ainda, é relevante que a ANPD aborde as consequências do consentimento – ou revogação deste - pelo adolescente em relação a eventual consentimento parental prévio.","705539":"Identificamos os seguintes parâmetros principais: (a) minimização de dados; e (b) privacidade desde a concepção. a)Minimização de dadosA autoridade britânica ICO no Children's Code - Age Appropriate Design: a code of practice for online service discorre sobre a minimização e a coleta mínima, que devem estar atrelados à finalidade específica do serviço online prestado, de modo se sejam coletados apenas os dados essenciais. Por exemplo, durante a criação de contas dos menores para jogos online, seria razoável coletar dados como nome de usuário e senha, mas devem ser evitadas informações como nome completo, endereço ou dados escolares. Ainda, a coleta de dados de localização de menores deve ser limitada a situações estritamente necessárias para o funcionamento do serviço, assim como cookies ou quaisquer outras tecnologias de rastreamento que coletam dados pessoais desnecessários. Por exemplo: uma ferramenta de controle parental que disponibilize funções de segurança para que pais localizem onde está o celular da criança e saibam onde ela está representaria uma situação em que a coleta de dados de localização é aceita; já a coleta deste mesmo dado para desbloquear customização de recursos de jogos (como "skins" de personagens), excederia a necessidade. Neste material, o ICO ainda orienta que a coleta de dados pessoais ocorra apenas quando o menor estiver usando ativamente e conscientemente aquele elemento do serviço. Deve, também, ser ressaltado para os controladores a importância de revisar regularmente a necessidade de armazenamento de dados e excluir qualquer informação desnecessária, minimizando a retenção de dados pessoais, para além da coleta. Por fim, a autoridade britânica também sugere a desidentificação de dados pessoais de menores antes de utilizações para fins secundários, como pesquisa e desenvolvimento de produtos. b) Privacidade desde a concepção Quanto a medidas de design a serem levadas em conta durante o desenvolvimento de ferramentas, como em plataformas de jogos online, indicamos as diretrizes previstas pela autoridade norueguesa de proteção de dados pessoais no guia "Datatilsynet Principles on Children & Online Gaming": • As configurações que interferem na privacidade e na proteção de dados das crianças sejam desabilitadas por padrão. Isso inclui evitar o rastreamento de localização geográfica, acesso a contatos, gravação de voz, sincronização com mídias sociais,

a menos que sejam fundamentalmente necessários para o funcionamento do jogo; • A natureza dos jogos online pode levar à coleta de uma grande quantidade de dados pessoais sobre as crianças. No entanto, sugere-se que as plataformas devem evitar a coleta automática e análise de dados para fins como a criação de perfis de jogadores, a derivação de dados sobre a personalidade da criança ou suas habilidades cognitivas. • Por fim, no lugar de coletar dados detalhados sobre as crianças, plataformas devem oferecer opções de personalização que permitam que as crianças escolham o gênero de jogo, o nível de dificuldade, sem a necessidade de coletar dados adicionais.","708762":"Com base no ICO no Children's Code - Age Appropriate Design: a code of practice for online service e em práticas de mercado, indicamos as seguintes técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais: • Autodeclaração com mecanismos de dissuasão: permitir que o usuário declare sua idade, mas utiliza mecanismos de dissuasão, como questionários sobre cultura popular ou eventos recentes, para desencorajar declarações falsas. • Provas de idade digitais: como carteiras de identidade digitais para verificar a idade do usuário. • Verificação de idade por proxy: solicitar a confirmação de idade por um adulto responsável, como um pai ou responsável legal. Esse método pode ser eficaz para crianças mais novas, mas exige mecanismos seguros para garantir a identidade do adulto e o consentimento informado. É relevante que a ANPD forneça exemplos de situações práticas sobre verificação de idade, especialmente de cenários em que a verificação de idade provavelmente não será necessária. Por exemplo: quando os produtos e serviços já tenham sido concebidos com a implementação de mecanismos de design específicos para atender ao público de crianças e adolescentes; quando o produto ou serviço requerer a identificação de um usuário único pelo qual já se tenha atribuído sua idade (como serviços de banco ou de plano de saúde). A verificação de idade implicará em um tratamento de dados pessoais – para o qual já se reconhece uma finalidade legítima. Assim, o tratamento relativo à verificação de idade não deverá implicar em usos secundários, sendo recomendável a exclusão dos dados coletados durante este processo assim que o nível adequado de confiança quanto à idade do usuário for atingido. Sobretudo, neste momento de verificação, independentemente do método escolhido, é importante reforçar a necessidade de ser transparente com o usuário sobre como sua idade está sendo verificada.","708764":"O art. 14, § 4º da LGPD prevê que controladores não deverão condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Nesse sentido, entendemos que a ANPD deve ter cuidado especial ao abordar a questão de formação de perfis comportamentais. Esse tem sido um tema bastante discutido internacionalmente e, dada a sensibilidade das informações que engloba, merece atenção especial da Autoridade. O objetivo não é que a ANPD determine uma proibição quanto à formação de perfis comportamentais, mas oriente os controladores sobre em que circunstâncias consistiria em um risco a esta categoria, desafiando inclusive o princípio do melhor interesse. Assim, o balizamento para determinar as orientações sobre o tema não precisam fugir do que já se debate acerca do tema de melhor interesse, mas acomodar exemplos claros envolvendo casos de perfilização.","708768":"É pertinente que a ANPD leve em conta as diferentes idades desses jovens e sua autonomia progressiva. As recomendações de métodos abaixo leva em consideração as faixas etárias definidas pelo ICO no "Children's

Code - Annex B: Age and developmental stages” acerca do desenvolvimento cognitivo em cada etapa: Para crianças mais novas, em idade pré-escolar e primeiro ciclo do ensino fundamental, sugerimos: • Restrição de conteúdo: bloquear o acesso a conteúdo impróprio, como violência, pornografia e linguagem inapropriada. • Limitação de tempo de tela: definir limites de tempo para o uso de dispositivos, incentivando atividades offline e interação social. •Bloqueio de compras: impedir compras acidentais ou não autorizadas dentro de aplicativos e jogos. Já para crianças mais velhas, no segundo ciclo do ensino fundamental e adolescentes, sugerimos: •Gerenciamento de redes sociais: supervisionar o uso de redes sociais, orientando sobre privacidade, cyberbullying e contato com estranhos. •Controle de localização: permitir o compartilhamento de localização apenas com contatos confiáveis e em situações específicas. •Monitoramento de atividades: acompanhar o histórico de navegação, downloads e interações online, sempre com diálogo e respeito à privacidade. Embora a ANPD busque mecanismos para ampliar o controle parental, é relevante considerar que implementação efetiva dos controles varia de acordo com a dinâmica familiar e o discernimento da criança, bem como o tipo de tratamento de dados e os riscos atrelados. Com base em diretrizes do ICO no “Children’s Code - 11. Parental controls”, o diálogo aberto e constante, a construção de uma relação de confiança e o acompanhamento atento às necessidades de cada criança são fundamentais para garantir uma experiência online segura e positiva. A orientação às crianças e adolescente deve ser transparente, informando que controles parentais estão em vigor, de forma contextualizada e quais são limites de como podem exercer controle sobre seus dados. Nesse sentido, as informações a serem fornecidas e formatos adequados poderão variar conforme faixa etária em relação ao desenvolvimento cognitivo de crianças e adolescente, conforme os seguintes exemplos pelo do ICO no Children’s Code - 11. Parental controls: para crianças em idade pré-escolar até primeiro ciclo do ensino fundamental, pode ser adequado o fornecimento de materiais de áudio ou vídeo para a criança explicar que seus pais estão sendo informados sobre o que ela faz on-line para ajudar a mantê-la segura; já para adolescentes até estágios próximos da fase adulta é razoável fornecer materiais escritos descrevendo como seu serviço funciona e o equilíbrio entre os direitos de privacidade dos pais e do adolescente. Por fim, a efetividade de uma experiência online segura e positiva nos ambientes digitais não se esgota apenas na atuação de controladores de dados, sendo uma tarefa compartilhada com os pais e responsáveis. Assim, a ANPD poderá contribuir com orientações destinadas aos pais e responsáveis abordando, por exemplo, os seguintes aspectos: •Diálogo e confiança: Priorizar a conversa sobre os riscos online, incentivando a responsabilidade e o uso consciente da tecnologia. •Acordos familiares: Estabelecer regras claras em conjunto sobre o uso de internet, mídias sociais e jogos, definindo limites e consequências. •Ferramentas de segurança: Orientar sobre o uso de senhas fortes, softwares de segurança e como identificar e evitar golpes online.","708772":"Considerando o artigo 14 § 6º da LGPD, o pilar da qualquer comunicação com crianças e adolescentes deve ser a transparência clara, acessível e compreensível, considerando as particularidades deste público-alvo. Assim, entendemos que a ANPD poderá promover orientações não exaustivas que explorem o atendimento ou não dessa adequação de linguagem, para que controladores possam aplicá-las conforme sua própria realidade. Assim, os controladores devem garantir que o vocabulário, tom e estilo da linguagem usada para transmitir as informações sobre o

tratamento de dados pessoais sejam apropriados e ressoem com as crianças para que reconheçam que a mensagem está sendo direcionada a ela. Nesse sentido, entendemos que podem ser métodos eficientes para o fornecimento de informações de maneira simples, clara e acessível quanto ao tratamento de dados pessoais de crianças e adolescentes: Uso de métodos não textuais, como desenhos animados, vídeos, imagens, ícones ou gamificação, para transmitir informações sobre proteção de dados de forma mais eficaz. Esses métodos são mais propensos a ressoar com as crianças do que blocos de texto. • Uso de formatos que sejam mais aplicáveis e relevantes ao serviço que oferecem. Por exemplo, se operam uma plataforma de compartilhamento de vídeos, os vídeos provavelmente são um meio mais apropriado para transmitir informações de transparência para crianças do que uma imagem ou um texto. • Apresentação de informações de forma atraente, por exemplo, usando tamanhos de fonte grandes, listas de marcadores fáceis de ler, cores. Considerar apresentar trechos breves, de modo a facilitar a compreensão. • Disponibilizar as informações essenciais sobre proteção de dados no início e incentivar as crianças ativamente pelos controladores a descobrir mais sobre como seus próprios dados pessoais serão usados e como esse uso as afetará, por exemplo, por meio de botões clicáveis. • Uso notificações oportunas e contextuais ao longo das interações para informar crianças e jovens sobre o tratamento de dados pessoais. Exemplos de momentos oportunos incluem: antes de postar ou compartilhar algo online, antes de alterar as configurações de privacidade padrão. • Fornecer explicações às crianças sobre o motivo pelo qual determinadas configurações são automaticamente desativadas ou negadas a elas por padrão. Caixas de aviso devem ser exibidas se as crianças usuárias tentarem ativar essas configurações e informações fornecidas explicando por que determinadas configurações de controle de usuário se aplicam a elas. • Incentivo, por meio de pop-ups ou prompts, por exemplo, a que crianças perguntem aos pais/adultos de confiança se tiverem alguma dúvida sobre as informações de transparência que receberam.","708775":"Destacamos dois temas principais: (a) direitos dos titulares; e (b) tratamento de dados de geolocalização. a)Direitos dos titulares É relevante que a ANPD considere direcionar orientações no que tange ao exercício de direitos de crianças e adolescentes enquanto titulares detentores destes direitos. É razoável que determinados direitos possam ser exercidos livremente por menores (como confirmação de tratamento, solicitação de informações sobre entidades com as quais houver compartilhamento etc.), e que pais e responsáveis desempenhem seu controle apenas para gestão ou acompanhamento. Já para exercício de direitos que possam gerar consequências aos menores, pais e responsáveis poderiam ser aproximados para ratificar ou intervir nas requisições, como em requisições para correção ou eliminação de dados. Nesse sentido, para que o controlador verifique se no caso concreto a criança pode entender seus direitos e suas implicações, deve-se levar em conta: o nível de maturidade da criança para tomar decisões como essa; a natureza dos dados pessoais; se há ordens judiciais relacionadas ao acesso ou responsabilidade dos pais; se há dever de sigilo devido ao menor; as consequências de permitir acesso aos responsáveis para exercer os direitos da criança – se houver alegações de abuso ou maus-tratos; qualquer prejuízo para a criança ou o adolescente se os responsáveis não puderem acessar os dados; e a opinião do menor sobre se seus pais devem ter acesso às informações sobre eles. Assim, é relevante que a ANPD suscite este tema a fim de orientar

controladores de que precisarão se preparar para um cenário mutável e viabilizar meios para recebimento e atendimento de requisições neste contexto. b) Tratamento de dados de geolocalização Por ser um tipo de dado particularmente crítico, já que pode colocar a segurança física da criança em risco, seria relevante que a Autoridade estabelecesse maiores diretrizes sobre como os controladores devem se portar frente a este tratamento e como garantir que ele está acontecendo da melhor forma. Caso a geolocalização seja imprescindível para o fornecimento do serviço, sugerimos como salvaguarda a coleta da localização aproximada dos usuários em vez da localização exata, reduzindo o risco de uso indevido dos dados, além da recomendação de que o controlador fornecer controles visíveis para permitir que a criança interrompa o fornecimento da geolocalização a qualquer momento ou após cada sessão, após um curto período ou quando o evento ou recurso que exige localização for concluído.

Contribuinte: Patrícia Carneiro Rodrigues PEREZ

Número: OP-731027

Data: 16/07/2024 - 15:56

Resumo: :"Podemos citar algumas questões como: a) Definição de critérios Objetivos para Avaliação do Melhor Interesse, ou seja, critérios objetivos que as empresas e organizações devem seguir para determinar o melhor interesse dos titulares dos dados; b) Diretrizes sobre como as organizações devem equilibrar os interesses comerciais e operacionais com os direitos fundamentais dos titulares dos dados, assegurando que o legítimo interesse não se sobreponha aos direitos dos titulares; c) Normas específicas para a proteção de dados sensíveis e de grupos vulneráveis, como crianças, adolescentes, idosos e pessoas com deficiência; d) Requisitos detalhados sobre a realização de Avaliações de Legítimo Interesse / Teste de Balanceamento (LIA) quando o tratamento de dados se baseia no legítimo interesse; e) Desenvolvimento de políticas públicas que buscam assegurar que as decisões sejam tomadas com foco no bem-estar dos indivíduos vulneráveis (crianças e adolescentes); e, f) Determinação de sanções específicas aos controladores que coletam dados de crianças e adolescentes sem consentimento dado por pelo menos um dos pais ou pelo responsável legal e sem respeitar esse melhor interesse.","708725":" Sim, devido à vulnerabilidade desses grupos e à importância de proteger seus direitos e interesses. Podemos citar como algumas situações como as seguintes: a) Regras específicas para proteger crianças e adolescentes contra práticas abusivas de publicidade e marketing; b) Diretrizes sobre o tratamento de dados em contextos educacionais, incluindo plataformas de aprendizagem online e aplicativos educacionais; c) Plataformas digitais que demandam regulamentação específica para o uso, por exemplo, de redes sociais por crianças e adolescentes, com foco na proteção contra cyberbullying, exposição a conteúdo inadequado e coleta excessiva de dados; d) Normas para o tratamento de dados em jogos online e aplicativos de entretenimento.

Além destes podemos destacar outros contextos que merecem cuidados específicos, tais como, saúde e bem estar; envolvimento em pesquisas; uso de tecnologias emergentes; demandas judiciais onde há menores envolvidos; e, transações bancárias, utilização de contas,

em especial as “contas adolescentes” que hoje já possuem uma maior adesão. Tudo isso deve ser tratado com transparência através de campanhas educativas para informar crianças, adolescentes e seus pais ou responsáveis sobre a importância da proteção de dados pessoais e os direitos associados.","705523":"Clareza e Compreensibilidade; Especificidade; Destaque; Informações completas; Facilidade de acesso e retirada; Registro do consentimento; Revisão do consentimento de forma periódica; e, Adequação ao contexto digital e/ou off-line; e, Mecanismos de segurança dos dados.","708742":"Solicitar a apresentação de documentos que comprovem a identidade e a relação do responsável com a criança (ex.: RG, CPF, certidão de nascimento); Utilizar serviços de verificação de identidade online que possam confirmar a autenticidade das informações fornecidas; Processo de Consentimento em Duas Etapas; Implementar assinaturas digitais ou eletrônicas avançadas para garantir que o consentimento seja formalizado e legalmente vinculativo; Integrar mecanismos de controle / consentimento parental que permitam aos pais ou responsáveis gerenciar as permissões de coleta e uso de dados diretamente através de painéis de controle dedicados; Manter registros detalhados e seguros de todos os consentimentos obtidos, incluindo data, hora, informações do responsável e finalidades do consentimento; e, Garantir que esses registros sejam auditáveis e acessíveis quando necessário para fins de conformidade. Importante destacar que se faz de suma importância a presente regulamentação sobre o tema, não somente através de guias orientativos, mas também por meio de regulamentação específica afim de garantir o cumprimento de determinados procedimentos por parte dos controladores, em especial quando a coleta de dados de vulneráveis são inerentes às atividades prestadas por estes controladores. ","708745":" De acordo com o Código Civil são absolutamente incapazes de exercer pessoalmente os atos da vida civil os menores de 16 anos e, relativamente incapazes os maiores de 16 e menores de 18 anos (arts. 3º e 4º do CC), sendo assim, entende-se por oportuno seguirmos essas diretrizes a fim de mantermos uma congruência dentro do ordenamento jurídico, inclusive considerando que, ao adotarmos uma posição de autonomia progressiva, antes de atingida a maioridade, poderemos expor os adolescentes em uma posição de maior vulnerabilidade, uma vez que para tanto haveria a necessidade de termos implementadas medidas rigorosas de proteção e transparência para assegurar que os direitos e interesses dos adolescentes sejam preservados, uma vez que o menor não possui capacidade civil para expressar consentimento sem que o responsável tenham, previamente, analisado e ponderado os riscos. Ademais, cumpre destacar que dentro do ordenamento jurídico temos a hierárquia das normas, uma teoria que dispõe que as normas jurídicas estão organizadas em uma estrutura hierárquica onde cada norma inferior deve ser consistente e compatível com as normas superiores. Assim sendo, todas as normas inferiores devem observar os direitos fundamentais dispostos na Constituição Federal, norma que consta no topo desta pirâmide.

A hierarquia de normas da pirâmide de Kelsen demonstra a importância da Constituição como norma suprema do ordenamento jurídico, estabelecendo que todas as outras normas devem estar em conformidade com ela. A observância aos direitos fundamentais (vida, liberdade, igualdade, segurança e propriedade) dispostos na Constituição Federal é crucial para a criação e aplicação de regulamentações justas e equitativas, garantindo a proteção dos cidadãos e a manutenção do Estado de Direito. Assim sendo, entende-se que um posicionamento divergente pode ferir preceitos constitucionais e de

normas superiores como é o caso do Código Civil se comparado à regulamentação, a qual deverá estar em consonância à estes preceitos.","705539":"Para assegurar o respeito ao melhor interesse das crianças e adolescentes, promover altos níveis de privacidade e proteção de dados, e mitigar os riscos decorrentes do uso de plataformas digitais, várias medidas e salvaguardas devem ser observadas. Em primeiro lugar, todos os processos e decisões devem priorizar o melhor interesse das crianças e adolescentes, garantindo sua segurança, bem-estar e desenvolvimento. As informações sobre o tratamento de dados devem ser claras, compreensíveis e acessíveis tanto para as crianças e adolescentes quanto para seus pais ou responsáveis. É importante coletar apenas os dados estritamente necessários para as finalidades específicas, evitando a coleta excessiva de dados pessoais. Além disso, medidas de segurança robustas devem ser implementadas para proteger os dados pessoais contra acesso não autorizado, perda, destruição ou qualquer forma de tratamento inadequado. Para obter consentimento, é essencial que ele seja claro, específico e verificável, obtido dos pais ou responsáveis antes de coletar e tratar dados pessoais de crianças e adolescentes. É importante utilizar mecanismos que garantam que o consentimento foi dado por adultos responsáveis, como verificações de identidade.","708762":"Seguem alguns exemplos de boas práticas que podem ser implementadas: A)A autodeclaração, onde o usuário informa sua idade ou data de nascimento, é uma técnica simples, mas pode ser complementada com perguntas de verificação que são difíceis para crianças menores responderem corretamente. Por exemplo, perguntas sobre eventos históricos ou cultura popular que seriam conhecidos principalmente por adultos. B)Upload de documentos: Solicitar documentos oficiais, como carteira de identidade, passaporte ou certidão de nascimento, para verificar a idade. C)A utilização de cartões de crédito para verificar a idade, já que apenas adultos ou adolescentes autorizados possuem cartões. D)Técnicas de reconhecimento facial podem estimar a idade dos usuários com base em suas características faciais. Entretanto, neste aspecto temos que ter um cuidado redobrado, uma vez que este tipo de técnica requer medidas de seguranças mais robustas, por conta de traduzir um dado pessoal sensível, ainda mais se se tratar de um grupo vulnerável. E)E-mail de verificação aos pais ou responsáveis, solicitando a confirmação da idade e o consentimento para o uso da plataforma.","708764":"Algumas limitações que podem ser observadas são: a) Limitação da Finalidade; b) Minimização de Dados; c) Consentimento dos pais ou responsáveis; d) Proibição de coleta oculta; e) Restrição no compartilhamento; e, f) Proibição de perfis e publicidade direcionada.","708768":"Plataformas digitais podem oferecer painéis de controle dedicados onde os pais podem gerenciar as configurações de privacidade e segurança dos perfis de seus filhos; sistemas de alerta que informam os pais sobre as atividades online de seus filhos, incluindo novas permissões solicitadas por aplicativos, mudanças nas configurações de privacidade e tentativas de acessar conteúdo restrito; Implementar processos de verificação de identidade para garantir que o consentimento para coleta de dados seja realmente fornecido por pais ou responsáveis legais; Disponibilizar para os pais um histórico das atividades online dos seus filhos, permitindo que revisem o uso de dados e as interações na plataforma; Criação de uma conta para a criança e o adolescente vinculada à conta do seu responsável; e, Sempre que possível, anonimizar os dados coletados para proteger a identidade das crianças e adolescentes.","708772":"Linguagem simples e clara, evitando o

uso de termos técnicos e utilizar explicações visuais; Design de Interfaces intuitivas (amigáveis com destaque de informações importantes); Transparência das políticas de privacidade (curtas e segmentadas, com o resumo das informações importantes, através do visual law com o uso de tabelas, fluxogramas, linguagem que conversa com o seu público); e, Exemplificação e contextualização, a partir de exemplos práticos e contextos a fim de demonstrar a relevância das práticas de coleta de dados para melhoria do serviço e segurança dos usuários.","708775":"Sim, podemos citar a necessidade de regulamentação do uso de Inteligência Artficial e Algoritmos; Especificação de como deve ser coletado o consentimento parental; Políticas públicas que fomentem a Educação e Conscientização referente ao tratamento de dados de vulneráveis; Formas de permissão para o monitoramento das atividades pelos responsáveis, em especial no que diz respeito à redes sociais; e, o Sharenting que se refere à prática de pais ou responsáveis compartilharem fotos, vídeos e outras informações sobre seus filhos nas redes sociais e outras plataformas online. Lembramos que as questões citadas acima são exemplificativas e não taxativas, uma vez que entendemos a necessidade e importância da ampla regulamentação sobre o tema de maneira detalhada.

Contribuinte: Asshaias Felippe Eugênio

Número: OP-731064

Data: 16/07/2024 - 16:14

Resumo: :"O que é de melhor interesse para cada criança deve ser determinado pelos pais e não ditado por políticos ou empresas privadas. Ao considerar o princípio do melhor interesse, também é importante considerar os desafios da operacionalização em escala e evitar a criação de metas móveis que impeçam a conformidade. A vantagem de um mercado dinâmico é que as empresas online são capazes de adaptar os seus serviços e produtos ao que é mais relevante e útil para o seu público específico. As empresas privadas que operam online não são capazes de fazer avaliações diagnósticas dos usuários de forma coerente ou consistente, incluindo a sua saúde física e mental.","708725":"As crianças têm direito a um nível mais elevado de segurança e privacidade nas suas experiências online. Nossa indústria tem se envolvido ativamente em diversas iniciativas para integrar recursos robustos de design de proteção em seus sites e plataformas. As empresas que representamos lideram esforços para implementar configurações e ferramentas de controle parental para adaptar individualmente a utilização online dos usuários mais jovens aos tipos de conteúdos e serviços mais adequados à sua experiência de vida única e às suas necessidades de desenvolvimento. Alguns exemplos podem ser encontrados aqui: https://ccianet.org/wp-content/uploads/2023/02/General-Child-Safety-Mechanisms_Fact-Sheet.pdf.","705523":"De maneira geral, o consentimento se refere a um ato claro e afirmativo que representa um aceite específico, informado e inequívoco dado livremente pelo consumidor para processar seus dados pessoais. O consentimento pode incluir uma declaração por escrito, inclusive por meio eletrônico, ou qualquer outra ação afirmativa inequívoca, como uma declaração verbal, se estiver usando um dispositivo doméstico inteligente (smart device). O método específico que uma empresa escolhe

implementar para obter o consentimento de um consumidor, incluindo de um dos pais ou guardião, dependerá de uma variedade de considerações: segurança e privacidade, acessibilidade e equidade, e outros riscos como a hesitação do usuário em fornecer determinadas informações pessoais. Mas, em algumas circunstâncias, não há explicação sobre como uma empresa pode verificar a relação entre um jovem utilizador e o adulto que consentiu, especialmente se o pai, mãe ou tutor que consentiu não tiver uma conta na respectiva plataforma. ","708742":"As empresas que fornecem serviços ou produtos digitais direcionados a crianças ou usuários mais jovens utilizam vários métodos para obter o consentimento dos pais ou responsáveis ¿¿antes de coletar as informações pessoais da criança. Seja um website ou uma aplicação de jogo móvel, essas organizações devem utilizar um método que seja razoavelmente concebido à luz da tecnologia disponível para garantir que a pessoa que dá o consentimento é o responsável da criança. O processo de identificação pode consistir em: ligação telefônica para um número gratuito ou videoconferência ao vivo; fornecimento de identidade emitida pelo governo para verificação em um banco de dados; processamento de um cartão de crédito ou débito para avisar o usuário adulto; ou o fornecimento de um conjunto de perguntas baseadas em conhecimentos específicos. À medida que a tecnologia continua a avançar, o mesmo acontece com os métodos escolhidos por uma empresa. Este padrão flexível fornece às empresas orientação suficiente para continuarem a desenvolver e melhorar os seus serviços. No entanto, ainda existem desafios de implementação. Por exemplo, muitos pais e responsáveis ¿¿legais não compartilham o mesmo sobrenome de seus filhos devido a um novo matrimônio, adoção ou outras decisões culturais ou familiares – inclusive no Brasil, onde é comum ter vários sobrenomes. Além disso, alguns familiares podem não ser proficientes em outras línguas além do português, não têm conhecimentos tecnológicos ou têm vários empregos. Isto levanta sérias preocupações sobre equidade, especialmente tendo em conta os familiares que não possuem a identificação governamental necessária ou outros mecanismos para acessar um serviço ou plataforma online – impedindo os adolescentes de ter acesso a serviços úteis e informações adequadas à sua idade. ","708745":"Devido às diferentes formas como as crianças e os adolescentes utilizam a Internet, é imperativo adaptar adequadamente esses tratamentos às respectivas faixas etárias. Assim, determinar o que constitui um esforço razoável para obter consentimento é ainda mais desafiador para conteúdos não infantis. Por exemplo, se um jovem de 16 anos estiver realizando uma pesquisa para um projeto escolar, espera-se que ele encontre, aprenda e consiga discernir uma variedade maior de materiais do que uma criança de 7 anos na Internet jogando videogames. Isto também permitiria que aqueles com mais de 13 anos, que utilizam a Internet de forma muito diferente dos seus pares mais jovens, continuassem a se beneficiar dos seus recursos. Em última análise, o jovem de 16 anos que está pesquisando, por exemplo, esforços de preservação da floresta tropical também acessa e usa a mesma enciclopédia, blog ou canal de vídeo on-line que adultos com interesses de pesquisa semelhantes. Qualquer requisito de consentimento dos pais que condicione o acesso a tais materiais online deve ter em conta as suas necessidades e interesses específicos, incluindo a capacidade dos adolescentes fornecerem o seu próprio consentimento na utilização destas ferramentas e serviços digitais importantes e benéficos. ","705539":"Qualquer abordagem à segurança e privacidade online dos jovens deve

reconhecer e ter em conta as diferenças inerentes entre as plataformas e os serviços online. Embora os líderes políticos esperem que surja uma solução abrangente para resolver todos os riscos associados aos serviços e plataformas online, não existe uma solução universal para manter os jovens usuários seguros em todo o diversificado ecossistema da Internet. Ao invés de um padrão de “melhor interesse”, qualquer potencial diretiva para a segurança online dos jovens precisa de ter uma abordagem baseada no risco que permita às organizações tomar as medidas necessárias à luz dos progressivos riscos e perigos mais relevantes específicos ao seu ambiente e usuários. Caso contrário, uma abordagem de melhor interesse forneceria pouca orientação e clareza de conformidade às organizações, dando azo a considerações subjetivas e vagas. Pessoas em geral, especialmente as crianças, têm opiniões muito diferenciadas sobre o que pode ser prejudicial para elas. As diversas experiências vividas por crianças, adolescentes e adultos variam significativamente, deixando as empresas sem um roteiro abrangente para navegar pela perspectiva única de cada usuário. Determinar as soluções ideais para o bem-estar de cada jovem envolvido numa plataforma online representa um sério desafio de viabilidade. ","708762":"Embora estejam disponíveis vários métodos para se garantir a idade de alguém, como a verificação da idade e a obtenção do consentimento dos pais, cada abordagem apresenta o seu próprio conjunto de desafios e pontos positivos e negativos. Embora a ideia de manter as crianças seguras online seja louvável, algumas medidas podem ser contraproducentes para essa iniciativa, exigindo um recolhimento maior de dados sobre os jovens. Especificamente, a tecnologia de verificação de idade ainda enfrenta sérios desafios técnicos que provavelmente prejudicam a segurança e a privacidade dos seus utilizadores. 404 Media relataram recentemente a violação de um provedor de verificação de idade, expondo informações confidenciais (link em inglês): https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/ Métodos mais precisos muitas vezes exigem a coleta de dados pessoais adicionais, potencialmente em conflito com os compromissos de privacidade de um serviço para com seus usuários e com suas obrigações legais. A obrigatoriedade de coletar e reter informações confidenciais adicionais sobre os usuários cria sérios e desnecessários riscos de cibersegurança para organizações e usuários. Se as empresas fossem forçadas a recolher dados de verificação da idade isso, paradoxalmente, forçaria as empresas a recolherem um volume maior de dados sobre crianças. As empresas podem ser forçadas a recolher informações pessoais que não querem recolher e os consumidores não querem dar, e esse recolhimento de dados cria riscos adicionais de privacidade e segurança para todos. Requisitos de verificação da idade levantam sérias questões relativas aos conflitos com os princípios de minimização de coleta de dados e outras medidas de proteção à privacidade dos dados dos consumidores. Para realizar de maneira eficaz medidas de verificação da idade, as empresas seriam obrigadas a recolher dados adicionais – incluindo o recolhimento e o armazenamento dos seus dados de geolocalização para garantir que não residam fora do estado ao confirmar que têm idade para utilizar estes serviços, o que resultaria em um volume maior de dados especificamente sobre crianças. A necessidade de recolher volumes adicionais de dados seria efetivamente aplicada a todos os usuários, pela natureza da necessidade de discernir entre utilizadores adultos e crianças e adolescentes. Além disso, os pais ou responsáveis ¿¿de usuários mais jovens provavelmente seriam obrigados a fornecer informações financeiras confidenciais e

informações de identificação pessoal ao consentirem e fornecerem verificação de idade em nome de usuários mais jovens. A agência francesa de proteção de dados analisou recentemente várias soluções existentes de verificação de idade online, mas descobriu que nenhuma das opções poderia satisfazer três padrões principais: 1) fornecer uma verificação suficientemente confiável; 2) permitir a cobertura completa da população; e 3) respeitar a proteção dos dados, privacidade e segurança dos indivíduos. Esse relatório está disponível em inglês em: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.","708764":"Esses métodos também podem levar a diferenciação entre os usuários, especialmente aqueles que não possuem documentos de identificação emitidos pelo governo ou acesso às instituições financeiras necessárias para verificação, potencialmente discriminando grupos demográficos específicos. Além disso, as pequenas empresas podem não ter recursos financeiros para implementar tais dispositivos de verificação. Aumentar a confiança em se saber a idade de um usuário específico tem implicações na salvaguarda dos seus direitos de privacidade, garantindo o seu acesso à informação e preservando a sua liberdade de participar em experiências digitais sem restrições.","708768":"À medida que continuam as discussões sobre segurança e privacidade infantil online, as principais empresas de tecnologia estão trabalhando tanto em conjunto quanto de forma independente para promover a segurança online. Estes empreendimentos críticos incluem o trabalho conjunto em organizações como a Digital Trust & Safety Partnership, a Technology Coalition e o Family Online Safety Institute, entre outras, cujos esforços coletivos promovem a segurança infantil online e fornecem recursos para que os pais possam fornecer experiências digitais mais seguras para os jovens. Além disso, muitas empresas desenvolveram os seus próprios produtos e ferramentas para alcançar este objetivo, fornecendo recursos com maior clareza e informações aos pais, mas evitando a confusão e os custos associados a um requisito de consentimento parental excessivamente prescritivo.","708772":"As empresas devem ser capazes de fornecer essas informações de forma simples, clara e acessível, sem a imposição de requisitos redundantes e separados que criariam uma confusão desnecessária para pais e empresas. Os pais encontrariam solicitações de consentimento mais longas e repetitivas que podem causar fadiga de consentimento e, principalmente, reduzir a sua compreensão das práticas de coleta de dados apresentadas. As empresas enfrentariam custos crescentes de conformidade para cada divulgação ou formulário adicional, o que, mais uma vez, não traria benefícios substanciais aos pais. Ao permitir que as empresas forneçam essas informações numa única página ou local, as empresas também podem informar as famílias sobre as inúmeras ferramentas e opções disponíveis para a sua segurança. Isso inclui guias completos para famílias, os quais fornecem detalhes e orientações sobre como criar uma conta supervisionada para crianças, definir os controles parentais corretos para a família e encontrar equilíbrio com a tecnologia online. ","708775":"Os benefícios generalizados e, mais importante ainda, as oportunidades proporcionadas e criadas pelas tecnologias de informação e comunicação devem ser consideradas. Um ponto forte único da Internet é que ela abre muitas portas para inúmeras pessoas com diferentes origens socioeconômicas. A inovação futura e o progresso social dependem desta integração e, embora todos os benefícios possam não ser imediatamente conhecidos, o retorno a longo prazo de permitir que a geração mais jovem aprenda sobre novos temas ou se envolve em causas sociais locais é imensurável.

Descobriu-se também que as redes sociais incentivam a aprendizagem colaborativa que ensina crianças e adolescentes sobre a importância de se valorizar diferentes perspectivas e pontos de vista para compreender melhor o mundo. Isso, por sua vez, ajuda a despertar sua curiosidade e o descobrimento de áreas de interesse para eles. As redes sociais também desempenharam um papel importante na alfabetização digital. É importante ressaltar que pesquisas mostram ser fundamental ajudar as crianças a aprenderem a navegar nos espaços digitais por conta própria. Habilidades socioemocionais como empatia, gentileza e responsabilidade pessoal, que são cruciais para interações offline, também podem ser ensinadas para melhorar as interações online. Mesmo para as crianças mais novas, o ensino de valores através da cidadania digital está ganhando força na prática. De acordo com um estudo sobre crianças em idade escolar nos Estados Unidos, 62% dos professores do ensino fundamental e médio e 69% dos professores do 3º ao 5º ano relataram usar algum currículo de cidadania digital, sendo as competências relacionadas ao desenvolvimento de características positivas de caráter as mais comuns, como a compreensão do cyberbullying e do discurso de ódio. As restrições ao acesso à informação online podem minar e impedir este progresso e avanços futuros, especialmente para os usuários que procuram comunidades de apoio, e levantam preocupações sobre os utilizadores mais vulneráveis ¿¿(ou seja, crianças em lares abusivos ou aqueles sem acesso a comunidades de apoio na sua localização física). Da mesma forma, tais disposições levantam preocupações sobre a liberdade de expressão, limitando o acesso ao discurso legal. A CCIA é uma associação comercial internacional sem fins lucrativos, que representa uma ampla variedade de empresas de comunicação e tecnologia. Há mais de 50 anos, a CCIA promove mercados abertos, sistemas abertos e redes abertas. Agradecemos a oportunidade de participar dessa tomada de subsídios e estamos sempre dispostos a fornecer maiores informações. Materiais em inglês que podem ser úteis à ANPD podem ser encontrados nos seguintes links: https://project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification/; https://project-disco.org/privacy/a-guide-for-how-not-to-pursue-child-protection-online/; https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/; https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

Contribuinte: LUKAS RUTHES GONCALVES

Número: OP-731256

Data: 16/07/2024 - 17:39

Resumo: :"De acordo com o Guia Orientativo da ANPD sobre o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas, “no caso de tratamento de dados pessoais de crianças e de adolescentes, este deverá ser realizado sempre em seu melhor interesse, nos termos da LGPD e das demais normas pertinentes, como o Estatuto da Criança e do Adolescente (ECA) e os padrões éticos aplicáveis à pesquisa realizada”. Tal determinação, no entanto, é extremamente ampla, o que gera um cenário de insegurança e incerteza prejudicial ao ambiente acadêmico e ao desenvolvimento da ciência

como um todo. Diante das inúmeras possibilidades de interpretração sobre o que constitui, caso a caso, o “melhor interesse”, tem-se que muitas instituições de pesquisa, representadas pelos seus Comitês de Ética, vêm adotando uma postura que se mostra conservadora quanto à autorização de estudos que envolvem crianças e adolescentes. Assim, acreditamos que as atenções da ANPD devem se voltar a este tópico, de forma a orientar e/ou a regulamentar especificamente o tratamento de dados de crianças e adolescentes no contexto da pesquisa acadêmica, definindo o escopo do “melhor interesse” nesse âmbito e evitando-se, com isso, a negativa que muitas/os pesquisadores/as têm recebido. Além disso, o fato de o consentimento dos pais ou responsáveis legais ser sempre exigido para a coleta e o tratamento dos dados de crianças e adolescentes dificulta e/ou impede a realização de uma série de estudos e pesquisas que podem estar a serviço do melhor interesse dessa população.","708725":"Quando pensamos na realização de estudos e pesquisas, há uma série de situações de tratamento de dados pessoais de crianças e adolescentes que demandam maior clareza do princípio do melhor interesse, como iniciativas voltadas a mapear e compreender: a) práticas e interesses de crianças e adolescentes que não são aprovados ou mesmo do conhecimento de seus pais ou responsáveis legais (ex: educação sexual, casamento infantil, consumo de drogas etc.); b) a realidade de vida de crianças e adolescentes que não convivem com seus pais ou responsáveis legais (ex: indivíduos em situação de rua, abrigados, em cumprimento de medida socioeducativa etc.); e c) a situação de crianças e adolescentes que vivem em um ambiente de conflito familiar em que haja colidência entre os interesses dos pais ou responsáveis legais (ex: disputas judiciais pela guarda, casos de alienação parental, ação de alimentos etc.). Estudos e pesquisas sobre tais temas são de enorme importância, mas com frequência acabam sendo inviabilizados pela necessidade de consentimento e acompanhamento dos pais ou responsáveis legais.","705523":"N/A","708742":"N/A","708745":"Assim como Isabelle da Nóbrega Carneiro, Luiza Caldeira Silva e Danielle Tabach (2019), Caio César Carvalho Lima (2019), Luiza Leite (2020), e Gustavo Tepedino e Milena Donato Oliva (2021), entendemos que o tratamento de dados pessoais e dados pessoais sensíveis de titulares entre 12 e 16 anos completos pode ser autorizado por consentimento manifestado pelo adolescente sem assistência ou representação de seus pais ou responsáveis legais, como hipótese de capacidade especial para este fim, especialmente em caso de participação em pesquisa. Com isso, busca-se atender ao princípio da “autonomia progressiva” previsto na Convenção sobre os Direitos da Criança da ONU e no ECA, combatendo-se uma lógica que privilegia uma concepção adultocêntrica em detrimento da participação de crianças e adolescentes nos processos que lhes dizem respeito. Tal interpretação possibilitaria que estudos sobre determinados contextos e situações - como o envolvimento de adolescentes com práticas e interesses que não são aprovados ou mesmo do conhecimento de seus pais ou responsáveis legais, as necessidades e realidades de vida de adolescentes que não convivem com seus pais ou responsáveis legais e, ainda, a situação de crianças e adolescentes que vivem em um ambiente de conflito familiar em que há colidência de interesses entre seus pais ou responsáveis legais - passassem a ser realizados em prol do melhor interesse desse grupo etário. Isso porque, a não realização dessas pesquisas tem como consequência a produção de um cenário de opacidade que acaba por invisibilizar e desproteger a população a quem o

ordenamento jurídico garante, justamente, prioridade absoluta. Referências: CARNEIRO, I. N.; SILVA, L. C.; TABACH, D. Tratamento de Dados Pessoais. In: FEIGELSON, B.; SIQUEIRA, A. H. (Coords.). Comentários à Lei Geral de Proteção de Dados (Lei 13.709/2018). São Paulo: Thomson Reuters Brasil, 2019. LEITE, L. Tratamento de Dados Pessoais. In: FEIGELSON, B.; BECKER, D.; CAMARINHA, S. (Coords.). Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2020. LIMA, C. C. Do Tratamento de Dados Pessoais. In: MALDONADO, V. N.; BLUM, R. O. (Coords.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. TEPEDINO, G.; OLIVA, M. D. Tratamento de Dados de Crianças e Adolescentes na LGPD e o Sistema de Incapacidades do Código Civil. In: LATERÇA, P. S.; FERNANDES, E.; TEFFÉ, C. S.; BRANCO, S. (Coords.). Privacidade e Proteção de Dados de Crianças e Adolescentes. Rio de Janeiro: ITS Rio; Obliq, 2021.","705539":"N/A","708762":"N/A","708764":"N/A","708768":"N/A","708772":"N/A","708775":"Ainda que a LGPD não devesse “ser interpretada ou aplicada de modo a impedir ou estabelecer obstáculos indevidos ao exercício” de estudos acadêmicos (VARGAS et al., 2023, p. 19), e que “dúvidas quanto à capacidade de consentimento” dos/as titulares não devesse “ser uma questão ou impeditivo para a pesquisa” (PENALVA, 2013, p. 78), é exatamente assim que os Comitês de Ética de várias instituições de ensino estão a utilizando. Devido a debates morais que cercam a infância e a adolescência e pela salvaguarda contra eventuais processos que poderiam resvalar em si, a proteção à intimidade de crianças e adolescentes é inflada por diversas instituições, públicas e privadas, inclusive de pesquisa, desconsiderando que “a proteção dos dados e a responsabilidade pelos mesmos é transferida também” aos/às pesquisadores/as (PENALVA, 2013, p. 78). A despeito da relevância geral da LGPD para disciplinar diferentes questões, no que diz respeito especificamente à realização de pesquisas, referida lei desperdiçou a oportunidade de traçar uma regulamentação que definisse a matéria sem deixar margens à interpretação, já que, no atual cenário, a postura de muitas instituições continua sendo, como regra, a de negar a condução de estudos envolvendo crianças e adolescentes. É urgente, portanto, se pensar alternativas que garantam tanto o resguardo de crianças e adolescentes quanto o desenvolvimento de pesquisas na área. Um caminho possível para tanto seria o de ouvir as experiências de pesquisadores/as e de crianças e adolescentes, contando com a sua participação no processo de regulamentação da matéria, de forma a não mais fragilizá-los/as no momento em que desenvolvem ou participam de estudos e investigações. Além disso, referido processo poderia se beneficiar da participação de representantes de Comitês de Ética de diferentes instituições, procurando formas de endereçar seus principais questionamentos e preocupações em relação ao tema. Referências: PENALVA, J. Empiria e Argumentação: Pesquisa e Intervenção Social. In: MINISTÉRIO DA JUSTIÇA. O Papel da Pesquisa na Política Legislativa: Metodologia e Relato de Experiências do Projeto Pensando o Direito. Brasília: Ministério da Justiça, 2013. VARGAS, A. G.; RABELO, A. A.; COSTA, D. V. et al. Tratamento de Dados Pessoais para Fins Acadêmicos e para a Realização de Estudos e Pesquisas: Guia Orientativo. Brasília: ANPD, 2023.

Contribuinte: LARISSA CRISTINA MARGARIDO

Número: OP-732491

Data: 17/07/2024 - 10:19

Resumo: :"Nada a acrescentar. ","708725":"Nas situações em que envolvam o escopo de segurança e bem-estar das crianças e adolescentes, como mecanismos de prevenção à fraude, controles de entrada e saída e rastreio em websites. ","705523":"Documentos que demonstrem legalmente a guarda da criança ou adolescente. ","708742":"Assinatura digital realizada via certificado ou reconhecida por firma, assinatura via gov, todas acompanhadas de documento que demonstre legalmente a guarda da criança ou adolescente, quando aplicável. ","708745":"Essa análise deve ser realizada em paralelo com o que dispões o Estatuto da Criança e do Adolescente, uma vez que há previsão no Art. 90, incisos V e IX, de proteção da privacidade da criança e do adolescente, bem como sobre a responsabilidade parental. Considerando as várias possibilidades que o ambiente digital oferece ao seu usuário, a manutenção/implementação deve considerar as disposições do Direito Civil e do Estatuto da Criança e do Adolescente, não devendo ser aplicado o "princípio do melhor interesse" para uma autonomia progressiva para estes usuários, por se tratarem de dados sensíveis e que podem ser tratados para fins os quais a criança ou/e adolescente não possuí maturidade suficiente para compreender a finalidade do tratamento, presumindo que a finalidade do tratamento atenda ao disposto na LGPD e seja clara, objetiva e de fácil acesso. Desta forma, o consentimento ao tratamento dos dados de crianças e adolescentes deve seguir através da autorização de seus representantes legais. ","705539":"Nada a acrescentar. ","708762":"Nada a acrescentar. ","708764":"Nada a acrescentar. ","708768":"Nada a acrescentar. ","708772":"Nada a acrescentar. ","708775":"Nada a acrescentar.

Contribuinte: INGRID FERNANDES GLORIA SATO

Número: OP-732931

Data: 17/07/2024 - 13:34

Resumo: :"CNseg: Considerando que a identificação do que representa o melhor interesse da criança e do adolescente exige uma análise contextual, não vislumbramos, ao menos pela perspectiva do Setor de Seguros, a necessidade de a ANPD prestar orientações adicionais sobre o tema ou regulamentá-lo mais especificamente.","708725":"CNseg: É razoável que a ANPD emita diretrizes mais específicas, que digam respeito a casos em que o tratamento de dados pessoais decorre do oferecimento de serviços dirigidos especialmente para crianças e adolescentes. Em nome do princípio do melhor interesse da criança, a Autoridade deveria abordar os limites e possibilidades do tratamento de dados pessoais de crianças e adolescentes no uso de plataformas digitais, de aplicativos, jogos e também de serviços e contratos, tais como internet banking e outros produtos que podem criar deveres jurídicos. Ainda que a criança não tenha capacidade civil, os adolescentes relativamente capazes podem, sob assistência do responsável legal, assumir obrigações e é preciso determinar os

limites dessa assistência e assunção, sobretudo num ambiente digital e de conexão com a internet quase que ininterrupta.","705523":"CNseg: O consentimento pressupõe a inexistência de outras bases legais para tratamento de dados do menor. Considerando o Enunciado CD/ANPD nº 1/2023, os dados de menores podem ser tratados por quaisquer bases elencadas nos artigos 7º e 11 da LGPD, desde que observado como prevalescente o melhor interesse do menor e, portanto, o entendimento do §1º do art. 14 da LGPD deveria ter uma interpretação restritiva aos casos em que o tratamento seja realizado mediante consentimento específico e em destaque dos pais/responsáveis legais. Quanto aos parâmetros, deve ser observado que, quando solicitado o consentimento para o tratamento do dado de um menor, exista campo para seleção/preenchimento do mesmo ou campo análogo, que contenha também as informações sobre a impossibilidade da prestação do serviço/execução do contrato caso não haja tal consentimento, por exemplo. O controlador que estiver em vias de coletar consentimento do responsável por criança e adolescente precisa se atentar para o fato de que tal consentimento observar uma linguagem clara, que expresse os futuros e possíveis usos que serão dados aos dados pessoais coletados. ","708742":"CNseg: Devem ser implementados métodos que garantam que o consentimento seja dado de maneira ativa e inequívoca pelos pais ou responsáveis. Tais métodos podem incluir formulários eletrônicos com confirmação por e-mail, assinaturas eletrônicas seguras, duplo fator de autenticação ou autenticação multifatorial para garantir a identidade dos responsáveis, ou outro meio que se mostrar eficaz, a critério do controlador.","708745":"CNseg: As disposições do direito civil, a respeito das capacidades civis, não nos parecem adequadas para regular a obtenção de consentimento para o tratamento de dados pessoais de adolescentes. Nos parece mais apropriado reconhecer a autonomia progressiva desses titulares, sempre levando em consideração a situação concreta do tratamento de seus dados pessoais. Sobre o tema, pode-se citar as seguintes lições doutrinárias dos professores Gustavo Tepedino e Milena Donato Oliva[1]: "Como se vê, o regime das incapacidades sofreu grande mudança com o advento do EPD, o qual, informado pela Constituição da República, poderá suplantar categorias formalistas e abstratas em prol da proteção da pessoa concretamente considerada, daí decorrendo a valorização do discernimento humano, notadamente nas situações existenciais. Nessa esteira também deve ser compreendida temática do consentimento para fins de tratamento de dados pessoais, consoante a normativa delineada na LGPD, e diante do evidente avanço da norma ao atribuir maior liberdade aos adolescentes para manifestarem sua vontade de forma autônoma e válida quanto aos seus dados, sem que se pretenda sobrepor ou confundir tal lei específica com o sistema em vigor para a prática dos atos por sujeitos considerados incapazes pelo regime atual." Em reforço ao argumento, cumpre chamar a atenção para o princípio da autonomia progressiva do adolescente, expressamente mencionado na Resolução nº 245/2024, do Conselho Nacional dos Direitos da Criança e do Adolescente - CONANDA, que dispõe sobre os direitos das crianças e adolescentes em ambiente digital. Além disso, também cabe aqui referir-se ao Comentário Geral nº 25 de 2021, do Comitê de Direitos da Crianças da ONU, que preconiza o seguinte: "Estados Partes devem respeitar o desenvolvimento progressivo das capacidades da criança como um princípio habilitador que trata do processo de aquisição gradual de competências, compreensão e agência. Este processo tem um significado

específico no ambiente digital, onde as crianças podem se engajar de forma mais independente da supervisão das mães, pais e provedores de cuidados. Os riscos e oportunidades associados ao engajamento das crianças no ambiente digital mudam dependendo de sua idade e estágio de desenvolvimento. Estados Partes devem ser guiados por essas considerações sempre que estiverem formulando medidas para proteger as crianças nesse ambiente ou facilitar seu acesso a ele. A elaboração de medidas apropriadas à faixa etária deve ser informada pelas melhores e mais atualizadas pesquisas disponíveis, a partir de uma gama de disciplinas." ","705539":"CNseg: Não vislumbramos, ao menos pela perspectiva do Setor de Seguros, a necessidade de a ANPD prestar orientações sobre o tema ou regulamentá-lo mais especificamente.","708762":"CNseg: Não vislumbramos, ao menos pela perspectiva do Setor de Seguros, a necessidade de a ANPD prestar orientações sobre o tema ou regulamentá-lo mais especificamente.","708764":"CNseg: Não vislumbramos, ao menos pela perspectiva do Setor de Seguros, a necessidade de a ANPD prestar orientações sobre o tema ou regulamentá-lo mais especificamente.","708768":"CNseg: Não vislumbramos, ao menos pela perspectiva do Setor de Seguros, a necessidade de a ANPD prestar orientações sobre o tema ou regulamentá-lo mais especificamente.","708772":"CNseg: Não vislumbramos, ao menos pela perspectiva do Setor de Seguros, a necessidade de a ANPD prestar orientações sobre o tema ou regulamentá-lo mais especificamente.","708775":"CNseg: As finalidades de tratamento que, se limitadas ou bloqueadas pela natureza dos dados, podem vir a limitar ou até impedir o acesso dos titulares menores de idade a produtos e serviços essenciais. A ANPD precisa garantir que os tratamentos que geram benefício aos menores de idade sejam sustentáveis para os controladores, sem um ônus desproporcional, evitando, assim, desencorajar a prestação de serviços para essa faixa etária. Por oportuno, vale acrescentar que se torna fundamental a promoção pelo Estado do pensamento crítico sobre o tratamento de dados pessoais entre crianças e adolescentes, por meio de conscientização em escolas e/ou políticas públicas, por exemplo.

Contribuinte: CAROLINA CARVALHO LUTTERBACH

Número: OP-733045

Data: 17/07/2024 - 14:21

Resumo: :"A Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (“FecomercioSP”), vem por meio desta, apresentar, suas respostas a todos os quesitos levantados pela ANPD na tomada de subsídios sobre o Tratamento de Dados Pessoais de Crianças e Adolescentes. - Considerando recente decisão da ANPD sobre a suspensão do treinamento de sistemas de Inteligência Artificial Generativa pela Meta[1], entendemos que deve ser explorada com maior aprofundamento pela ANPD a adequada aplicação do melhor interesse no desenvolvimento de produtos e serviços, notoriamente o treinamento de sistemas de IA no contexto de dados publicamente disponíveis – considerando a altamente provável presença de dados de crianças e adolescentes e a inviabilidade prática de removê-los. Nesse contexto, além da necessidade de se avaliar se existe, de fato, risco acrescido ao menor,

sobretudo no caso de dados publicamente disponíveis (considerando a presença dessas informações de forma acessível ao público), defendemos a necessidade de avaliar o "melhor interesse", não apenas de forma individualizada, mas também de forma coletiva. Isso se opera tendo em vista, em primeiro lugar, que os impactos positivos do desenvolvimento de tais tecnologias pode não ser individual, mas auferido por toda uma classe de menores, ou mesmo pela sociedade globalmente considerada, de modo que a avaliação exclusivamente individualista possa gerar uma conclusão inadequada pela não satisfação do melhor interesse, em prejuízo aos menores (ou a sociedade) globalmente considerada. Em segundo lugar, no contexto acima apresentado, de exploração de dados publicamente disponíveis, a identidade do menor pode sequer ser conhecida, pelo que avaliação individualista seria impossível – resultando, em última análise, na inviabilidade de treinamento de sistemas de IA pautados em mineração de dados, o que representa um entrave ao desenvolvimento socioeconômico absolutamente não desejável. Com isso, não queremos afirmar que o melhor interesse da criança e adolescente como indivíduos, sempre que possível essa avaliação, não sejam considerados, mas que os riscos sejam ponderados, também, com o interesse do grupo no qual esses menores se enquadram. Com efeito, existem medidas apropriadas para garantir o melhor Interesse do menor já previstas na literatura, por exemplo, a consideração de seu ponto de vista e a obtenção de sua aquiescência, quando viável, avaliação dos impactos concretos aos menores com, minimamente razoável probabilidade de ocorrência, avaliação de formas com que os direitos fundamentais podem vir a ser afetados [2]. Ainda, devem ser adotadas medidas de segurança que busquem reduzir os riscos aos menores a níveis assemelhados ao padrão de risco habitual do menor ("risco mínimo"), de modo que situações em que o menor se encontre sujeito a risco significativamente acrescido sejam sempre excepcionais [3]. [1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf. Acesso em 09.07.2024 [2] Disponível em: https://www.jusbrasil.com.br/doutrina/secao/51-marco-civil-da-internet-mci-5-regulacao-normativa-do-ambiente-digital-no-brasil-das-multiplas-infancias-direitos-fundamentais-da-crianca-no-ambiente-digital-ed-2023/1929470121 . Acesso em 09.07.2024 [3] Disponível em: https://periodicos.unb.br/index.php/rbb/article/view/7701. Acesso em 09.07.2024 ","708725":"Por conta dos motivos apresentados no questionamento 1 deste item, acreditamos que a ANPD deve adotar posicionamento mais cuidadoso sobre o tratamento de dados pessoais de crianças e adolescentes no contexto no desenvolvimento de produtos e serviços, notoriamente o treinamento de sistemas de inteligência artificial com uso de dados publicamente disponíveis. ","705523":"Entendemos que, seguindo as boas-práticas, especialmente a NBR ISO 29184:2021 e o Guideline 05/2020 do European Data Protection Board [1], o consentimento satisfará os requisitos de "específico e em destaque", quando atender aos seguintes requisitos: (a) forem fornecidas as informações requeridas pelo art. 9° da LGPD; (b) caso se adote consentimento em camadas, a finalidade for claramente declarada na primeira camada (em que o consentimento é efetivamente aceito); e (c) que o consentimento para finalidades distintas seja obtido de forma apartada. [1] Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em 09.07.2024. ","708742":"A autenticação, que consiste na verificação de

identidade, geralmente é realizada por meio da apresentação de um ou mais dos seguintes elementos: (a) algo que a pessoa possui (como um token ou cartão); (b) algo que a pessoa é (como uma característica biométrica); e (c) algo que a pessoa sabe (como uma senha). Consideramos que a solução para validar a identidade do pai ou responsável legal deve ser analisada de acordo com o contexto em que o consentimento foi obtido, a existência de uma relação prévia entre o agente de tratamento e o responsável legal do menor, e os impactos de longo prazo para o menor caso o consentimento não seja obtido com a intervenção adequada dos pais – sendo necessária ponderação desses três fatores para avaliar a solução mais adequada ao caso concreto. Em relação ao impacto, é necessário resguardar razoável proporcionalidade entre os potenciais impactos ao menor afetado e os impactos potenciais decorrentes do processo de verificação da obtenção do consentimento pelos pais: quanto mais graves forem os impactos, mais robustos devem ser os meios de validação utilizados, por exemplo em grande parte das situações de menor risco, a mera declaração do pai ou do responsável pode se perfazer suficiente [1] – tal diretriz deriva, destacamos, do próprio princípio da necessidade, o qual demanda proporcionalidade entre a finalidade perseguida e a operação de tratamento. No que diz respeito ao contexto, é crucial avaliar se o consentimento foi obtido de forma presencial ou remota. Em situações presenciais, acreditamos que a apresentação de documentos que comprovem a relação entre o responsável legal e o menor (como documentos comprovativos de identidade que incluam a filiação) é suficiente para a verificação de identidade, a menos que haja razões concretas para suspeitar de fraude ou outras irregularidades. Já em casos de coleta remota, pode ser necessário implementar outros mecanismos de autenticação – seja pela inviabilidade de obtenção dos documentos, seja pela possível inadequação e desproporcionalidade, em muitas das situações da vida prática, de se requerer cópia da documentação de identidade. Quanto à existência de relação prévia com o pai ou responsável legal do titular, e considerando que os impactos potenciais da ausência de intervenção parental não exigem medidas mais robustas, acreditamos que: (a) Quando há relação prévia, o consentimento pode ser vinculado à apresentação de informações ou a execução de ações que, considerando os dados detidos da relação pré-existente, provavelmente envolvam a participação do responsável legal. Isso pode incluir: (i) envio de token para endereço de contato cadastrado do pai ou responsável legal; (ii) obtenção de consentimento diretamente pelo responsável legal em seu ambiente logado; (iii) fornecimento da senha pessoal do pai ou responsável legal; e (iv) envio da solicitação de consentimento diretamente ao endereço de e-mail cadastrado do Pai ou do responsável legal. (b) Nos casos em que não há relação prévia com o responsável legal, entendemos que a solicitação de informações que provavelmente não sejam conhecidas pelo menor (considerando tratar-se de uma criança), mas que possam ser facilmente verificadas pelo agente de tratamento (como o número de CPF e a data de nascimento do responsável legal), é suficiente para cumprir o requisito legal, ressalvado se a natureza da operação de tratamento, e os riscos advindos ao menor, demandarem um maior cuidado. [1] Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf. Acesso em 09.07.2024. ","708745":"Entendemos que a consideração da autonomia progressiva dos titulares, possibilitando a obtenção do consentimento sem a representação ou assistência dos pais e dos responsáveis legais, é a

opção que melhor atende o texto legal da LGPD, devendo, portanto, ser a interpretação necessariamente adotada, sob pena de tornar a diferenciação feita entre crianças e adolescentes, pelo texto legal, efetivamente inútil. Explicamos: o Estatuto da Criança e do Adolescente[1] estabelece como adolescente a pessoa maior de 12 (doze) anos e menor de 18 (dezoito) anos, e crianças os menores de 12 (doze) anos (Art. 2°) – se fossemos adotar o modelo de capacidade previsto no Código Civil, mormente em seu art. 1.690, apenas adolescentes com mais de 16 (dezesseis) anos poderiam ofertar o seu consentimento e, ainda assim, apenas se assistidos pelos pais. Transcorre que essa não foi a opção legislativa na LGPD: inspirado pelo diploma europeu, o legislador determinou que apenas crianças precisariam ter seu consentimento ofertado pelo responsável legal (art. 12, §1°), possibilitando, portanto, que adolescentes exerçam o seu direito de autonomia informacional diretamente. Em outras palavras: o legislador optou que, para efeitos da oferta do consentimento, este é plenamente válido, desde que o menor tenha idade superior a 12 (doze anos). Existindo confronto aparente entre o dispositivo da LGPD e o disposto no Código Civil (que determina que apenas o maior de dezesseis anos poderia ofertar citado consentimento), precisamos nos fazer valer das regras de conflito aparente de normas (antinomia) – dentre as quais destaca-se o princípio da especialidade, segundo a qual a lei especial derroga a lei geral[2]. Sendo a LGPD lei especial, quanto ao tratamento de dados pessoais, em relação ao Código Civil (lei geral), deve prevalecer o disposto na LGPD, segundo o qual, reforçamos, o consentimento de maiores de 12 (doze) anos é plenamente válido, satisfeitos os demais requisitos previstos em lei. [1] Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 09.07.2024. [2] Disponível em: https://www.jusbrasil.com.br/doutrina/secao/331-antinomia-33-completude-do-ordenamento-introducao-a-ciencia-do-direito-privado/1327556345. Acesso em 09.07.2024. ","705539":"Não há solução única que se aplique a todos os casos. Por isso, a abordagem de qualquer regulação ou guia elaborado pela ANPD deve necessariamente basear-se em abordagem principiológica. Nesse contexto, deve-se dar centralidade ao Princípio do Melhor Interesse, com instruções claras e objetivas sobre como aplicá-lo de forma verificável, alinhando-o aos demais princípios previstos na legislação. Com base na literatura especializada sobre o tema [1] [2], propomos "leitura conforme" dos seguintes princípios legais, à luz do melhor interesse do menor: (a) Princípio da Finalidade: O tratamento de dados deve gerar benefícios para o menor, ou para a categoria de menores afetados, mesmo que os benefícios sejam meramente potenciais. (b) Princípios da Adequação e Necessidade: O tratamento deve ser adequado e limitado ao estritamente necessário para alcançar o benefício potencial desejado. (c) Princípios da Segurança e Prevenção: Devem ser adotados controles para reduzir ao máximo os riscos enfrentados pelos menores. Esses riscos, exceto em situações excepcionais, não devem ser superiores aos habitualmente enfrentados pelo menor no contexto em que se encontra – a título de exemplo, a base de dados utilizadas por uma instituição de ensino para enviar avisos aos seus estudantes menores de idade, não pode ter segurança inferior a base de dados utilizada para armazenar o cadastro ou a matrícula do estudante. (d) Transparência: Além dos requisitos expressos na LGPD, especialmente no artigo 9º, as informações fornecidas aos titulares menores de idade devem ser claras, concisas, simples e apropriadas para a faixa etária correspondente [3]. Além disso, é essencial

que, ao planejar novos projetos envolvendo o tratamento de dados de crianças e adolescentes, sejam adotados cuidados apropriados, incluindo a observância dos princípios de Privacy by Design e Privacy by Default. Isso inclui a avaliação da necessidade de Relatório de Impacto, a realização de testes de balanceamento (sendo o caso) e o gerenciamento de riscos de privacidade. Recomenda-se que a ANPD trace diretrizes para a implementação desses controles, não como uma obrigação legal, mas como uma boa prática a ser considerada. [1] Disponível em: https://ibdpac.com.br/o-assentimento-ao-consentimento-das-crianc%CC%A7as-para-participar-em-pesquisa-clinica-por-uma-capacidade-sanitaria-juridicamente-reconhecida/. Acesso em 09.07.2024 [2] Disponível em: https://periodicos.unb.br/index.php/rbb/article/view/7701. Acesso em 09.07.2024 [3] Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf. Acesso em 09.07.2024.
","708762":"Conforme orientam as Autoridades de Dados do Reino Unido[1] e da França [2] em seus guias sobre o tema, a técnica utilizada para verificar a identidade do titular deve ser proporcional aos riscos que o serviço ofertado e as operações de tratamento implicam ao titular, bem como às tecnologias disponíveis ao controlador. Entendemos que esse entendimento deve prosperar por dois motivos: em primeiro lugar, caso não seja guardada a devida proporcionalidade entre os meios utilizados para validar a identidade e os riscos que o titular corre caso a operação seja executada, é possível que o meio utilizado para validar a identidade gere maior risco potencial ao titular, do que a operação em si. Em segundo lugar, caso não se considere as tecnologias disponíveis ao controlador (e a razoabilidade de sua exigência) pode-se criar um entrave demasiadamente pesado ao desempenho da atividade econômica. Isso posto, entendemos que, em geral, para operações de tratamento de menor risco (como o recebimento de e-mail marketing ou do newsletter de determinada página), a mera declaração da idade pelo titular deve ser considerada suficiente para verificar a identidade [1] – isto porque a coleta ulterior de dados do titular para validar a sua identidade tendem a gerar riscos mais agravados ao titular do que a mera execução do tratamento, a qual, no pior dos casos, tendem a gerar spam. No entanto, em situações que envolvam um risco acrescido ao titular, medidas mais robustas podem se perfazer necessárias[2]. Por outro lado, em situações em que o risco para o titular seja mais significativo, podem ser necessárias medidas mais robustas. No entanto, não é possível delinear exaustivamente quais medidas devem ser adotadas, pois estas dependem da situação concreta. A seguir, apresentamos alguns entendimentos gerais sobre o tema. Se existe uma relação prévia com o titular, especialmente se o acesso a uma aplicação de internet está vinculado a outro serviço contratado em favor do menor de idade (como serviços educacionais no caso de uma aplicação escolar), é razoável pressupor que a idade do titular já tenha sido validada no momento da contratação do serviço, ou mesmo tenha sido diretamente fornecida por seus responsáveis legais. Nesse caso, não seria necessária qualquer verificação posterior, e a idade constante na aplicação refletiria aquela nos dados cadastrais junto ao agente de tratamento. Se, no entanto, não houver relação prévia com o titular, e os riscos envolvidos no serviço demandarem a validação da idade do menor, consideramos suficiente a apresentação do CPF e da respectiva data de nascimento, levando em conta: (a) a baixa invasão de privacidade proporcionada pelo fornecimento desses dados, dado que além de serem dados meramente

cadastrais, o CPF é um dado de domínio público, conforme o art. 1°, §2°, da Instrução Normativa SRF nº 19/1998 [3]; (b) a facilidade com que esses dados podem ser validados, seja por meio de serviços públicos, como os disponibilizados pela própria Receita Federal para validação do CPF, seja por meio de serviços de terceiros. Destacamos, contudo, que é possível o emprego de técnicas mais intrusivas para a verificação da idade e identidade do titular, como biometria facial, quando a o bem jurídico protegido, especialmente a necessidade de prevenção a fraudes, assim requerer. [1] Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf. Acesso em 09.07.2024. [2] Disponível em: [1] Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf. Acesso em 09.07.2024. [3] Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=13242&visao=compilado. Acesso em 09.07.2024. ","708764":"Entendemos que o princípio do melhor interesse é, em si mesmo, limitação suficiente e adequada para o tratamento de dados pessoais de crianças e adolescentes, sobretudo quando analisado à luz dos demais princípios legais já previstos na Lei Geral de Proteção de Dados, sobretudo finalidade, adequação e necessidade. Isto se opera, em primeiro lugar, porque o princípio do melhor interesse requer que os agentes de tratamento considerem e observem os interesses do menor (ou do grupo de menores) afetado por sua operação de tratamento, eivando de ilicitude, por conseguinte, atividades de tratamento que sejam razoavelmente contrárias à referidos interesses. Nessa esteira, conforme observado no primeiro questionamento deste item “III”, a própria interpretação dos princípios legais deve se operar em conformidade com o Melhor Interesse. Não obstante, tal qual a base legal do legítimo interesse, o princípio do melhor interesse permite que os agentes de tratamento tenham a flexibilidade necessária para se amoldar ao caso concreto, evitando o enrijecimento da atividade – o que poderia se dar em caso de determinação de medidas específicas a serem observadas. O que é recomendável, no entanto, que seja feito pela ANPD é que estabeleça mecanismos (assim como o teste de balanceamento elaborado para a base legal do legítimo interesse) que facilite a avaliação objetiva, pelos agentes de tratamento, do atendimento do princípio do melhor interesse. ","708768":"Conforme bem pontua a Autoridade de Dados da França (CNIL), os exemplos típicos de controle parental envolvem a (a) filtragem de conteúdo inapropriado (permitindo, por conseguinte, que os pais restrinjam o conteúdo fornecido aos menores); (b) regulem a utilização de serviços digitais (limitando o tempo de tela, definindo a possibilidade de gasto online e regulamentando interações com aplicações e dispositivos); e (c) monitoramento de atividade (possibilitando aos pais acesso ao histórico de navegação, conversas e conteúdo, bem como geolocalização dos menores)[1]. No entanto, como outros aspectos relativos às crianças e aos adolescentes, o controle parental deve ser avaliado de forma contextual, considerando o objeto, os riscos existentes ao menor de idade, bem como o setor e as regras a ele aplicáveis – sobretudo considerando que a adoção de controles parentais demanda o tratamento de dados pessoais, os quais podem ser, inclusive, significativamente intrusivos. Tendo isso em consideração, conforme bem pontua a CNIL, ao se pensar em controle parental é necessário considerar: (a) adequada proporcionalidade, tomando em consideração

o direito de privacidade do menor, inclusive em relação aos pais e responsáveis legais, em conformidade com a sua capacidade de discernimento; (b) transparência adequada para com a criança fornecendo-lhe explicações adequadas sobre o funcionamento dos controles parentais; (c) adotar medidas de segurança adequada para proteger os dados dos menores, impedindo seu acesso por terceiras partes[1]. [1] Disponível em: https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests. Acesso em 10.07.2024. ","708772":"De acordo com a pesquisa TIC Kids Online Brasil realizada em 2023 [1], constatou-se que 88% da população brasileira de 9 a 17 anos possui perfis em plataformas digitais, com essa porcentagem aumentando para 99% na faixa etária de 15 a 17 anos. Na mesma pesquisa, verificou-se que 53% dos entrevistados entre 11 e 12 anos afirmaram ler as políticas de privacidade dos aplicativos e sites que utilizam, e essa proporção sobe para 57% entre os jovens de 15 a 17 anos [2]. Observa-se, portanto, uma grande oportunidade de educar este público sobre privacidade e proteção de dados. Para tanto, é necessário ofertar informações que, em atenção as particularidades de sua faixa etária, seja razoavelmente fáceis de ler e compreender, nesse sentido, com base no Guia da Autoridade de Dados do Reino Unido [3], destacamos a necessidade de que as informações destinadas aos menores de idade sejam claras, concisas e simples. Sempre que possível, é recomendada a utilização de recursos visuais para fornecer informações – como diagramas, desenhos, gráficos, vídeos e painéis. Nesse sentido, o chamado "visual law" desempenha um papel relevante ao tornar as informações não apenas compreensíveis, mas também atraentes e divertidas. Nessa esteira, destacamos que a Autoridade de Proteção de Dados Francesa, a CNIL, desenvolveu uma plataforma dedicada à conexão entre dados pessoais e design, denominada “Données & Design par LINC” [4]. Nesta plataforma, são disponibilizadas sugestões de padrões de design (que vão além de recursos visuais) para implementar o princípio da transparência nas interfaces e jornadas dos usuários em serviços digitais. Algumas dessas sugestões incluem: (i) organizar a estrutura das informações por finalidade, perguntas ou níveis de informação; (ii) sintetizar informações por meio de resumos ou tabelas; (iii) facilitar o acesso a determinados blocos de informação por meio de barras de pesquisa, hiperlinks e índices clicáveis No entanto, ao avaliar as boas práticas, é necessário considerar que nem todas as informações podem ser comunicadas exclusivamente por meio de recursos visuais. Consequentemente, a adoção de avisos de privacidade em camadas pode ser necessária. Isso significa fornecer uma versão resumida das informações em formato visual, permitindo uma compreensão geral sobre o tratamento de dados pessoais, enquanto informações mais detalhadas ficam disponíveis em documentos elaborados em formatos tradicionais. [1] Disponível em: https://cetic.br/en/noticia/tic-kids-online-brasil-2023-criancas-estao-se-conectando-a-internet-mais-cedo-no-pais/#:~:text=Conforme%20o%20levantamento%2C%2088%25%20das,%25%20TikTok%20e%2041%25%20Facebook. Acesso em 02.07.2024 [2] Disponível em: Indicadores (cetic.br). Acesso em 02.07.2024 [3] Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf. Acesso em 09.07.2024. [4] Disponível em: https://design.cnil.fr/design-patterns/ . Acesso em 02.07.2024 ","708775":"Entendemos que as questões atinentes a adequada aplicação do melhor interesse no desenvolvimento de produtos e serviços, notoriamente o

treinamento de sistemas de inteligência artificial no contexto de dados publicamente disponíveis, conforme exposto nas respostas apresentadas aos quesitos do item “I”, deste questionário.

Contribuinte: Jean Michel Duarte Santana

Número: OP-733410

Data: 17/07/2024 - 16:52

Resumo: :"A garantia da proteção à infância para crianças que acessam o ambiente online, atualmente não possui um controle satisfatório de conteúdos impróprios e deve ser uma responsabilidade multissetorial compartilhada entre órgãos com poder fiscalizatório, dentre os quais se encontra a ANPD. Desse modo, a ANPD deve fornecer um arcabouço regulamentar capaz de coibir práticas que exponham negativamente crianças e adolescentes, penalizando as empresas responsáveis por aplicações, sites e conteúdos que não garantam, por exemplo, um controle de acesso eficaz, conforme a classificação etária. Nesse sentido sugere-se que a ANPD estabeleça, mediante regulamento: (i) medidas de segurança e atenção ao melhor interesse do menor a serem adotadas pelos provedores de conteúdo online, (ii) delimite as situações em que haverá a responsabilidade compartilhada, o que se tratando de direito da criança e do adolescente deve ser abordado como regra (conforme competência estabelecida no art. 227 da CF/1988), e (iii) sanções administrativas em face de descumprimentos. Entende-se que essa ponderação é válida quando avaliado o princípio do melhor interesse e a aplicação da base legal do interesse legítimo, posto que a garantia de um ambiente seguro na internet não pode onerar a parte mais frágil da relação; um jogo com caráter socioeducativo não vislumbra a necessidade de um prévio consentimento dos pais, contudo, de igual modo, um jogo com alto teor de violência ou alto potencial viciante não pode ser pautado exclusivamente em um consentimento dos responsáveis, que muitas vezes são hipossuficientes tecnicamente, e não possuem o conhecimento do prejuízo que aquele conteúdo fará à criança, por exemplo. Nesse sentido, a base legal do legítimo interesse, observando-se sempre o melhor interesse da criança, não necessariamente precisa ser uma exceção, mas sim, possuir medidas eficazes de fiscalização e garantia de que esse melhor interesse será observado pelas empresas, em especial, no ambiente online. Cita-se como exemplo a regulamentação de serviços digitais da União Europeia (Digital Services Act) que entrou em vigor em março de 2024. Dentre muitas obrigações e mecanismos de segurança recomendados para empresas de tecnologia, dispõe sobre a efetivação de um maior controle sobre o conteúdo online, proibição de publicidade dirigida aos menores e a obrigação de agir para combater o conteúdo ilegal e nocivo em suas plataformas, por exemplo. Nesse contexto, recentemente o grupo Meta foi alvo de investigações por parte da União Europeia por possíveis violações de regras de conteúdo online relacionadas à segurança infantil, sendo passível de multas pesadas. Segundo comunicado do Executivo da UE “A Comissão está preocupada com o fato de que os sistemas do Facebook e do Instagram, incluindo seus algoritmos, possam estimular vícios comportamentais em crianças, bem como criar os chamados “efeitos de buraco de coelho"”, e completou, “Além disso, a Comissão também está

preocupada com os métodos de verificação e garantia de idade implementados pela Meta". As preocupações do órgão regulador estão relacionadas ao acesso de crianças a conteúdo inadequado (fonte: https://www.cnnbrasil.com.br/internacional/meta-enfrenta-investigacao-da-uniao-europeia-sobre-riscos-a-seguranca-infantil/). ","708725":"Sim. Conforme abordado no item anterior, a temática de navegação online de crianças e adolescentes em plataformas e aplicativos é preocupante. Segundo levantamento realizado pelo estudo Tic Kids Online Brasil, 95% das crianças e adolescentes de 9 a 17 anos usam internet no Brasil (um total de 25 milhões). Em 2023, 24% desse público disseram ter começado a se conectar à internet antes dos 6 anos de idade. Ainda, segundo a pesquisa mencionada acima, 82% das crianças e adolescentes que possuem acesso à internet, usam para realizar trabalhos escolares (fonte: https://cetic.br/pt/pesquisa/kids-online/). Observados os benefícios do uso da internet para crianças e adolescentes em fase escolar e, entendendo que o acesso à internet deve ser uma garantia também para elas (nos termos da Lei n. 13.979/ 2020 a internet, junto com os serviços de telecomunicações foram considerados serviços essenciais e Res. 245/2024 que dispõe sobre o direito de crianças e adolescentes em ambientes digitais), entende-se como mais eficaz a criação de barreiras regulamentares à disseminação de conteúdo ilícito, abusivo ou impróprio pelos órgãos fiscalizadores, que devem agir com total independência e poder de polícia. Logo, evitando-se proibir, impedir ou limitar todo e qualquer tipo de acesso para crianças, observado que há conteúdos que podem ser educativos e não representem risco. Nesse sentido, manifesta-se especial atenção aos jogos disponíveis online, em especial jogos de aposta com alto caráter viciante e prejudicial. Em matéria da BBC News (https://www.bbc.com/portuguese/articles/c033r0p2z76o) foi levantado que "Jogo do tigrinho e outros cassinos online contratam influenciadores mirins e direcionam propaganda para crianças no Instagram". Este tipo de abordagem deve ser veementemente coibido e penalizado pelas autoridades públicas e plataformas e responsáveis legais devem ser penalizados conforme a gravidade das consequências danosas em crianças e adolescentes que, conforme noticiado, estão ficando viciadas nos jogos, havendo casos inclusive de suicídio infantil (fonte: https://noticias.uol.com.br/opiniao/coluna/2024/07/02/criancas-e-adolescentes-so-jogam-o-tigrinho-porque-o-instagram-deixa.htm). ","705523":"Devem ser observados os mesmos parâmetros aplicáveis à base legal do consentimento, em especial no que concerne ao disposto no art. 5º, XII e art. 8º ambos da LGPD. Ainda, um ponto de atenção em relação à obtenção do consentimento "específico" deve ser quanto à finalidade pretendida: havendo finalidades distintas, deverá haver a ciência e a autorização do responsável para cada finalidade pretendida. Por fim, "em destaque" demonstra a preocupação do legislador em separar de modo claro e visível o consentimento para tratamento de dados pessoais de crianças. Assim, havendo a aplicação da base legal de consentimento, e sendo necessário, portanto, o consentimento dos responsáveis, esse deve ser dado para uma única finalidade específica e determinada, bem como deverá ser apartado de eventuais autorizações que se façam necessária por motivos diversos. Em suma, o consentimento deverá abordar de modo claro e de fácil compreensão da finalidade do tratamento dos dados a serem informados. Casos de obtenção de consentimento com textos informativos de difícil leitura, confusos ou ambíguos devem ser evitados. ","708742":"Entende-se que não deve ser determinada uma metodologia ou ferramenta

específica para efetivação de consentimento válido dos responsáveis, tendo-se em vista a variedade de ferramentas que podem ser desenvolvidas para este fim. Contudo, deve ser evidenciado por meio de autenticação tecnicamente efetivo, que de fato foram os responsáveis daquela criança que consentiram com o tratamento. Desse modo, meios com duplo fator de autenticação em que sejam, por exemplo, utilizados apenas o documento do responsável ou um envio de token para um número de telefone, que a criança pode facilmente acessar, devem ser desconsiderados. ","708745":"Entende-se que não é necessário observar as disposições do direito civil a respeito das capacidades civis seguindo a regra geral de representação e de assistência de pais ou responsáveis. Assim, compreende-se que seja mais razoável haver um balanceamento dos riscos do tratamento de dados e do benefício e melhor interesse do adolescente. Tratamentos com baixo risco, com poucos dados pessoais e que seja facilmente evidenciado o benefício ao adolescente não devem exigir a chancela de seus responsáveis, pois a depender do contexto socioeconômico poderia dificultar o acesso do adolescente a determinado benefício proporcionado no ambiente digital. Casos específicos em que haja o tratamento de dados pessoais sensíveis, excesso de tratamento de dados pessoais, ou ainda, conteúdos com certo grau de violência, sexo e drogas, devem observar a classificação indicativa de competência do Ministério da Justiça e Segurança Pública, podendo ser exigido o consentimento dos pais/responsáveis legais. ","705539":"Estímulos viciantes devem ser proibidos. Medidas de aviso de tempo decorrido/bloqueio de permanência na plataforma a partir de determinado período, avisos visíveis alertando sobre o risco do uso excessivo e recomendações de boas práticas de uso podem ser mecanismos ofertados ao usuário de forma obrigatória pelos fornecedores do serviço. Outra sugestão é a possibilidade de oferecer para os próprios pais ou responsáveis ferramentas para monitorar o uso da plataforma por seus filhos, definir limites de tempo de uso e restringir o acesso a determinados conteúdos. Salvaguardas como a criteriosa fiscalização do governo com aplicação de multas com caráter pedagógico-punitivo para plataformas que não consigam controlar o uso de crianças abaixo da classificação indicada, publicidade direcionada, ainda que, ao caso específico de redes sociais, seja feito pelos próprios perfis de usuários e, ainda, a penalização de responsáveis legais que permitam a divulgação desse tipo de publicidade por meio do perfil de crianças e adolescentes sob sua responsabilidade. Outro tipo de salvaguarda é a promoção de campanhas educativas pelo governo federal com ampla divulgação nacional. Todas as ações de marketing ou publicidade deverão seguir as disposições legais já existentes acerca do tema, como por exemplo, mas não limitado, as estipuladas pelo CONAR, CONANDA, ECA e CDC. Vale pontuar sobre o estudo “Publicidade Infantil na TV Paga – Monitoramento 2020”, realizado pelo instituto Alana, que alerta sobre o alto índice de publicidade infantil em 4 canais de TV paga. Esse estudo serve de alerta para como hoje as autoridades públicas lidam (ou não lidam) com a questão da exposição da publicidade para crianças. Entende-se que muitas medidas de adequação podem ser adotadas por instituições detentoras de plataformas e aplicações, contudo, não haverá muito resultado na propositura dessas medidas, se os órgãos fiscalizadores não exercerem seu papel e tutelar o melhor interesse de crianças e adolescentes. ","708762":"Preliminarmente, é importante ressaltar que não existe uma solução única: a melhor abordagem dependerá das características específicas da plataforma, da finalidade do tratamento, do público-alvo e dos recursos disponíveis.

Entende-se que a combinação de diferentes técnicas pode ser uma medida mais eficaz, como, por exemplo, a combinação de métodos online e offline, podendo oferecer um nível mais alto de segurança e confiabilidade. Outro ponto a ser considerado é que a transparência é essencial: os usuários devem ser informados sobre quais métodos de verificação de idade estão sendo utilizados e como seus dados estão sendo tratados. Feito esse disclaimer inicial, aponta-se para um único exemplo de técnica a ser utilizada: a verificação de identidade por meio de documentos oficiais de identidade, como carteira de identidade, carteira de motorista ou passaporte em conjunto com a autenticação através de contas existentes em plataformas confiáveis, como redes sociais, serviços bancários ou a própria plataforma do governo, que já possuem informações de idade verificadas. ","708764":"Quanto à natureza dos dados, para fins de jogos online, entende-se que o tratamento de dados sensíveis não é viável. Quanto as demais aplicações na internet de modo geral, entende-se que o tratamento de dados sensíveis de crianças e adolescentes deve ser avaliado com máxima cautela e observado também o melhor interesse da criança e do adolescente, de modo que não sejam tratados de forma desnecessária ou que não atendam o seu melhor interesse. Ainda, deve ser evitado por padrão o tratamento de dados de geolocalização e de navegação, excetuando-se neste último caso, de igual modo, os dados que sejam necessários às funcionalidades da plataforma. Já em relação à finalidade, esta deve ser proporcional e adequada ao tratamento, devendo ser tratados apenas os dados necessários e vinculados à finalidade que se destina, além de ser garantida a comunicação simples e acessível ao titular, ou responsável legal quanto àquele tratamento, a fim de observar o princípio da transparência.","708768":"Entende-se que as plataformas digitais devem oferecer aos pais ou responsáveis legais ferramentas para monitorar o uso da plataforma por crianças e adolescentes sob sua responsabilidade, definir limites de tempo de uso e restringir o acesso a determinados conteúdos, permitindo ainda que os pais e responsáveis configurem perfis para crianças e adolescentes sob sua responsabilidade e consigam monitorar as atividades online realizadas na plataforma. Além disso, as plataformas digitais devem disponibilizar de maneira fácil e acessível ferramentas para que os responsáveis possam ver quais dados estão sendo tratados e quais finalidades, bem como canais de comunicação claros e acessíveis para que os responsáveis legais possam tirar dúvidas, apresentar reclamações e exercer seus direitos em relação aos dados pessoais tratados. Por fim, entende-se, como uma boa prática, que é possível que as plataformas promovam campanhas de educação e conscientização sobre os riscos e benefícios do uso da internet para crianças e adolescentes, orientando os responsáveis e as crianças e adolescentes sobre o uso e como se proteger no ambiente digital. Estas campanhas podem, inclusive, serem realizadas em parcerias com escolas e instituições de ensino para oferecer programas de educação digital para crianças e adolescentes. ","708772":"Esta contribuição já foi dada de modo mais abrangente no item acima.","708775":"Não.

Contribuinte: Alessandra Rigueti Barcellos

Número: OP-744166

Data: 30/07/2024 - 12:35

Resumo: :".Temos as crianças em ONG's e igrejas que são obrigadas a oferecer o tratamento medico e psicologico.. Saúde e Politicas Publicas","708725":"..Temos as crianças em ONG's que são obrigadas a oferecer o tratamento medico e psicologico.. Saúde e Politicas Publicas","705523":"Aprovação para viajens, eventos escolares, igrejas. Batizados Encontros e Crianças e Jovens, com publicação de imagens ","708742":"aprovação de im dos pais para uso de ambiente digital","708745":"O jovem fica muito vulneravel quando dentro da autonimia","705539":".","708762":"Podemos usar a obrigação de aprovação de um dois pais. ","708764":"Devemos limitar a formação de perfil de gostos e locais mais visitados","708768":".","708772":".","708775":"Sim.. Temos que ver o tratamento de dados extremamente sensiveis, devido a fragilidade do menor, como no caso de crianças em abrigos e ONG's. O antes e o depois do tratamento,

Contribuinte: WENDEL DE OLIVEIRA BABILON

Número: OP-750306

Data: 09/08/2024 - 09:28

Resumo: :"Sugere-se que a ANPD estabeleça critérios claros para avaliar o melhor interesse em diferentes situações de tratamento de dados pessoais, indo além das hipóteses relacionadas à aplicação da base legal do legítimo interesse. Isso se justifica pelo fato do princípio do melhor interesse dever ser observado em todos os casos de tratamento de dados destas categorias de titulares, mesmo quando outras bases legais são utilizadas. Essas diretrizes são fundamentais para assegurar que as organizações compreendam os requisitos necessários para proteger efetivamente os interesses dos titulares nos mais variados contextos. Um posicionamento claro da ANPD sobre este tema não apenas fomentaria a conformidade com a legislação, mas também fortaleceria a proteção dos direitos das crianças e adolescentes, alinhando-se aos princípios de responsabilidade e transparência exigidos pela LGPD. Ao analisar as melhores práticas internacionais relacionadas à avaliação do melhor interesse , observamos que é comum as autoridades estabelecerem critérios específicos para avaliar o impacto do tratamento de dados de crianças e as medidas de mitigação necessárias, utilizando a Convenção sobre os Direitos da Criança como referência normativa. Tais diretrizes são aplicadas nos Relatórios de Impacto de Proteção de Dados voltados para crianças, conhecidos como Avaliações de Impacto sobre os Direitos da Criança (CRIAs), que se concentram nos direitos humanos das crianças. Tais avaliações de impacto são reconhecidas como uma ferramenta essencial para concretizar de forma estruturada e prática a priorização do interesse da criança, conforme estabelecido na Convenção sobre os Direitos da Criança, especialmente em seu artigo 3 . Além disso, o Comentário Geral nº 25 do Comitê da ONU destaca a importância de os Estados-Membros incorporarem o uso de CRIAs na regulamentação e no design do ambiente digital para garantir a proteção adequada dos direitos das crianças. O ICO do Reino Unido, através do “Age appropriate design: a code of practice for online services”, estabelece critérios essenciais para as empresas garantirem o melhor interesse no desenvolvimento de serviços, conforme o "Best interests of the child self-assessment" . Um dos principais critérios é considerar o impacto dos serviços nos direitos das

crianças - isso inclui proteger contra riscos de exploração, promover o desenvolvimento físico e emocional, estimular a identidade e autonomia, reconhecer o papel dos pais e respeitar a capacidade das crianças em formar suas próprias opiniões . Por fim, são oferecidas diretrizes sobre como os controladores podem identificar e avaliar os potenciais riscos associados ao tratamento de dados de crianças. Isso inclui considerar os impactos físicos, emocionais, de desenvolvimento ou materiais resultantes do uso desses dados, avaliando a probabilidade e a gravidade desses impactos de acordo com as diferentes idades e estágios de desenvolvimento das crianças, visando implementar medidas preventivas eficazes para sua proteção . ","708725":"N/A ","705523":"Inicialmente, fundamental destacar que, a partir da publicação do Enunciado CD/ANPD nº 1/2023, a ANPD consolidou o entendimento de que todas as bases legais previstas nos artigos 7º e 11º da LGPD podem ser utilizadas para fundamentar o tratamento de dados de crianças e adolescentes. Assim, o consentimento de pais ou responsáveis legais, conforme abordado nesta questão, deve ser entendido como uma base legal ordinária, sem qualquer prevalência ou superioridade em relação às hipóteses previstas nos artigos 7º e 11º da LGPD. Posto isso, com base na definição de consentimento da LGPD, o consentimento parental ou de responsáveis pode ser entendido como a manifestação livre, informada e inequívoca dos pais ou responsáveis legais, autorizando o tratamento de dados pessoais de menores sob sua responsabilidade para uma finalidade específica e determinada. Considerando o texto do §1º do artigo 14 da LGPD, devem ser somados aos requisitos também os de consentimento “específico e em destaque”. Nesse sentido, a caracterização do consentimento como específico nos parece implicar que o consentimento obtido dos pais ou responsáveis deve ser dado de forma direcionada para uma ou mais finalidades específicas . Isso significa que o consentimento deve ser solicitado separadamente para diferentes operações de tratamento, desde que elas envolvam finalidades distintas, oferecendo opções granulares que permitam aos responsáveis consentirem separadamente. O consentimento específico está intrinsecamente ligado a outro aspecto do consentimento - o de ser informado -, que estabelece a necessidade de fornecer ao titular informações claras, precisas e facilmente acessíveis sobre como seus dados serão tratados . Portanto, os agentes de tratamento devem acompanhar cada solicitação de consentimento com informações detalhadas sobre quais dados serão tratados para cada finalidade específica. Essa prática é fundamental para que pais ou responsáveis legais compreendam plenamente as implicações das decisões de consentimento em nome dos menores, de modo que estejam em posição de conceder um consentimento informado e específico , assegurando um tratamento dos dados alinhado com os interesses e a proteção dos menores. Posto isso, em relação ao requisito de específico, entendemos que é importante que a ANPD indique, de maneira clara, qual o nível de granularidade que se espera dessa manifestação – inclusive considerando as diversas plataformas que podem ser utilizadas para obtenção dessa manifestação. Considerando os requisitos legais aplicáveis, nos parece que a definição da finalidade de tratamento e a indicação de que a manifestação é dada por um responsável, em nome do menor, seriam suficientes para cumprimento das exigências e, ao mesmo tempo, não gerariam fricções profundas para as atividades dos agentes de tratamento. O termo em destaque, por sua vez, refere-se à prática de obter o consentimento de maneira clara, e de forma distinta, não sendo apenas um item em meio a condições gerais ou termos contratuais .

O consentimento deve, assim, ser obtido em um momento de destaque e em meio que garanta sua fácil identificação. Em linha com o requisito de específico, sugere-se que a ANPD defina o nível de destaque que o consentimento deve ter. Considerando que ele pode ser fornecido nos mais variados contextos, nos parece que indicação clara do consentimento solicitado e a finalidade específica do tratamento, de maneira distinta de outros termos em discussão, seria suficiente para atendimento do critério. Por fim, cumpre destacar que, para que o consentimento seja lícito, é essencial garantir que seja tão fácil retirá-lo quanto concedê-lo, a qualquer momento, pelo pai ou responsável, até o momento em que a criança atingir a idade para o consentimento digital, nessa contribuição defendida como a idade de 12 anos completos. Ao atingir a idade para dar consentimento digital, defende-se que o adolescente terá o direito de revogar o consentimento por iniciativa própria, garantindo a sua autonomia no ambiente digital . ","708742":"O artigo 14, §5°, da LGPD estipula que o controlador deve empregar todos os meios razoáveis para verificar que o consentimento foi concedido pelo responsável pela criança, levando em conta as tecnologias disponíveis. Assim, esse dispositivo enfatiza dois conceitos essenciais: "esforços razoáveis" e "tecnologias disponíveis". Para determinar as medidas que devem ser adotadas, recomenda-se adotar uma abordagem baseada em riscos, permitindo ao controlador adaptar as melhores ferramentas de acordo com os riscos inerentes ao tratamento de dados. A definição de "esforços razoáveis" para verificar o consentimento parental varia conforme o contexto da atividade e os riscos envolvidos para as crianças, não havendo um critério único e absoluto. Para analisar os eventuais riscos inerentes ao tratamento, a ANPD e os controladores podem valer-se dos critérios já estabelecidos para a definição de tratamento de alto riscos trazidos pela art. 4º, §3º, do Regulamento de aplicação da LGPD pelos agentes de tratamento de pequeno porte, além de observar, no caso concreto, aspectos como: • Tipo de serviço destinado à criança – como plataformas de hospedagem de vídeos ou imagens, serviços educacionais, serviços de saúde ou apoio social, aplicativos de mídia social que facilitam conexões com conhecidos ou estranhos, sites de jogos, plataformas de compras, entre outros. A depender do tipo de serviço e dos potenciais impactos à privacidade e à proteção dos dados da criança, os esforços a serem adotados pelos agentes de tratamento deverão ser maiores. • A disponibilidade dos dados pessoais coletados para outras pessoas – considerando se o serviço tem a natureza de publicar ou disponibilizar os dados pessoais, ou partes deles, para o público em geral, ampliando a exposição das crianças. • O tratamento adicional dos dados pessoais, incluindo se os dados coletados são compartilhados com outras organizações e os motivos para isso – por exemplo, para fins de publicidade, marketing ou criação de perfis. De toda forma, os “esforços razoáveis” devem também levar em conta a própria natureza e condição do agente de tratamento, de modo a identificar, com base nesses aspectos, qual o nível dos esforços que ele teria condições de empreender. Já, em relação ao termo “tecnologia disponível”, sugere-se que a escolha da tecnologia disponível seja elaborada por meio dos seguintes critérios: • Viabilidade: o método exigido pelo controlador deve ser tecnicamente viável, considerando o estado da arte atual. Isso significa que deve ser implementável utilizando as tecnologias existentes e disponíveis ou ser facilmente adaptável às inovações tecnológicas emergentes. • Custos: deve haver viabilidade econômica e recursos operacionais disponíveis para implementar métodos de verificação. Isso inclui não

apenas os custos financeiros diretos, mas também os esforços operacionais e administrativos relacionados. Ao sugerir tais critérios, objetiva-se estabelecer a necessidade de um equilíbrio entre os métodos empregados para verificar o consentimento parental e os potenciais riscos envolvidos na atividade de tratamento de dados. Este princípio é importante para garantir que os procedimentos de verificação sejam eficazes sem impor ônus desnecessários aos responsáveis pela obtenção do consentimento, ou infringir os princípios da finalidade, da necessidade e da adequação. ","708745":"O art. 14, §1º, da LGPD estabelece que o consentimento parental é necessário para o tratamento de dados de crianças, definidas pela legislação brasileira como indivíduos de até 12 anos incompletos (art. 2º, caput, do ECA), excluindo os adolescentes de sua redação. Ainda que o tema tenha sido posteriormente detalhado no Enunciado CD/ANPD nº 1/2023, que tratou da possibilidade de uso de outras hipóteses legais, entendemos ser possível inferir que maiores de 12 anos podem consentir por si mesmos sem a necessidade da intervenção de pais ou responsáveis legais, desde que esse processo respeite os requisitos legais aplicáveis. Por outro lado, o regime de capacidade civil estabelecido pelo Código Civil considera os menores de 16 anos como absolutamente incapazes, demandando ações específicas para eliminação de tal incapacidade (conforme previsto no art. 5º, parágrafo único, do Código Civil). Essa aparente discrepância entre as disposições legais torna imperativa uma interpretação sistemática das regras estabelecidas pela LGPD em relação ao consentimento parental para sua correta aplicação. Essa interpretação deve ser guiada não apenas pelo princípio do melhor interesse, mas também pela progressiva autonomia dos titulares de dados. Neste sentido, entendemos que a possibilidade de adolescentes manifestarem sua vontade de forma autônoma quanto ao uso de seus dados pessoais está alinhada com o princípio da autonomia progressiva. Esse princípio deriva do reconhecimento de que crianças e adolescentes são sujeitos plenos de direitos, devendo ter participação significativa nas decisões que afetam seus planos de vida, especialmente no ambiente digital. O princípio defende que, à medida que os adolescentes desenvolvem maturidade e discernimento, devem ser capacitados gradualmente a tomar decisões autônomas sobre questões que impactam diretamente suas vidas, como o tratamento de seus dados pessoais. Esse princípio encontra respaldo no artigo 12 da Convenção sobre os Direitos da Criança de 1989, tratado internacional incorporado ao ordenamento jurídico brasileiro, que assegura aos adolescentes o direito de expressar suas opiniões sobre todos os assuntos que lhes dizem respeito, considerando sua idade e maturidade. O princípio da autonomia progressiva não busca abolir o regime de incapacidades aplicável a crianças e adolescentes, mas sim incorporar novas premissas que reconhecem a capacidade desses indivíduos de tomar decisões jurídicas vinculativas sobre suas próprias vidas . Ele destaca que as capacidades de compreender, escolher e querer refletem o contínuo desenvolvimento da pessoa, que, como detentora de direitos fundamentais inalienáveis, deve ser capacitada a exercê-los plenamente, sem obstáculos legais ou práticos que restrinjam seu exercício , incluindo o direito à autodeterminação informativa, que é um dos alicerces da disciplina de proteção de dados. Além disso, é importante destacar a crescente participação dos adolescentes na internet, onde frequentemente exercem direitos relacionados à sua personalidade. Eles devem ter a liberdade, por exemplo, de consentir com o tratamento de seus dados pessoais para buscar informações sobre educação sexual ou para se informar sobre

o combate à violência doméstica, sem depender do consentimento dado por suas mães, pais ou responsáveis. Esse posicionamento é reforçado pela ONU em seu Comentário nº 25 , que orienta os Estados a promoverem a conscientização para respeitar a crescente autonomia e necessidade de privacidade das crianças, à medida que estas desenvolvem progressivamente suas capacidades. O objetivo é alcançar um equilíbrio adequado entre a proteção da criança e a sua emergente autonomia, pautado na empatia e no respeito mútuo, ao invés de recorrer à proibição ou ao controle excessivo. Assim, sugere-se que, com base no princípio da autonomia progressiva, a idade para consentimento digital no Brasil - ou seja, o limite a partir do qual os adolescentes podem consentir independentemente para o tratamento de seus dados pessoais - seja estabelecida em 12 anos completos, aplicando-se a todos aqueles considerados adolescentes. ","705539":"O ambiente digital não foi originalmente desenvolvido para crianças e adolescentes, porém é inegável a sua relevância para o desenvolvimento dessas pessoas. Portanto, ao tratar do melhor interesse, é necessário considerar todos os seus direitos no ambiente digital, incluindo o de livre acesso às informações, mas, igualmente, a proteção de sua privacidade e de seus dados pessoais. É necessário pensar que independente do serviço oferecido por plataformas, em razão da própria essência da internet, há a possibilidade de que crianças e adolescentes as acessem em algum momento. Assim, ao considerar essa possibilidade ainda na fase de design, as plataformas poderão planejaram um produto ou serviço que também respeite os direitos e liberdades da criança ou do adolescente de aprender, desenvolver e explorar o ambiente online de forma própria e segura, em linha com seu melhor interesse . Afinal, é preciso levar em conta que incorporar medidas de design no início do projeto é mais fácil do que incorporá-las quando o produto ou sistema já estiver lançado e acessível ao público. Ainda, é importante atenção ao princípio da transparência. Uma das dificuldades de novas tecnologias é buscar uma forma mais clara, direta e transparente de explicar aos titulares o que está sendo feito com seus dados, quais os riscos e salvaguardas implementados, e como exercer seus direitos. Tais pontos se tornam mais difíceis quando consideramos o uso dessas plataformas por crianças e adolescentes, que mesmo levando em conta sua autonomia progressiva, ainda apresentam diferenças na capacidade de compreensão da importância dos seus dados quando comparados com adultos. Assim, é necessário buscar formas de garantir que a informação seja transmitida de forma que a criança ou adolescente possam entender sobre seus direitos e as consequências do tratamento dos seus dados, com clareza e facilidade de acesso. Quanto as recomendações a serem adotadas, podemos observar as estratégias recomendadas pela Agencia de Acceso a la Información Pública da Argentina (AAIP) para evitar que crianças tenham acesso a conteúdos inadequados em plataformas digitais, tais como: (i) promoção do acompanhamento contínuo e seguro do acesso de menores ao ambiente digital pelo grupo familiar; (ii) estabelecimento de mecanismos de limitação e controle de acesso a dispositivos; (iii) utilização de motores de busca em aplicações com conteúdo exclusivo para crianças e controle parental; (iv) pré-configuração de privacidade e segurança de aplicativos, e; (v) verificação da idade recomendada para o uso de plataformas e a leitura atenta dos termos e condições . Tais recomendações podem ser aproveitadas tanto como medidas de conscientização para pais e responsáveis, como para o incentivo à criação de ferramentas que facilitem esses mecanismos de segurança para os agentes de tratamento de dados.

","708762":"Atualmente, a Organização Internacional de Normatização (ISO) está em processo de desenvolvimento de um documento que determina o padrão internacional para sistemas de verificação de idade. Pela primeira versão disponível do documento , é possível obter uma compreensão geral de como a comunidade internacional vê e o que se espera desses sistemas. O documento se refere a essas ferramentas de verificação de idade como sistemas que podem ser fornecidos e operados por provedores específicos de serviços de identidade, ou operados internamente por empresas que tenham produtos, conteúdo ou serviços com restrição de idade. Dentre as funcionalidades, se espera que possuam mecanismos que integrem bases de dados de diferentes sistemas para verificação de idade, análise comportamental, identificadores biométricos, e formas de obtenção de consentimento dos pais ou responsáveis. Assim, é necessário expandir o que se considera como finalidade legítima para o tratamento de dados de crianças e adolescentes, ampliando a aplicabilidade do art. 14, §3º, da LGPD e reconhecendo a verificação de idade como uma medida necessária para garantir a segurança da criança, aumentando o leque de possibilidade de tratamento dos dados voltados para essa finalidade. Para determinar corretamente a idade do usuário que utiliza da plataforma, é necessário estabelecer medidas eficazes de verificação de idade. Ao estabelecer uma visão ampla sobre a necessidade de coleta de certas informações de verificação de idade para garantia da segurança e funcionamento da plataforma, é possível realizar essa verificação por meio da autodeclaração com a apresentação de documentos exclusivos de maiores de idade. Outra forma, conforme abordado anteriormente, é o uso de plataformas terceiras que realizam a verificação de idade, como a necessidade de login pela plataforma gov.br, que já possui dados suficientes que comprovam a idade daquele usuário como adulto . Necessário, de toda forma, considerar o contexto de cada atividade e de cada agente de tratamento envolvido, de modo que as medidas exigidas não se tornem excessivamente custosas ou prejudiquem tecnicamente o serviço oferecido. Em linha com a abordagem baseada em riscos mencionada nos itens anteriores, alguns fatores podem ser levados em conta para definir a necessidade de mecanismos de verificação mais ou menos robustos – por exemplo: - Número de usuários; - Natureza do produto/serviço e tipos de dados utilizados; - Possíveis impactos negativos aos titulares de dados pessoais como decorrência do uso do produto/serviço. Tais fatores devem, ainda, ser avaliados em conjunto com as boas práticas de governança adotadas pelo próprio agente de tratamento, criando assim um cenário que possa conferir mais segurança e previsibilidade em relação às atividades de tratamento realizadas e possíveis impactos aos menores.
","708764":"Primeiramente, é importante destacar que o art. 14, §4º, da LGPD está fundamentado pelo princípio da necessidade que rege a proteção de dados no Brasil. Esse princípio, estabelecido no art. 6º, III, limita o tratamento de dados ao necessário para a finalidade proposta pela atividade, visando reduzi-lo ao mínimo possível . Nessa linha, o citado § 4º proíbe, com base nesse princípio, que as plataformas que realizem o tratamento de dados de crianças e adolescentes condicionem a participação no serviço ao fornecimento de informações pessoais além daquelas estritamente necessárias para a atividade. Com isso, as plataformas possuem uma clara limitação referente ao que elas podem requisitar como informações obrigatórias, por exemplo, para a criação de uma conta em determinado serviço. Por um lado, esse parágrafo é relevante para garantir o cumprimento do princípio da

necessidade, visando reduzir a quantidade de dados tratados. Por outro lado, estabelecer uma visão excessivamente restritiva sobre o tratamento de dados de crianças e adolescentes inviabiliza o uso de certos mecanismos para que as plataformas possam verificar de forma adequada a idade do usuário de seus serviços, como, por exemplo, o uso de perfis comportamentais. A formação de perfis comportamentais pode ter diferentes finalidades. Em geral, quando se traça um perfil comportamental de um titular adulto, ele é utilizado para atividades legítimas de marketing direcionado, obtenção de dados de inferência para criar um perfil demográfico, entrega de conteúdo personalizado, entre outros fins comerciais. Para além dessas finalidades, é relevante considerar que esses dados podem ser utilizados para aferir a idade do usuário e garantir a segurança de menores. Conforme exposto anteriormente, as medidas para verificação de idade do usuário são essenciais para garantia da segurança de uma criança em plataformas online. Dentre as formas para verificação de idade, uma das medidas eficazes é a criação e análise de perfis comportamentais dos usuários para averiguar, pelo tipo de conteúdo consumido, se aquele usuário é ou não uma criança, configurando uma medida de salvaguarda em casos em que a criança ultrapasse os primeiros sistemas de verificação de idade. Apesar de não ser uma parte essencial para o funcionamento da atividade, devemos considerar que medidas de segurança como a criação de um perfil comportamental do usuário são necessárias para a garantia da segurança de eventual usuário menor. Assim, é totalmente compreensível que as plataformas condicionem a participação no serviço à criação de um perfil comportamental que tenha a finalidade de verificar a idade de um usuário, adotando uma visão mais ampla do princípio da necessidade para abarcar medidas de segurança essenciais ao funcionamento da plataforma em conformidade com a LGPD, principalmente no que se refere ao art. 14, bem como em atenção ao princípio do melhor interesse. Dessa forma, uma das limitações possíveis para a coleta desses dados é estabelecer uma diferenciação entre a criação de um perfil comportamental de um adulto e o de uma criança. Quando identificado um perfil infantil, a conta poderia, por exemplo, ser “marcada” e o perfil comportamental criado não forneceria nenhum tipo de conteúdo impróprio ou que não seja seguro para menores, como publicidade voltada para adultos ou conteúdo que os ponha em risco. Já para os perfis “não marcados”, as disposições sobre criação de perfis comportamentais permaneceriam abertas, porém tendo o dever constante de avaliar se aquele usuário não é um menor de idade utilizando o serviço de forma indevida. ","708768":"De início, é importante destacar que o controle parental deve ser aplicado em intensidades compatíveis com as idades da criança e do adolescente, sempre em respeito ao seu grau de autonomia e discernimento, bem como seus processos de desenvolvimento. Assim, entende-se como medida adequada a de conferir espaços de liberdade e privacidade para o menor, inclusive no meio digital, para que haja o devido desenvolvimento de sua autonomia e comunicação, com um equilíbrio entre seu exercício de direitos em ambientes apoiados e sua segurança online. Conforme estudo de 2018 que analisou 75 aplicativos de celular, foi constatado que 89% deles apresentavam medidas excessivas de monitoramento e restrição, como acesso pelos pais das telas dos filhos, do histórico de navegação, das mensagens enviadas e recebidas, entre outras, todas feitas “por design" para contribuir com um ambiente em que as crianças estejam sendo sempre monitoradas e com falta de um ambiente suficiente privado para seu desenvolvimento pessoal. Dessa forma, é preciso buscar

estratégias que ampliem o controle parental sobre o tratamento dos dados de crianças e adolescentes, sem criar um ambiente hostil de constante fiscalização por parte deles. Nesse sentido, o Código de Boas Práticas para serviços online em relação ao tratamento de dados de crianças e adolescentes elaborado pelo ICO do Reino Unido, ao recomendar estratégias de controle parental, ressaltou a importância de que a criança ou o adolescente sejam devidamente informados, de forma clara, que tais medidas estão sendo utilizadas, e que ferramentas de monitoramento ou rastreamento estão em uso. Estratégias como essa estabelecem um equilíbrio entre o controle parental e o respeito à privacidade do titular, desenvolvendo um ambiente de confiança no uso da tecnologia . Outra maneira de possibilitar o controle parental de forma equilibrada, por exemplo, é estabelecer ferramentas de controle para criação de contas de crianças em plataformas digitais, ampliando seu controle sobre o uso desses dados sem necessariamente ter uma fiscalização e observação contínua do ambiente de desenvolvimento dos menores. É importante destacar a imprescindibilidade de que esses mecanismos de controle parental estejam de acordo com o melhor interesse do menor e respeitem sua privacidade. No processo de desenvolvimento de uma criança ou adolescente, é essencial que existam espaços privados em relação aos pais onde eles possam desenvolver sua personalidade, criatividade e autonomia, e que aumentem progressivamente conforme a idade avance. Assim, é preciso que os mecanismos de controle parental sejam equilibrados e não abusivos, sinalizando de forma clara às crianças e aos adolescentes, por exemplo, que seus pais ou responsáveis terão acesso às informações e conteúdo de seu dispositivo, permitindo uma educação digital de cunho emancipatório, que seja pautada em responsabilidade e diálogo aberto entre pais e crianças . ","708772":"Uma das principais boas práticas deve ser a de garantir que a política de privacidade e outros textos destinados aos usuários sejam escritos em linguagem que seja compreensível não apenas pelos pais ou responsáveis, mas também para as crianças e adolescentes, quando apropriado. Assim, as plataformas devem priorizar que os textos de suas políticas de privacidade utilizem uma linguagem clara e direta que facilite o entendimento dos mais jovens, evitando, na medida do possível, o uso de termos legais e técnicos desnecessários. Além disso, deve-se considerar a criação de diferentes versões da política de privacidade para diferentes faixas etárias ou, caso haja apenas uma versão, garantir que ela seja acessível e compreensível para todas as idades. Outra prática relevante é a criação e disponibilização de sumários ou versões resumidas das principais informações sobre a coleta, uso e compartilhamento de dados. Essa abordagem permite que os usuários, especialmente as crianças e seus responsáveis, possam rapidamente entender as práticas da plataforma sem se perder em detalhes excessivos, facilitando que as informações mais relevantes sejam comunicadas de maneira eficiente e direta . Além disso, as interfaces para o consentimento e gerenciamento de dados, caso aplicáveis ao caso concreto, devem ser intuitivas e fáceis de navegar. Isso pode incluir a necessidade de criar dashboards e outras ferramentas de gestão de dados que sejam visualmente atraentes e simples de usar, considerando a possibilidade de integrar elementos como ícones, símbolos e gráficos que ajudem a explicar os processos envolvidos. É importante que essas interfaces sejam desenhadas de forma a considerar a evolução da capacidade das crianças conforme elas crescem e as necessidades especiais de pessoas com deficiência, conforme estipulado pelo art. 14, §6º, da LGPD. Finalmente, a aplicação de

métodos visuais e interativos, como diagramas, cartoons e vídeos, pode ser extremamente benéfica para engajar uma audiência jovem e assegurar que a informação sobre a privacidade seja apresentada de maneira adequada à sua idade e de forma que chame a atenção. Além disso, a incorporação de elementos como camadas de informações e avisos just-in-time pode ajudar a explicar aspectos mais complexos do tratamento de dados de maneira gradual e acessível . Em resumo, para que as plataformas digitais assegurem boas práticas de transparência no tratamento de dados pessoais de crianças e adolescentes, é necessária a criação de interfaces intuitivas e a adaptação da mensagem para diferentes idades e necessidades. Estas práticas garantem não apenas a conformidade legal, mas também a promoção de um ambiente online seguro e transparente para os usuários mais jovens e suas famílias. Necessário, de toda forma, considerar o contexto de cada atividade e de cada agente de tratamento envolvido, de modo que as medidas exigidas não se tornem excessivamente custosas ou prejudiquem tecnicamente o serviço oferecido. ","708775":"Certas questões permanecem em aberto quando falamos, de forma geral, do tratamento de dados pessoais de crianças e adolescentes. Primeiramente, é preciso esclarecer ou eventualmente estabelecer uma diferenciação eficaz entre serviços voltados para crianças e serviços em geral que podem ser utilizados por crianças. A Comissão Federal de Comércio dos Estados Unidos (FTC), por exemplo, adotou em sua Norma de Proteção de Dados de Crianças Online (COPPA) uma diferenciação entre os serviços voltados para crianças menores de 13 anos de idade e os serviços que podem ser acessados por menores de 13 anos, aplicando expectativas diferentes no tratamento de dados dos usuários quanto à coleta de informações de idade, entre outros . Ao criar uma separação entre esses dois tipos de serviço, é possível equilibrar o tratamento de dados de plataformas online e desenvolver estratégias de segurança mais específicas para serviços que tem como principal público-alvo as crianças. De acordo com o Centro para Liderança de Políticas de Informação (CIPL) , existem duas formas de observar a situação: estabelecer uma necessidade de que todos os serviços que podem ser acessados por crianças realizem a checagem direta da idade de seus usuários, ou que essa obrigação recaia apenas aos serviços especificamente voltados para menores. Ao final, o CIPL recomenda a criação de testes baseados em riscos para determinar se uma plataforma intencionalmente faz conteúdo voltado para crianças e adolescentes, o que auxiliaria a ditar se seria necessária a coleta de dados referentes à idade de todos os usuários ou não. Analisando o cenário internacional, é perceptível que essa discussão é de alta relevância quando se discute o tratamento de dados de crianças. Assim, é necessário que a ANPD aborde tal tópico como uma forma de equilibrar o tratamento de dados por plataformas online, estabelecendo uma maior diferenciação acerca dos limites no tratamento de dados para diferentes serviços.

Contribuinte: FERNANDO BOUSSO

Número: OP-750584

Data: 12/08/2024 - 08:33

Contribuinte: Patrícia Leal Ferraz bove

Número: OP-750587

Data: 12/08/2024 - 08:43

Resumo: :"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Considerando que o princípio do melhor interesse da criança e do adolescente já está previsto no art. 14, caput, da LGPD, no Enunciado CD/ANPD nº 1 bem como na Convenção Internacional dos Direitos da Criança, tendo interpretação extensiva de seu conteúdo, visando ao bem-estar do menor, não identificamos a necessidade de regulamentação específica pela ANPD sobre o referido princípio. Eventual regulamentação específica poderia desencadear disposições conflitantes, restritivas e/ou taxativas e dúvidas na sua implementação. Não obstante, além da previsão de que tal princípio deve ser avaliado "no caso concreto", contida no Guia Orientativo das Hipóteses Legais de Tratamento de Dados Pessoais baseado no Legítimo Interesse, parece-nos que a ANPD poderia tratar do tema em guia orientativo específico sobre a aplicação do princípio do melhor interesse em diferentes contextos do tratamento de dados pessoais de crianças e de adolescentes e com outras bases legais. O guia orientativo, estudo ou outro documento de orientação da ANPD, elaborado com a contribuição da sociedade, poderia abordar situações de forma mais objetiva sobre tal conceito, com exemplos práticos de sua aplicação indicando o melhor interesse da criança e do adolescente. Sugerimos como exemplos que poderiam ser abordados como adequados ao seu melhor interesse os tratamentos que buscam proteger o próprio titular e terceiros, como no caso de prevenção a fraudes e verificação e proteção de identidade, além de indicar que, no contexto da LGPD, o melhor interesse não deve ser considerado atendido apenas em situações de proteção de direitos/interesses ou de prestação de serviços que os beneficiem, mas também em situações em que o tratamento não gera qualquer prejuízo para as crianças e os adolescentes. O melhor interesse da criança é um conceito dinâmico que requer uma avaliação apropriada ao contexto específico, levando em consideração a variação de maturidade e compreensão desse público e preservando a segurança da criança e do adolescente, inclusive no contexto digital. Nessa linha, tal documento também poderia abordar diretrizes para a avaliação prática do melhor interesse, ponderando os direitos e interesses do controlador, inclusive em fornecer produtos e/ou serviços a esse público e os interesses e direitos de terceiros. ","708725":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Como mencionado na resposta anterior, entendemos que situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que podem demandar maior atenção e detalhamento do princípio do seu melhor interesse, tais como aqueles em que o tratamento é direcionado exclusivamente a tais públicos, podem ser tratados pela ANPD por meio de orientação, ao invés de regulamentação. A temática demanda análise do caso concreto e a ponderação de diferentes interesses, direitos, critérios e situações. De forma não exaustiva e exemplificativa, citamos alguns exemplos de situações que podem ser abordadas: (i) os casos em que o melhor interesse está voltado única e exclusivamente ao interesse/benefício dos pais ou responsáveis, e não do menor; (ii) as situações já abordadas no Guia de Orientação do Legítimo Interesse, com os ajustes que propusemos anteriormente à ANPD sobre o referido documento e que reiteramos nesta

oportunidade, como coleta de dados em rede wi-fi de escola, utilização de dados para publicidade e marketing direcionados para esses públicos e câmera de segurança em shopping center; (iii) aplicativos e jogos digitais voltados para esses públicos, considerando a coleta excessiva de dados, exposição a conteúdos inadequados e práticas que exploram a vulnerabilidade das crianças; (iv) mídias sociais, considerando a privacidade e segurança de dados, cyberbullying e impacto sobre a saúde mental e emocional desses públicos; (v) tratamento de dados pessoais sensíveis relacionados à saúde. De qualquer forma, importante destacar que, em geral, os tratamentos de dados de crianças e adolescentes são totalmente alinhados com o tratamento de dados de demais titulares e não demandam atenção específica somente por envolverem dados de crianças e adolescentes. Por exemplo, há situações em que o tratamento de dados é necessário, por exemplo, para fins de prevenção a fraudes, prevenção a lavagem de dinheiro e cumprimento de obrigações legais e regulatórias, inclusive com o tratamento de dados biométricos, assim como é feito para outros titulares. Referidos tratamentos são alinhados ao melhor interesse da criança e do adolescente e são extremamente necessários, inclusive para prevenir que os dados pessoais de menores sejam usados por terceiros mal intencionados expondo, indevidamente os titulares. Além disso, existem situações em que o agente de tratamento não tem conhecimento prévio de que os dados pessoais tratados são de crianças ou de adolescentes, o que não deve, por si só, configurar como em desacordo com o melhor interesse do menor. Em outras situações, é preciso tratar o dado do menor para não realizar tratamentos para determinadas finalidades, o que também é considerado adequado e no seu melhor interesse. De modo geral, aspectos importantes a serem considerados nessas situações e contextos são a aplicação indispensável de outros princípios previstos na LGPD, como o da finalidade, minimização e segurança. Além dos contextos acima citados, há de se dar atenção ao design e desenvolvimento de serviços online que podem ser acessados por crianças e adolescentes de forma que facilitem o seu entendimento e compreensão relativos ao uso dos seus dados pessoais. Considerando um design específico e simples para esse público, no caso de aplicações destinadas exclusivamente a eles, casos que demandem uma avaliação dos pais ou responsáveis, podem gerar um debate no ambiente familiar promovendo a educação digital.
","705523":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Conforme o Enunciado CD/ANPD nº 1/2023, os dados de crianças podem ser tratados por quaisquer bases elencadas nos artigos 7º e 11 da LGPD, desde que observado o melhor interesse do menor e, portanto, o entendimento do §1º do Art. 14 da LGPD aplica-se aos casos em que o tratamento seja realizado com fundamento na base legal do consentimento. Entendemos que devem ser observados os mesmos parâmetros e critérios já estabelecidos para a coleta de consentimento para tratamento de dados pessoais dos “demais titulares”, maiores de idade. O consentimento “específico e em destaque” previsto no mencionado dispositivo legal visa enfatizar a necessidade de consentimento de um dos pais ou do responsável legal pela criança. De qualquer forma, quanto aos parâmetros no caso de obtenção de consentimento para o tratamento de dados de crianças devem ser observados: transparência e informação suficiente, acessível, adequada e em destaque das demais cláusulas sobre o consentimento, a finalidade do tratamento e outras informações relevantes, inclusive que contenha também as informações sobre a impossibilidade da prestação do

serviço/execução do contrato caso não haja tal consentimento, por exemplo, se for o caso. Ainda, o consentimento poderá ser revogado a qualquer momento, o que também pode ser informado de maneira clara aos pais/responsáveis. Além disso, é importante que se sabia que o consentimento foi dado por um dos pais ou responsáveis legais. Tal identificação pode ser feita a critério do controlador ou do agente que coleta o consentimento, podendo envolver o cadastro e/ou confirmação de identidade, verificação de documentos ou outros meios utilizados pelos agentes de tratamento. Tal ponto é relevante também considerando a possibilidade de a criança se fazer passar pelos pais ou responsável e dar o consentimento. ","708742":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Entendemos que os esforços previstos na LGPD são os razoáveis, considerando meios adequados e viáveis para a obtenção e verificação de que o consentimento foi fornecido por um dos pais ou responsável pela criança. Dessa forma, a adoção de esforços que sejam inviáveis ou demasiadamente onerosos não deve ser exigida dos agentes de tratamento. Nessa linha, existem meios diversos que os agentes de tratamento podem adotar a seu critério, sendo esses não cumulativos e exemplificativos: (i) realização de cadastro em nome do menor e de um dos pais ou responsável; (ii) validação do consentimento via Token ou push, enviado ao e-mail, celular ou aplicativo de um dos pais ou responsável; (iii) envio do documento da criança e de um dos pais ou responsável; (iv) envio consentimento ou autorização assinada por um dos pais ou responsável; (v) consentimento de um dos pais ou responsável coletado por telefone; (vi) processamento de pedidos online por meio do cartão de crédito dos pais ou responsáveis legais; (vii) após informar a idade, se for o caso, fornecimento do seu endereço de e-mail e do endereço de e-mail dos pais ou responsáveis de modo que tanto o titular dos dados como os pais/responsáveis recebem um e-mail automático solicitando a confirmação do consentimento dos pais/responsáveis para o tratamento dos dados pessoais do menor de idade; (viii) dar transparência quanto à necessidade de consentimento dos pais ou responsáveis para tratamento de dados de criança durante a "jornada" de coleta dos dados pessoais e do consentimento é uma forma adequada de garantir a observância dos princípios legais; (ix) além dos dados cadastrais da criança, nos casos dos pais, a verificação de dados de identificação. No caso de representantes legais desconstituídos do poder familiar, além do documento de identidade, mostra-se pertinente a procuração; (x) obtenção do consentimento e/ou confirmação realizada por um dos pais ou pelo responsável em ambiente seguro, com acesso mediante utilização de senha, pessoal e intransferível; (xi) uso de Tecnologias de Verificação, tais como assinaturas digitais, tokens, reconhecimento facial, ou outras formas de verificação eletrônica que viabilizem o reconhecimento legítimo de quem concedeu o consentimento; (xii) autenticação de Identidade, sendo que há vários processos possíveis, tais como como autenticação em duas etapas (2FA), uso de certificados digitais ou login e senha. Outros pontos importantes que os controladores podem adotar, a seu critério, são a rastreabilidade do consentimento, mantendo registros dos consentimentos fornecidos e realizar processos de verificação sobre a conformidade dos processos de obtenção de consentimento. Importante ter em conta que nenhum processo ou mecanismo é infalível. Em última análise, é importante que os pais e responsáveis orientem e previnam ações por parte dos menores e que haja informação de que, eventualmente, o respectivo responsável responderá perante qualquer manifestação falsa do menor.

","708745":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Nos parece possível, em observância ao princípio do melhor interesse e considerando a autonomia progressiva dos adolescentes (conforme idade definida na legislação aplicável) que haja a possibilidade de dispensa de representação ou assistência dos pais ou responsáveis legais para concessão do consentimento, quando esta for a base legal aplicável ao tratamento de dados pessoais. Nesse sentido, é possível verificar a autonomia dos adolescentes em alguns cenários da vida civil, como, por exemplo, na possibilidade de votarem nas eleições nacionais, estaduais e municipais, casarem-se sem a autorização de representante legal, e de viajarem sem os pais e/ou representantes legais por todo território nacional, apenas com a apresentação do documento de identificação. Além disso, o Código Civil corrobora com esse entendimento, ao possibilitar aos adolescentes de 16 a 18 anos praticarem atos da vida civil. Portanto, os adolescentes poderiam fornecer o consentimento para o tratamento de seus dados, uma vez que já dispõem de meios de exercer certos direitos e atos da vida civil, além de não haver renúncia a seus direitos, uma vez que podem revogar o consentimento a qualquer momento. Assim, para as situações em que se pretende tratar dados pessoais de adolescentes, deve ser avaliado o contexto e a situação para entender se existe a necessidade de consentimento de um dos pais ou responsável ou alguma situação de representação ou assistência dos pais ou responsáveis legais. Por exemplo: 1) Um site destinado exclusivamente para adolescentes, com conteúdo de história, geografia e recursos para atividades escolares, possibilita a assinatura de um newsletter educativo, através do envio do nome e e-mail do adolescente. Neste caso não deveria ser necessária a representação ou assistência dos pais ou responsáveis legais. 2) Feiras de Estágio: para os casos de inscrição de adolescentes entre 16 e 18 anos em feiras de estágio não deveria ser necessária a representação ou assistência dos pais ou responsáveis legais. Ainda, citamos como exemplo o disposto no GDPR – General Data Protection Regulation, em seu capítulo II, que muito embora tenha disposição distinta da LGPD, menciona que no caso de consentimento em relação à oferta direta de serviços da sociedade da informação às crianças, o consentimento dado por adolescentes de pelo menos 16 anos é válido, devendo ser dado ou autorizado pelos titulares das responsabilidades parentais das crianças se tiverem idade abaixo de 16 anos. Ainda, os Estados Membro poderiam definir idade menor, desde que não inferior a 13 anos. Nessa linha, entendemos que pode haver situações em que a autonomia progressiva dos titulares seja considerada para dispensar a necessidade de consentimento prevista no §1º do art. 14 da LGPD por parte de um dos pais ou responsável legal, hipóteses que poderão ser melhor descritas e orientadas pela ANPD, podendo configurar importante ação para assegurar o pleno desenvolvimento de sua personalidade e formação cidadã. ","705539":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Muito embora o conceito de plataforma digital não esteja claro, entendemos, inclusive pelo disposto na explicação introdutória deste capítulo III, que se trata de redes sociais, jogos e outras plataformas de entretenimento ou outras aplicações destinadas ou mais utilizadas por crianças e adolescentes. Nessa linha, entendemos que serviços financeiros e aplicações de serviços financeiros, muito embora possam ser usados por esses públicos, não são prioritariamente destinados a esses públicos ou para o seu uso constante ou com superexposição de usuários, tal como indicado acima no texto introdutório deste capítulo III. Com este conceito em mente, ou seja, no caso

de plataformas digitais destinadas ou prioritariamente usadas por tais públicos, sem necessidade de padronização, é importante que os agentes de tratamento implementem medidas de segurança adequadas aos padrões de mercado para proteger os dados pessoais de menores de idade contra acesso não autorizado, vazamento e outras ameaças. Assim como para os tratamentos de dados pessoais de adultos, nos parece válido observar o "privacy by design" no desenvolvimento das plataformas direcionadas para crianças e adolescentes, adotando-se melhores práticas de transparência, com informações claras e acessíveis sobre o tratamento de dados, bem como de design de aplicação para que as ações tomadas pelos usuários desses públicos sejam por eles bem compreendidas. Além disso, o atendimento aos princípios da LGPD deve ser garantido, como os de finalidade, necessidade e adequação, garantindo que a coleta de dados seja limitada ao mínimo necessário para alcançar objetivos específicos e legítimos. No caso de plataformas digitais para esses públicos, ou nos dispositivos que possam ser usados por crianças e adolescentes para acessar tais plataformas, desde que viável do ponto de vista tecnológico, operacional e de negócios, é desejável a existência de controles parentais que permitam aos pais ou responsáveis monitorar e controlar o acesso e uso de seus filhos. ","708762":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. O principal ponto é a possibilidade de verificação da informação sobre a idade dos usuários. Tal verificação, especialmente em ambiente digital, pode ser feita de algumas formas, que indicamos de forma exemplificativa e não exaustiva. A sugestão não é para a sua adoção cumulativa, mas apenas trazer opções que possam ser adotadas alternativamente, a critério dos agentes de tratamento. As sugestões a seguir referem-se a opções para verificação da idade de usuários de plataformas digitais, e não de obtenção de consentimento. Nessa linha, o cadastro é um passo essencial para identificação do usuário e de sua idade. Há a possibilidade de o cadastro ser feito em nome do menor e/ou de um dos pais ou responsável com indicação de informações do menor. Sobre a verificação da idade, algumas opções são: •Implementar na jornada, seja no cadastro inicial ou em outra a critério do agente de tratamento, uma etapa de informação e/ou de verificação de idade, com o fornecimento e/ou verificação da data de nascimento ou de outra informação de identificação que permita a verificação da idade. Se a plataforma for proibida para uso a depender da idade, pode ser incluído aviso sobre tal fato com declaração sobre a veracidade da idade adequada e/ou com possibilidade de trava para continuar a depender da idade informada; •Através da coleta do CPF e da data de nascimento, também é possível checar a veracidade das informações em sites e sistemas públicos e/ou privados, inclusive em bases oficiais, como no no site Receita Federal e, com isso, confirmar a idade do titular e mitigando riscos de criação de contas em plataformas com dados falsos ou incorretos; • Comprovar a identidade da pessoa (por meio de reconhecimento facial, por exemplo) com a solicitação e verificação de documento de identidade. ","708764":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Como mencionado acima na resposta à questão 1 deste capítulo, o conceito de plataforma digital não está claro, mas consideramos como aquelas prioritariamente destinadas ou utilizadas por crianças e adolescentes, o que não inclui aplicações relacionadas a serviços financeiros. Nessas plataformas destinadas e/ou prioritariamente utilizadas por crianças e adolescentes, é importante que o controlador realize a coleta dos dados mínimos necessários, justificando a coleta de dados pessoais em sua

política de privacidade de forma adequada. Conforme destacado pelo mencionado dispositivo legal, que os controladores não deverão condicionar a participação dos titulares de que trata o § 1º do artigo 14 em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Em outras palavras, os dados coletados devem se limitar aos estritamente necessários à realização das atividades (serviço) fornecidas pela plataforma digital e não se prestem a usos que não se mostrem adequados ao melhor interesse das crianças e adolescentes titulares dos dados. Não visualizamos a necessidade de limitações específicas para a coleta de dados de crianças e adolescentes, considerando as regras já postas pela LGPD e pelo Enunciado CD/ANPD nº1, de observância do melhor interesse da criança e adolescente. Quanto ao exemplo trazido, de formação de perfis comportamentais, nos parece que, se respaldados em uma base legal legítima e observarem as diretrizes da LGPD e o melhor interesse da criança e do adolescente, não haveria limitações específicas para tal tratamento. A título de exemplo, perfis comportamentais, podem desencadear produtos e serviços mais adequados para tal público e atingirem, por consequência, o melhor interesse para estes ou ser utilizados para prevenção a fraudes e a proteção do titular. De modo geral, importante reforçar a aplicação dos princípios da LGPD, especialmente (i) finalidade específica, limitando a coleta de dados apenas àqueles necessários para a finalidade declarada; (ii) transparência e consentimento, garantindo a plena informação sobre a coleta de dados e suas finalidades, bem como que, quando seja a base legal aplicável, o consentimento seja dado conforme previsto na LGPD; (iii) dados sensíveis, efetuando a coleta de dados sensíveis somente se estritamente necessário e com fulcro em base legal adequada, considerando a natureza de tais dados; e (iv) minimização de dados, adotando práticas de minimização, coletando apenas o mínimo necessário de informações para alcançar os objetivos pretendidos. ","708768":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Um dos pilares mais importantes para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes é a educação. A educação sobre o uso do ambiente digital é essencial para trazer mais conhecimento, com o fornecimento de materiais educativos e orientações para pais e responsáveis sobre a proteção de dados pessoais e privacidade online. No caso de produtos e serviços digitais, no caso de plataformas digitais prioritariamente destinadas e/ou utilizadas por crianças e adolescentes, nos parece adequado existir um mecanismo que possibilite a visualização, controle dos pais/responsáveis e/ou alertas e notificações do que os menores estão adquirindo e utilizando na internet. Importante mencionar que determinados controles e/ou ferramentas que permitam controle parental ou espaço familiar por meio dos quais os pais e/ou responsáveis possam controlar o tempo de uso, acesso e/ou visualizar conteúdos acessados ou transações efetuadas podem ser instalados pelos próprios pais nos dispositivos utilizados por crianças e adolescentes para acesso à internet e a aplicativos, e não necessariamente são passíveis de serem implementados nas aplicações em si.","708772":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. O principal instrumento de transparência é a política/aviso de privacidade, pois traz maiores informações sobre o tratamento de dados. Além desse instrumento essencial, a critério dos agentes de tratamento, podem ser usados outros recursos para trazer essas informações de maneira mais pontual, simples, clara e acessível, seja na referência à política de privacidade

dentro de jornadas, por meio de páginas ou informações específicas, ou outros tipos de materiais com finalidade informativa e/ou educativa (tais como FAQs, vídeos e outros recursos audiovisuais, políticas/avisos de privacidade simplificados ou resumidos e/ou informações sobre o tratamento de dados pessoais adaptadas a esses públicos e seus responsáveis). Além disso, nos parece adequado observar, como boas práticas de transparência, as orientações já postas pelo ECA e pelo Conar no que diz respeito à publicidade infantil, quando for o caso. Neste sentido, no artigo 37 do Código de Ética do Conar, há os cuidados e boas práticas ao ter como interlocutor com o público de crianças e adolescentes, que podem ser adotados, quando for o caso, em comunicações sobre dados pessoais com este público. ","708775":"Contribuição conjunta encaminhada em nome da FEBRABAN e ABECS. Como indicamos anteriormente, muito embora entendamos não ser necessária regulamentação neste momento, podem ser desejáveis orientações e ações educativas da ANPD sobre o tratamento de dados pessoais de crianças e de adolescentes, especialmente no caso de novas tecnologias inovadoras. Considerando a autonomia progressiva desses titulares para lidar com os seus dados pessoais, seria de se considerar tais medidas educativas e orientativas de aspectos necessários a possibilitar uma transição consciente para a maioridade, visto a necessidade cada vez maior de cuidado com os seus dados pessoais para a garantia dos direitos fundamentais de liberdade e privacidade, bem como o desenvolvimento de sua personalidade.

Contribuinte: Arthur Gomez Villar Maruca

Número: OP-750672

Data: 12/08/2024 - 13:44

Resumo: :"O princípio do melhor interesse, embora central na proteção de dados de crianças e adolescentes, ainda apresenta lacunas que demandam maior detalhamento e regulamentação pela ANPD. Além das questões abordadas no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo, é preciso aprofundar a discussão sobre a definição concreta do "melhor interesse" em diferentes contextos, a hierarquia de valores a serem considerados, o papel dos pais e responsáveis, e os impactos a longo prazo das decisões sobre o tratamento de dados. A ANPD precisa fornecer orientações mais claras sobre como avaliar o melhor interesse em situações complexas, como o uso de inteligência artificial, a coleta de dados biométricos e o tratamento de dados de saúde de crianças.","708725":"Sim, existem diversas situações e contextos que demandam maior atenção e detalhamento sobre o princípio do melhor interesse. Por exemplo, o uso de dados de crianças em pesquisas científicas, a personalização de conteúdos em plataformas digitais, a coleta de dados biométricos para fins de identificação e a utilização de dados de crianças em marketing direcionado. Nestes casos, é fundamental que a ANPD estabeleça critérios claros para a avaliação do melhor interesse, considerando os riscos e benefícios para a criança, a necessidade de consentimento dos pais ou responsáveis, e a proteção da privacidade. Além disso, é preciso analisar como o princípio do melhor interesse se aplica a novas tecnologias e modelos de negócios que envolvem o tratamento de dados de crianças, como a internet das coisas e a realidade virtual.","705523":"- O

consentimento deve ser obtido em linguagem clara e acessível, utilizando recursos visuais e exemplos práticos para facilitar a compreensão. - Os pais ou responsáveis devem ser informados de forma completa sobre a finalidade do tratamento, os dados coletados, os destinatários e os direitos do titular. - Os pais ou responsáveis devem ter a opção de recusar o consentimento sem sofrer qualquer tipo de penalidade.","708742":"- A utilização de mecanismos de autenticação fortes para verificar a identidade dos pais ou responsáveis. - Confirmação por e-mail ou SMS: O envio de um código de confirmação para o e-mail ou número de telefone cadastrado. - A gravação em vídeo do momento da obtenção do consentimento, com a devida proteção dos dados pessoais.","708745":"- A capacidade de fornecer consentimento deve ser avaliada caso a caso, considerando o grau de maturidade e compreensão da criança. - Para adolescentes com maior grau de maturidade, pode ser considerado o assentimento, ou seja, a manifestação de concordância da criança, desde que acompanhado do consentimento dos pais ou responsáveis.","705539":"- A privacidade deve ser integrada desde o projeto das plataformas, com a adoção de medidas técnicas e organizacionais para proteger os dados pessoais. - A coleta de dados deve ser limitada ao estritamente necessário para a prestação do serviço. - Os dados pessoais devem ser anonimizados ou pseudonimizados sempre que possível. - Transparência: As plataformas devem fornecer informações claras e acessíveis sobre as práticas de coleta, uso e compartilhamento de dados.","708762":"- A verificação de idade deve ser realizada por meio da combinação de diferentes métodos, como a validação de documentos, a análise de dados de pagamento e a utilização de tecnologias de reconhecimento facial. - A verificação de idade deve ser realizada periodicamente, especialmente para adolescentes em fase de desenvolvimento.","708764":"- A coleta de dados sensíveis, como dados biométricos e dados de saúde, deve ser restrita ao estritamente necessário e com o consentimento explícito dos pais ou responsáveis. - A criação de perfis comportamentais de crianças deve ser limitada e transparente, com a possibilidade de os pais ou responsáveis acessarem e controlarem esses perfis. ","708768":"- As plataformas devem oferecer painéis de controle para que os pais possam monitorar as atividades de seus filhos, gerenciar as configurações de privacidade e limitar o acesso a determinados conteúdos. - As plataformas devem facilitar a comunicação direta entre os pais e a plataforma, para que os pais possam tirar dúvidas e solucionar problemas.","708772":"- As informações sobre a coleta e o uso de dados devem ser apresentadas em linguagem clara e simples, utilizando recursos visuais e exemplos práticos. - As informações devem ser facilmente acessíveis e atualizadas regularmente.","708775":"Sim, há diversas outras questões: Como limitar a coleta e o uso de dados pessoais de crianças para fins de publicidade direcionada? Qual o papel dos influenciadores digitais na proteção dos direitos das crianças e adolescentes, especialmente em relação à publicidade infantil? Qual o nível de transparência necessário para que os pais e responsáveis compreendam como os algoritmos (de IA) influenciam as experiências de seus filhos nas plataformas digitais?

Contribuinte: EZEQUIEL SOUZA DOS SANTOS

Número: OP-751407

Data: 13/08/2024 - 18:06

Resumo: :"Este tópico é bastante sensível para a Data Privacy Brasil, conectando-se ao nosso trabalho sobre Legítimo Interesse de 2021 e ao estudo com Alana e ADC sobre o “melhor interesse”. Nossas sugestões para a ANPD em 2023 não foram totalmente acatadas no Guia do Legítimo Interesse da ANPD. Reiteramos que o melhor interesse não é um elemento adicional em um teste de balanceamento, mas o núcleo de qualquer relação entre um controlador de dados e um titular criança ou adolescente. Defendemos uma abordagem procedimental centrada em um teste, inspirado nos mecanismos do Reino Unido e da Califórnia, denominado “Children’s Rights Impact Assessment (CRIA)”. O CRIA, criado pelo Comitê dos Direitos das Crianças da ONU, traduz o artigo 3 da Convenção dos Direitos das Crianças, priorizando o melhor interesse da criança de forma estruturada e concreta. Como destacado na nossa contribuição ao Estudo Preliminar do Guia de Legítimo Interesse da ANPD, organizações como a Digital Futures Commission estudam e propõem o uso de CRIA para o ambiente digital. Em 2021, essa organização, em conjunto com a 5Rights Foundation, lançou o relatório “Child Rights Impact Assessment (CRIA): A tool to realise child rights in the digital environment”, que revisita o uso dessa documentação e lista os principais modelos de CRIA. O governo canadense também disponibiliza um modelo de CRIA para orientar autoridades federais sobre como considerar os direitos das crianças. Importante dizer também que o Guia Orientativo foi pensado para aspectos gerais do legítimo interesse, incluindo a discussão de crianças e adolescentes como um capítulo, o que, ao nosso sentir, não seria a forma mais adequada de tratar a discussão. Essa tendência de pensar o tópico de crianças e adolescentes como um “anexo”, acabou produzindo uma lógica mais frouxa e flexível, por exemplo, para produção de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) quando há uma situação concreta de risco aos direitos fundamentais. Nós defendemos que, no caso de crianças e adolescentes, essa regra flexível do Guia Orientativo é incompatível com a gramática constitucional de proteção de crianças e adolescentes, que possui uma base normativa forte na Constituição Federal, considerando que a proteção de crianças e adolescentes é dever de todos e uma prioridade absoluta. A proteção de crianças e adolescentes requer um regime jurídico específico com obrigações robustas de mitigação e prevenção. Portanto, recomendamos que a elaboração de RIPD seja obrigatória para qualquer tratamento de dados de crianças e adolescentes, especialmente no caso de legítimo interesse. Isso permitirá mapear e reconhecer os riscos efetivamente, possibilitando mitigação ou a impossibilidade de realizar a operação de tratamento. O caso recente da Meta ilustra essa questão. Na oportunidade, a ANPD verificou que que dados pessoais de crianças e adolescentes, como fotos, vídeos e postagens, poderiam estar sendo coletados e utilizados para treinar os sistemas de Inteligência Artificial (IA) da Meta. Tal conjuntura estaria totalmente incompatível não apenas com a Constituição Federal, mas com toda arquitetura jurídica de proteção dos mais jovens. Além disso, a ANPD reforçou que a Meta deveria adotar salvaguardas e medidas de mitigação de risco para demonstrar que o tratamento de dados seria feito no melhor interesse das crianças e adolescentes, o que não foi verificado no caso concreto. A Diretora Miriam Wimmer destacou que a proteção de dados de crianças e adolescentes exige uma atuação incisiva da ANPD. Assim, a postura flexível na elaboração de RIPD não é adequada. Em nossa visão, para evitar tratamentos ilegais de dados que gerem

riscos a direitos fundamentais, como no caso da Meta, é necessária a obrigatoriedade de RIPD para qualquer operação envolvendo dados de crianças e adolescentes, especialmente sob a base legal de legítimo interesse. ","708725":"Na Data Privacy Brasil entendemos que existem algumas questões sobre melhor interesse que merecem maior detalhamento. De início, reforçamos a necessidade de uma abordagem procedimental e documentada, como o CRIA (Child Rights Impact Assessment), para entender que o controlador está, de fato, pautando o tratamento de dados pessoais pelo melhor interesse da criança. Para isso, entendemos que é de extrema relevância considerar o Estatuto da Criança e do Adolescente (ECA), que orienta a avaliação de situações reais. Deve ser analisado se a situação concreta amplia direitos fundamentais, como o direito à vida, educação e desenvolvimento pessoal, e se a mediação tecnológica e o uso de dados introduzem novos riscos que possam afetar a dignidade e liberdade futuras. Além disso, é necessário investigar se o uso de dados pessoais pode gerar novas violações de direitos e liberdades. Um exemplo ilustrativo desse contexto é a implementação de câmeras de reconhecimento facial em escolas do Paraná, utilizadas para automação das chamadas. Este caso destaca a importância de avaliar o "contexto específico de tratamento de dados pessoais" e os riscos associados. A implementação das câmeras de reconhecimento facial para automação das chamadas é um exemplo de “contexto específico de tratamento de dados pessoais” no qual a produção de riscos aos direitos fundamentais é detrimental às crianças, falhando em atingir o teste do melhor interesse no ambiente digital, nos termos da Resolução n. 245/2024 do Conanda. A coleta e o tratamento massivo de dados biométricos de crianças, realizada por meio dessas tecnologias, levantam preocupações significativas, como o risco de discriminação e desvios de finalidade. As tecnologias de reconhecimento facial podem reproduzir vieses discriminatórios e gerar inferências errôneas sobre as crianças, além de permitir o compartilhamento de dados entre órgãos públicos, o que pode aumentar o risco de acessos indevidos e desvios de finalidade. Outro ponto de preocupação é o uso dessas tecnologias para capturar emoções dos alunos, o que levanta questões sobre privacidade e os impactos psicológicos dessa prática. Uma análise mais aprofundada revela que a implementação dessas tecnologias pode não atender ao princípio do melhor interesse por várias razões. A discriminação potencial contra grupos minorizados e a possibilidade de inferências prejudiciais são preocupações centrais. O uso de dados biométricos pode cristalizar características pessoais e prejudicar o desenvolvimento livre da criança. Além disso, a vigilância contínua e a falta de regulamentação adequada podem ter efeitos negativos duradouros na saúde mental e na liberdade de expressão das crianças. Resta nítido, portanto, que a análise do melhor interesse da criança precisa de procedimentalização e documentação, pautando-se por critérios concretos. Nesse sentido, reiteramos a recomendação de realização de um CRIA e o estabelecimento de parâmetros específicos, como os que foram acima sugeridos. ","705523":"A crescente utilização das Tecnologias da Informação e Comunicação (TICs) e a crescente participação de crianças e adolescentes em ambientes digitais trazem novos desafios para a proteção desses grupos. Dados da Pesquisa TIC Kids Online de 2022 revelam que 92% das pessoas entre 9 e 17 anos têm acesso à internet, 70% baixam aplicativos e 98% jogam online, o que reforça a necessidade de uma proteção rigorosa dos dados pessoais desses jovens. O melhor interesse da criança e do adolescente, conforme o art. 14 da LGPD, deve ser priorizado no tratamento

de seus dados pessoais. Seguir esses princípios garante legitimidade e proporciona uma interação segura com produtos ou serviços. A Data Privacy Brasil defende que o consentimento para o tratamento de dados deve ser claro, específico e destinado a finalidades previamente informadas, evitando termos genéricos que possam gerar ambiguidades. O consentimento deve ser destacado dos demais termos contratuais para garantir que pais ou responsáveis compreendam plenamente o que estão autorizando, alinhando-se com os arts. 7º e 8º da LGPD. A Resolução n. 245/2024 do Conanda exige que o consentimento para o tratamento de dados pessoais de crianças e adolescentes seja livre e prévio, solicitado de forma específica e destacada, observando o grau de maturidade da criança ou adolescente. O termo de consentimento deve detalhar claramente os agentes de tratamento, dados coletados, finalidades, uso, compartilhamento, tempo de retenção e procedimentos em caso de incidentes, evitando jargões jurídicos complexos. Dada a diversidade social e linguística do Brasil, formas alternativas de consentimento, como oral ou por vídeo, podem ser consideradas onde a formalização escrita seja um obstáculo. Em comunidades onde o português não é a língua principal, o consentimento deve estar disponível em outros idiomas e dialetos locais. A acessibilidade dos termos é fundamental para que pessoas com deficiências possam compreender plenamente. O consentimento deve estar disponível em formatos acessíveis, como braille e recursos auditivos ou visuais adaptados. Além disso, controladores devem manter uma cultura de transparência, oferecendo informações claras e acessíveis sobre os dados coletados, suas finalidades, e os direitos dos titulares, como acesso, correção, anonimização, bloqueio ou eliminação de dados desnecessários, e portabilidade. Devem fornecer mecanismos que facilitem a interação e o exercício dos direitos pelos pais ou responsáveis. ","708742":"A LGPD, no § 5º do art. 14, atribui aos controladores a responsabilidade de identificar e autenticar o consentimento para proteger os direitos de crianças e adolescentes. O Comentário Geral n° 14, de 2013, do Comitê dos Direitos da Criança da ONU e a ANPD enfatizam que esse conceito deve priorizar a proteção da privacidade e dignidade das crianças, integrando-o como direito, princípio e regra processual. Para garantir essa proteção, consideramos fundamental que os controladores adotem processos claros e transparentes para a obtenção do consentimento, conforme o § 1º do art. 9 da LGPD. Esses processos devem considerar desigualdades sociais, diversidade linguística e limitações físicas e sensoriais, garantindo que pais ou responsáveis compreendam os termos. Cabe destacar que crianças e adolescentes, como titulares de dados, em nossa percepção, têm direito a uma transparência qualificada, conforme previsto no § 2º do artigo 14 da LGPD. Esse direito exige uma abordagem diferenciada, que vá além das obrigações de transparência geral aplicáveis a todos os titulares de dados. O artigo 14, especialmente nos parágrafos 2º e 6º, estipula que as informações sobre os dados coletados, sua utilização e os procedimentos para o exercício dos direitos devem ser disponibilizados de forma proativa e detalhada, mesmo na ausência de uma solicitação direta dos titulares. Essa exigência impõe aos controladores a obrigação de garantir que a transparência no tratamento de dados seja específica e destacada para esse público vulnerável, diferenciando-se das regras aplicáveis a adultos. A ANPD já ressaltou a importância dessa transparência qualificada na Nota Técnica 6/2023, criticando a generalidade das finalidades de tratamento apresentadas pela plataforma TikTok e sublinhando a necessidade de informações precisas e adaptadas às particularidades

das crianças e adolescentes. Portanto, entendemos que a transparência qualificada deve ser implementada desde o design, com diretrizes robustas que assegurem o pleno cumprimento dos direitos desses titulares. No ambiente digital, onde a autenticação pode ser desafiadora, os controladores devem adotar mecanismos robustos para verificar a idade do consentidor. Métodos como verificação via smartphone, assinatura digital e autenticação multifatorial são recomendados. Além disso, práticas recomendadas para a criação de ambientes digitais seguros incluem o uso de interfaces intuitivas, ícones visuais, vídeos explicativos e fluxos de consentimento passo a passo, como sugerido pelo relatório "But how do they know it is a child?" da 5 Rights Foundation. Nós consideramos que os controladores devem também adotar boas práticas para a criação de ambientes digitais seguros e adequados. A Agência Espanhola de Proteção de Dados (AEPD) oferece diretrizes para a verificação etária e proteção contra conteúdos impróprios, enquanto a Lei COPPA dos EUA exige práticas rigorosas para a coleta de dados de crianças abaixo de 13 anos, incluindo ferramentas precisas para obter o consentimento dos pais e notificação sobre o uso dos serviços. Portanto, consideramos que os controladores devem adotar uma abordagem multifacetada, que inclua termos de consentimento claros, verificação robusta de identidade, consideração das desigualdades sociais e linguísticas, e transparência em todos os processos. Essas medidas garantirão uma interação segura e responsável com os dados pessoais de crianças e adolescentes, alinhando-se à LGPD e às melhores práticas internacionais. ","708745":"De antemão, ressaltamos que a LGPD não existe no vácuo, mas está inserida em um contexto jurídico mais amplo, que inclui a Constituição Federal, o Estatuto da Criança e do Adolescente (ECA), o Código Civil e demais regulamentações infraconstitucionais e infralegais que visam o melhor interesse da criança e do adolescentes. Sendo assim, a Data Privacy Brasil defende que a obtenção de consentimento para o tratamento de dados pessoais de crianças e adolescentes no ambiente digital deve seguir as disposições do direito civil em relação às capacidades civis. Para jovens considerados absolutamente incapazes, ou seja, aqueles com menos de 16 anos, a regra geral é a necessidade de representação para que seja fornecido o consentimento por seus pais ou responsáveis. Já para adolescentes relativamente incapazes, que são aqueles na faixa etária entre 16 e 18 anos, o consentimento deve ser dado com a assistência dos pais ou responsáveis legais, interpretação conforme disposto no Código Civil. É importante mencionar que existem narrativas em construção de que, com base na autonomia progressiva de crianças e adolescentes, seria possível que o consentimento parental fosse "suprido" pelos próprios jovens, independentemente de assistência ou representação, posição que tendemos a discordar. Em nosso sentir, ainda é necessário um maior aprofundamento das discussões sobre a conexão entre esses dois temas (consentimento para tratamento de dados pessoais e autonomia progressiva) no caso concreto, especialmente em se tratando do ambiente digital, que possui diversos riscos sistêmicos para os mais jovens, podendo agravar a sua condição de vulnerabilidade. Merece destaque o fato de que encontramos apenas três teses de doutorado, na Biblioteca de Teses da CAPES, sobre o tema "autonomia progressiva", que tratam sobre o tema de forma aprofundada. Sendo assim, reforçamos a necessidade de aprofundamento do debate no contexto nacional sem a adoção de interpretações irrefletidas que possam colocar em risco o melhor interesse e a proteção integral dos mais jovens. A argumentação sobre "autonomia progressiva" para suprir eventual

consentimento parental não deve servir como escudo ou proteção para flexibilização de regras que envolvem tratamento de dados pessoais de crianças e adolescentes. Tal cautela é importante ao se considerar as evidências científicas sobre danos em usos de redes sociais e aplicações de Internet, tal como feito por Jonathan Haidt no seu livro “A Geração Ansiosa”. Essa também é uma discussão que está sendo amplamente debatida no cenário internacional, com a realização de investigações sobre o potencial dano à saúde causado pelas plataformas digitais, como a recente denúncia do Departamento de Justiça dos Estados Unidos, junto com a Federal Trade Comission (FTC) contra a plataforma Tik Tok. ","705539":"Para garantir a proteção do melhor interesse de crianças e adolescentes e promover a privacidade e a segurança de dados pessoais em plataformas digitais, consideramos fundamental observar diversos princípios e medidas de design. A LGPD estabelece princípios fundamentais como a finalidade, necessidade e adequação, que determinam que o tratamento de dados pessoais deve ser restrito ao mínimo necessário para realizar finalidades específicas, legítimas e informadas aos titulares, sem permitir usos posteriores incompatíveis com essas finalidades. Além disso, a transparência é essencial, exigindo que os controladores forneçam informações explícitas, precisas e de fácil acesso sobre o tratamento dos dados. Também é preciso que se leve em conta as características das crianças e utilizando recursos apropriados, conforme o parágrafo 6º do art. 14 da LGPD. No contexto internacional, regulamentos como o Age Appropriate Design Code (ICO) do Reino Unido, o código da Irlanda e a legislação da Califórnia estabelecem diretrizes importantes. O Age Appropriate Design Code impõe normas que incluem a configuração de privacidade padrão para o nível mais alto e a limitação do uso de técnicas que incentivem o uso prolongado das plataformas, priorizando a proteção da privacidade infantil desde o design inicial. O código da Irlanda enfatiza a transparência e o consentimento informado, assegurando que as crianças e seus pais compreendam claramente como os dados são coletados e utilizados, e restringe a coleta de dados a informações essenciais. A proposta da Califórnia sugere a implementação de padrões rigorosos de proteção, como a minimização da coleta de dados e restrições à segmentação comportamental, mesmo com consentimento parental. Além disso, acreditamos que o design e desenvolvimento de serviços devem priorizar o melhor interesse da criança, incorporando boas práticas e padrões técnicos que assegurem a privacidade e a segurança. Essas exigências são aplicáveis não apenas a jogos, mas a qualquer serviço ou plataforma online acessível para crianças. Para alinhar-se com esses princípios, é útil criar um checklist operacional baseado nas normas da Califórnia, que inclui perguntas como: Qual é o propósito do produto ou serviço e como isso pode impactar o bem-estar das crianças? Como as informações pessoais de crianças são utilizadas e existe uma justificativa clara para a coleta e uso desses dados? O design expõe crianças a conteúdos ou contatos prejudiciais e há medidas para prevenir isso? Os algoritmos e a publicidade direcionada podem prejudicar as crianças e estou garantindo que a publicidade seja adequada? O design pode prolongar o uso de forma não saudável e estou avaliando o impacto psicológico e o tempo de tela? A coleta de informações pessoais sensíveis é adequada e como estou garantindo sua proteção? Estou realizando e atualizando uma Avaliação de Impacto de Proteção de Dados (DPIA) completa e documentada? Essas perguntas refletem um processo de due diligence comum em grandes organizações e equipes de privacidade na Califórnia. No Brasil, a garantia dos direitos das crianças e adolescentes em

ambientes digitais é pautada pelo princípio da "garantia dos direitos das crianças e adolescentes por design dos produtos e serviços em ambientes digitais", conforme o art. 3, X, da Resolução n. 245/2024. ","708762":"Fixamos que é necessário encontrar um equilíbrio entre a liberdade empresarial e a proteção de dados pessoais, garantindo que a ANPD não estabeleça restrições excessivas. A verificação de idade, comumente feita através da solicitação de documentos de identidade, pode ser eficaz, mas também levanta preocupações sobre privacidade e proteção de dados, devido à coleta excessiva de informações e ao risco de vazamentos. Métodos menos intrusivos para a verificação de idade incluem o uso de algoritmos de inteligência artificial que estimam a idade com base em padrões de comportamento online ou características faciais. Essas técnicas ainda precisam ser aprimoradas para garantir precisão e proteger a privacidade. Outra abordagem são as técnicas contextuais, que utilizam conhecimentos históricos que uma criança dificilmente teria, como identificar uma fita VHS em meio a outras imagens ou reconhecer objetos obsoletos, como disquetes. Essas soluções podem ser eficazes na verificação da idade sem recorrer à coleta de dados biométricos. Na França, a discussão sobre métodos não intrusivos ganhou destaque com o Decreto de 2021, que proibiu a raspagem de histórico de navegação para verificação de idade. O objetivo foi equilibrar a proteção de crianças e adolescentes com a privacidade dos indivíduos, evitando que técnicas invasivas expusessem informações sensíveis. O Decreto refletiu a preocupação com métodos intrusivos e promoveu o uso de abordagens que minimizam o impacto sobre a privacidade, como a utilização de terceiros confiáveis para gerenciar a verificação sem coletar dados identificáveis diretamente pelos sites. A Comissão Nacional de Informática e Liberdades (CNIL) recomendou que a verificação de idade não envolvesse a coleta direta de documentos de identidade, dados biométricos ou inferências baseadas em histórico de navegação. A CNIL enfatizou a necessidade de soluções que minimizem a coleta de dados e garantam a proporcionalidade das medidas, de maneira que não exigisse a coleta de documentos de identidade diretamente pelos sites, evitando também o uso de dados biométricos ou inferências baseadas em histórico de navegação. A CNIL também recomenda o uso de sistemas de autenticação fornecidos por terceiros para reduzir o risco de reutilização de dados coletados durante a verificação. Um estudo técnico de 2022 destacou a importância de evitar que a verificação de idade seja feita diretamente pela plataforma para minimizar riscos. A CNIL sugeriu um modelo de autenticação para terceiros que utilize camadas de anonimização, denominado dual third-party. Para criar um ambiente digital seguro para crianças, os profissionais de design devem adotar boas práticas que vão além da conformidade regulatória. Os engenheiros e designers devem proteger a privacidade das crianças desde o início, adotando padrões elevados de segurança e minimizando a coleta de dados. As interfaces devem ser projetadas com usabilidade infantil, sendo intuitivas e adaptadas à compreensão das crianças, com testes regulares para garantir uma experiência positiva e educativa. Além disso, devem ser implementados mecanismos robustos de controle de conteúdo e moderação eficaz, com filtros para bloquear material inadequado e sistemas de denúncia, além de garantir o consentimento parental em situações que envolvem transações financeiras ou compartilhamento de informações pessoais. Incentivar o desenvolvimento e a adoção de métodos de verificação de idade que respeitem a privacidade dos usuários e sejam proporcionais à finalidade do tratamento de dados é essencial. É importante promover

soluções que equilibram a proteção de dados pessoais com a liberdade empresarial, sem a imposição de regulamentações excessivamente rigorosas por parte da ANPD. ","708764":"Na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, é fundamental observar as limitações estabelecidas pelo art. 14, § 4º, da LGPD, que determina que o tratamento deve ser restrito às informações “estritamente necessárias à atividade”. Essa diretriz está em consonância com os princípios da LGPD, que destacam a necessidade e a proporcionalidade no tratamento de dados. Primeiramente, o princípio da necessidade, previsto no art. 6º da LGPD, exige que a coleta de dados seja limitada ao mínimo necessário para atingir a finalidade pretendida. Isso significa que plataformas digitais não devem coletar dados além do essencial para a operação do serviço, como em jogos e aplicativos. Essa limitação visa prevenir a coleta excessiva e proteger a privacidade dos usuários, particularmente de crianças e adolescentes, que estão em fase de desenvolvimento e podem não compreender totalmente as implicações da coleta de seus dados. A Resolução do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) proíbe a formação de perfis comportamentais de crianças e adolescentes para fins comerciais. Essa prática é considerada abusiva, pois utiliza dados pessoais para criar perfis detalhados que podem ser explorados de maneiras que não beneficiam diretamente o bem-estar dos jovens. A proibição reflete a preocupação com a proteção da privacidade e a prevenção de práticas discriminatórias e exploratórias. No contexto das Edtechs, essas plataformas devem garantir que a coleta de dados pessoais de estudantes seja estritamente necessária para fins educacionais e que não haja uso desses dados para formar perfis comportamentais ou para finalidades além da educação. As Edtechs precisam adotar medidas que assegurem a proteção de dados e a conformidade com os princípios da LGPD, evitando práticas que possam violar os direitos dos alunos. Considerando o regime jurídico de proteção de crianças e adolescentes, conforme o art. 14 da LGPD, é essencial que a coleta de dados pessoais seja estritamente limitada ao necessário, mesmo quando aplicados processos de anonimização ou remoção de identificadores pessoais. A anonimização dos dados não elimina totalmente os riscos associados à exploração comercial e ao uso indevido dessas informações. O art. 14 da LGPD, junto com a Resolução Conanda, impõe restrições rigorosas para proteger crianças e adolescentes de práticas abusivas, como a criação de perfis comportamentais. Mesmo com dados agregados ou transformados em metadados, a possibilidade de reidentificação e exploração comercial continua sendo uma preocupação significativa. Essas práticas, que exploram a vulnerabilidade dos jovens, violam os princípios de necessidade e proporcionalidade que regem o tratamento de dados pessoais. Portanto, a coleta de dados de crianças e adolescentes deve se restringir ao estritamente necessário, pois, mesmo com a anonimização, os riscos de exploração abusiva e violação dos direitos fundamentais persistem. A proteção integral desses direitos exige um controle rigoroso e uma justificativa clara para qualquer coleta de dados, assegurando que esteja sempre em conformidade com os princípios da LGPD e priorize a proteção da privacidade e o bem-estar dos jovens. É importante distinguir entre coleta abusiva e coleta excessiva. A coleta abusiva refere-se a práticas que exploram a vulnerabilidade das crianças e adolescentes, enquanto a coleta excessiva diz respeito à obtenção de mais dados do que o necessário para a finalidade declarada. A LGPD estabelece novos parâmetros jurídicos que buscam equilibrar a

necessidade de dados para a operação de serviços com a proteção dos direitos das crianças e adolescentes, impondo limites que evitam tanto a coleta abusiva quanto a excessiva. ","708768":"Para assegurar que os pais e responsáveis por crianças e adolescentes desempenhem um papel mais ativo na proteção dos dados pessoais, acreditamos que as plataformas digitais podem adotar boas práticas que descrevemos a seguir. Uma abordagem possível é oferecer ferramentas que possibilitem aos pais e responsáveis o gerenciamento e o uso das tecnologias pelas crianças e adolescentes. Essas ferramentas poderiam incluir funcionalidades vinculadas ao acesso a conteúdos adultos, notificações de tempo de uso e definição de limites na coleta de dados pessoais. Além disso, as plataformas podem garantir que as configurações de privacidade sejam intuitivas e acessíveis, facilitando ajustes adequados por parte dos pais e responsáveis. Um aspecto importante é a implementação de sistemas que tenham o consentimento explícito dos pais e responsáveis para a coleta e o tratamento de dados pessoais. Este processo deve ser evidente e direto, assegurando que os pais e responsáveis compreendam o que estão autorizando. A transparência é igualmente essencial, as plataformas devem fornecer informações claras sobre como os dados são coletados, utilizados e compartilhados, permitindo que os pais e responsáveis compreendam os riscos e as práticas associadas. É essencial encontrar um equilíbrio entre proteger a privacidade das crianças e adolescentes e permitir que desenvolvam autonomia e habilidades digitais. O controle excessivo pode limitar a capacidade das crianças e adolescentes de aprender a gerenciar sua própria privacidade e segurança. Além disso, a privacidade dos pais também deve ser considerada, garantindo que as ferramentas de controle não sejam invasivas. ","708772":"Para garantir transparência e fornecer informações de maneira clara e acessível, as plataformas digitais devem adotar boas práticas que atendam às necessidades de crianças e adolescentes e estejam alinhadas com diretrizes como a Resolução do Conanda. Essas práticas devem permitir que jovens compreendam como seus dados são coletados, utilizados e protegidos, e que exerçam seus direitos de forma eficaz. A Resolução do Conanda exige que as informações sejam apresentadas de forma acessível e compreensível, considerando as características cognitivas e de desenvolvimento dos jovens. Isso inclui criar seções dedicadas à privacidade e proteção de dados, facilmente localizáveis. Recursos audiovisuais, como animações e jogos educativos, podem ser eficazes para envolver crianças e adolescentes e facilitar a compreensão sobre privacidade. As plataformas devem projetar interfaces adequadas para a faixa etária dos usuários, utilizando linguagem simples e direta, evitando jargões técnicos. Informações sobre tratamento de dados pessoais devem ser apresentadas de forma que crianças possam entender, com o uso de recursos visuais, como ícones e gráficos. Por exemplo, elementos visuais e interativos, como infográficos e vídeos curtos, podem explicar como os dados são coletados e usados. É necessário que as plataformas ofereçam mecanismos que permitam aos jovens acessar e gerenciar seus dados pessoais facilmente. Isso pode incluir funcionalidades para visualizar e ajustar configurações de privacidade, e opções claras para solicitar correções ou exclusões de dados. Por exemplo, um painel de controle em um jogo digital pode permitir que o usuário ajuste configurações de privacidade e faça solicitações de alterações ou exclusões de dados. As plataformas devem evitar textos longos e complexos, preferindo resumos ou explicações breves que destaquem informações essenciais sobre privacidade e proteção de dados. Exemplos de boas práticas incluem

interfaces amigáveis, como as usadas por plataformas educacionais que utilizam mascotes e personagens animados para explicar a proteção de dados de forma lúdica. Jogos digitais podem usar tutoriais interativos para ensinar sobre privacidade enquanto os jogadores progridem, integrando a educação sobre dados pessoais de forma natural. A comunicação sobre privacidade deve ser visual e interativa. Em vez de textos extensos, podem ser usados gráficos e tutoriais curtos. Por exemplo, o LEGO usa elementos gráficos e interativos para permitir que crianças entendam e gerenciem seus direitos de forma prática e envolvente, como em painéis de controle com animações e explicações curtas. O conceito de linguagem clara e acessível também inclui a adaptação a diferentes contextos linguísticos. Em comunidades com diversidade linguística, como povos indígenas, plataformas podem utilizar sistemas de IA para adaptar textos para línguas locais, como o guarani. Nesse sentido, a acessibilidade deve guiar a apresentação dos termos de consentimento. Esses termos devem ser oferecidos em formatos acessíveis, como texto em braille e recursos auditivos ou visuais adaptados, garantindo que todos possam compreender plenamente os termos aos quais estão consentindo. Essas abordagens facilitam a compreensão das políticas de privacidade e permitem que crianças exerçam seus direitos de forma prática e acessível, alinhando-se às boas práticas de transparência e proteção de dados. ","708775":"Sim, há questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem um esclarecimento mais detalhado ou uma regulamentação adicional. Um aspecto fundamental a ser considerado é a exceção prevista no parágrafo 3º do art. 14 da LGPD, que permite o tratamento de dados pessoais de crianças sem o consentimento dos pais ou responsáveis legais, desde que a coleta seja necessária para contatá-los ou para a sua proteção. Isso porque, ainda não firmadas interpretações concretas sobre o que significa a exceção da exigência do consentimento para garantir a proteção da criança. Desse modo, é relevante que a ANPD se posicione para que tal interpretação seja azeitada com o arcabouço de proteção dos mais jovens. Um caminho que entendemos como adequado, em síntese, seria que a interpretação “de proteção” estivesse pautada pelo cumprimento expresso, devidamente justificado, de algum dos direitos estabelecidos no Estatuto da Criança e do Adolescente. Outra agenda urgente de ser incluída no Projeto Regulatório da ANPD sobre o tema é o desenvolvimento e a adoção de um Código de Design Apropriado à Idade,que deve incluir diretrizes específicas que ajudem a garantir que as práticas de coleta e tratamento de dados respeitem o melhor interesse em todos os serviços e produtos que sejam destinados ou que possam ser acessados por crianças ou adolescentes. O caso do LEGO serve como um bom exemplo de boas práticas nesse contexto. A política de privacidade do LEGO exemplifica como a empresa coleta e utiliza dados pessoais de forma transparente e adequada. O LEGO informa aos usuários sobre a coleta de dados de maneira clara e acessível, destacando a necessidade de autorização para a coleta, o uso restrito dos dados para as finalidades acordadas e a conformidade com a legislação local. O LEGO também oferece informações sobre como os dados são usados, armazenados e protegidos, e garante que dados pessoais não sejam compartilhados sem autorização ou, no caso de pessoas abaixo de 16 anos, sem a permissão dos pais. O LEGO emprega práticas que facilitam a compreensão dos usuários sobre seus direitos. Por exemplo, oferece instruções evidentes sobre como acessar, corrigir, ou excluir informações pessoais e como lidar com cookies e outros aspectos relacionados à privacidade.

O design das interfaces e a comunicação visual são projetados para serem amigáveis e apropriados para a faixa etária dos usuários, o que contribui para uma melhor compreensão e gestão dos dados pessoais. Essas práticas exemplificam como a criação de interfaces e políticas de privacidade adaptadas à idade pode ajudar a proteger a privacidade de crianças e adolescentes, assegurar a transparência no tratamento de dados e garantir que as informações sejam acessíveis e compreensíveis para crianças e adolescentes e seus responsáveis legais.

Contribuinte: Júlia Fernandes de Mendonça

Número: OP-751448

Data: 13/08/2024 - 19:59

Contribuinte: JEIEL DE SANTANA BARBOSA

Número: OP-752479

Data: 14/08/2024 - 16:26

Resumo: :"Não há como falar em “melhor interesse” quando há crescente dependência de crianças e adolescentes em relação às redes sociais, que por sua vez, acarreta danos à saúde mental e física desse público e traz a necessidade de regulamentação a fim de proteger estes jovens do ambiente nocivo digital. O princípio do melhor interesse deve conceber a real possibilidade da dependência causada nas crianças e adolescentes e os numerosos problemas de saúde física e mental dela derivados, além dos impactos no desenvolvimento social, como já têm sido investigados e combatidos na União Europeia e nos Estados Unidos. Essa questão é transversal em todo o processo, desde a efetiva utilização do ambiente digital até a coleta e tratamento de dados. Assim, os dados têm sido utilizados como forma de promover o uso desregulado e em desconformidade com as diretrizes da Sociedade Brasileira de Pediatria. Nesse sentido, O cirurgião norte-americano Vivek Murthy, em entrevista à CNN Brasil, afirmou que as redes sociais apresentam um “risco profundo de danos” para crianças e que não há evidências de que essas redes são seguras o suficiente para esse público.

Ademais, segundo pesquisa divulgada pelo portal Terra e elaborada pela Fundação Marília Cecília Souto Vidigal , feita em 13 capitais brasileiras, 33% das crianças de até 5 anos de idade ficam mais de duas horas por dia nas telas, consumindo grande parte desse tempo em redes sociais. Na mesma matéria, a psicopedagoga Ildeci Bessa afirma que o uso intenso das redes piora o desempenho escolar, pois atrapalha a concentração, a memorização, a interpretação e o raciocínio dos usuários. Renata Episcopo, neurologista infantil, enumera outros problemas causados pelo uso precoce e excessivo das redes sociais: problemas visuais, auditivos, transtornos posturais, impactos na comunicação, no aprendizado e no comportamento, atraso na linguagem, déficit de atenção, prejuízo na coordenação motora, aumento da sonolência diurna e ressalta que ocorre modificações no funcionamento cerebral, predispondo a dependência. Já o Comitê Gestor da Internet no Brasil efetuou uma pesquisa em 2019 que traz dados acerca do impacto das redes sociais frente aos jovens. Segundo o

levantamento, 89% da população entre 9 e 17 anos está conectada à internet (24,3 milhões de crianças e adolescentes). O levantamento mostra que um quarto dos jovens brasileiros considera que passam muito tempo conectados e confessam que não têm controle sobre esse período na frente das telas. Conforme mostra a pesquisa, 43% dos jovens já testemunharam episódios de discriminação online. As meninas são as mais impactadas por conteúdos prejudiciais: 31% foram tratadas de forma ofensiva, 27% acabaram expostas à violência e 21% acessaram materiais sobre "estratégias" para emagrecer. Por sua vez, a pesquisa realizada pela Universidade do Ceará e pela Universidade de Harvard, e divulgada pelo Child Fund Brasil, ao acompanharem 3155 crianças de até 5 anos de idade, 69% tiveram uso excessivo de tela, e, nos primeiros 12 meses de vida, 41,7% dos recém-nascidos tiveram acesso a vídeos e outros estímulos visuais passivos além da medida, porcentagem que aumenta e atinge 85,2% quando chegam aos 4 e 5 anos. Assim, o levantamento mostrou que cada hora de uso dos dispositivos eletrônicos diminuiu consideravelmente a capacidade de comunicação, de resolução de problemas e de sociabilidade das crianças. PPor sua vez, a pesquisa realizada pela Universidade do Ceará e pela Universidade de Harvard, e divulgada pelo Child Fund Brasil, ao acompanharem 3155 crianças de até 5 anos de idade, 69% tiveram uso excessivo de tela, e, nos primeiros 12 meses de vida, 41,7% dos recém-nascidos tiveram acesso a vídeos e outros estímulos visuais passivos além da medida, porcentagem que aumenta e atinge 85,2% quando chegam aos 4 e 5 anos. Assim, o levantamento mostrou que cada hora de uso dos dispositivos eletrônicos diminuiu consideravelmente a capacidade de comunicação, de resolução de problemas e de sociabilidade das crianças. ","708725":"O tratamento de dados de crianças e adolescentes devem ser sempre concebidos em conjunto com o tempo de uso de telas, uma vez que os algoritmos trabalham para criar dependência, assim, lucrando em cima de anúncios que aparecem para o público mais vulnerável e acarretando danos à saúde física e mental no processo. Propaganda: é necessário ter restrições para anúncios feitos a crianças e adolescentes, bem como limitar as publicidades, em especial às crianças menores de 12 anos, às quais qualquer tipo propaganda deve ser vedada, conforme Resolução nº 163 do CONANDA. Para os adolescentes de 13 a 18 anos, deve haver rigor quanto ao consentimento dado pelos pais e responsáveis, nos moldes do art. 14 da LGPD, bem como rigor quanto ao tipo de publicidade exibida e quanto à quantidade permitida. Efeito Toca de coelho: A Comissão Europeia, por meio de seu Comissário Europeu Thierry Breton, investiga atualmente a Meta pelos problemas aqui já relatados e decidiu abrir processo formal contra e empresa. Segundo o comissário, a Meta não está agindo diligentemente para mitigar os efeitos negativos para a saúde física e mental dos jovens europeus em suas plataformas. A União Europeia também acredita que os sistemas das redes sociais têm potencial lesivo de causar dependência em crianças, causando isolamento e depressão. A comissão expressou preocupação em relação ao funcionamento dos algoritmos das redes sociais, visto que estimulam a dependência ou o "efeito toca do coelho": o algoritmo instiga o usuário a ir cada vez mais fundo em um tipo de conteúdo, levando a ciclo vicioso e a conteúdos manipuladores e perigosos. A ação da Comissão Europeia se baseia na Lei de Serviços Digitais (DSA) do bloco europeu, segundo a qual as empresas de tecnologia são obrigadas a combater conteúdo ilegal que circula nas plataformas, como fraudes e abuso de crianças. Dessa forma, é imperativo haver a regulamentação para que haja

limites no funcionamento do algoritmo no que tange ao “efeito toca de coelho”, com vistas a evitar o vício em espirais de conteúdo, que podem levar à exibição de conteúdos extremos e radicais, ao mesmo tempo em que gera dependência e compulsividade. ","705523":": Critério: ciência em relação aos parâmetros da Sociedade Brasileira de Pediatria para evitar o risco à dependência: •Crianças com idades entre 2 e 5 anos, limitar o tempo de telas ao máximo de 1 hora/dia, sempre com supervisão de pais/cuidadores/ responsáveis. •

Crianças com idades entre 6 e 10 anos, limitar o tempo de telas ao máximo de 1-2 horas/dia, sempre com supervisão de pais/responsáveis. • Adolescentes com idades entre 11 e 18 anos, limitar o tempo de telas e jogos de videogames a 2-3 horas/dia. ","708742":"Autorização por vídeo acompanhado de comprovação da identidade dos pais ou responsáveis. Toda e qualquer conta de menor de idade em rede social, criada sem a autorização dos pais ou responsáveis, deve ser suspensa e seja concedido prazo para que o requisito seja cumprido em 15 dias, sob pena de exclusão da conta e multa. ","708745":"Considerando o caso de adolescentes (13 a 17 anos), seguir as disposições do direito civil parece adequado. Logo, de 13 a 16 anos deve haver representação pelos pais ou responsáveis, bem como haver maior limitação de tratamento de dados, anúncios e conteúdos, com critérios mais rigorosos. Para adolescentes de 16 e 17 anos, deve haver assistência, considerando a capacidade relativa, com permissão intermediária para tratamento, anúncios e conteúdos.","705539":"Utilizar técnicas para anonimizar ou pseudonimizar os dados pessoais para reduzir os riscos de identificação","708762":"Métodos de Confirmação Parental: Enviar solicitações de verificação para os pais ou responsáveis, como e-mails ou códigos de confirmação, para assegurar que o consentimento foi realmente dado por um adulto responsável. Criar mecanismos para verificar a compatibilidade entre o cadastro do usuário e o usuário efetivo a fim de evitar o uso indevido de contas por menores, que ficam expostos ","708764":"restrições para o tratamento como forma de impedir a dependência, conforme o tempo de uso do usuário. Restrições para treinamento de algoritmo com o fim de promover anúncios e conteúdos problemáticos (efeito toca de coelho).","708768":"informar aos pais e responsáveis antes do tratamento de dados para obter o consentimento, enumerando todas as finalidades e funcionamento do tratamento. Informar aos pais e responsáveis periodicamente acerca do comportamento dos menores no ambiente digital, como o tempo de uso, com o fim de evitar a dependência. Que aA informação deve ser informação seja clara e direta a fim que trazer assimetria da informação. ","708772":"6.

Informar com clareza e objetividade a finalidade do uso dos dados, criar mecanismo de opt out para evitar o uso e o compartilhamento de dados a ser decidido pelos pais ou responsáveis. Criar uma lista mostrando com quais empresas são compartilhados os dados, também dando opção de opt out. Criar checklist para cada finalidade do uso de dados, dando aos pais ou responsáveis e ao usuário comum a possibilidade de opt out para cada finalidade. ","708775":"Deve haver mecanismos em tempo real para averiguar que o usuário de uma rede social é, de fato, aquele cadastrado para uso de determinada conta. Assim, deve-se criar mecanismos para evitar o burlamento do usuário, o que pode criar situações nas quais uma criança está usando contas de adultos, e, assim, tendo seus dados tratados como se assim o fossem, sendo expostas a anúncios e conteúdos inadequados.

Contribuinte: ELEN PRATES DE SOUZA

Número: OP-752734

Data: 15/08/2024 - 11:13

Resumo: :"Considerando a aplicabilidade limitada no âmbito do Poder Público, entende-se que a hipótese do legítimo interesse no caso das Ouvidorias não se aplique, sendo recomendável o uso de outras bases legais que fundamentem o tratamento. No Distrito Federal, as finalidades de uso dos dados coletados são as seguintes: 1) Tratamento da demanda apresentada com foco no relato (incluindo anexos, se houver); 2) Elaboração dos relatórios de trabalho e 3) Aplicação em estudos e pesquisas governamentais.","708725":"Tendo como base a resposta ao item anterior, entendemos que a única questão aplicável à realidade das Ouvidorias públicas seja o consentimento “específico e em destaque” fornecido por um dos pais ou pelo responsável legal.","705523":"Entendemos que a Ouvidoria, enquanto unidade governamental responsável por estabelecer o relacionamento com o cidadão, deva fomentar e estimular o exercício do controle social por pessoas físicas (titulares de dados pessoais). Nesse contexto, eliminar ou minimizar exigências que possam ser interpretadas como barreiras de acesso torna-se um desafio que pode ser superado com o uso da tecnologia, viabilizando o uso das ferramentas de registro das manifestações por menores “previamente autorizados” por um dos pais ou responsável legal. Dessa forma, o momento de cadastro da conta por pessoa maior de idade ou mesmo a funcionalidade “gerenciamento de conta” já criada deve possibilitar a inclusão de menores de idade que eventualmente queiram abrir sua própria conta na mesma plataforma em momento futuro. Ressalta-se aqui que a ação é concluída somente após a leitura e concordância do termo de consentimento, apresentado com os dados informados de forma específica e em destaque. Essa medida, além de contribuir para a adequação às questões da LGPD, gera segurança à rotina das Ouvidorias.","708742":"As bases de dados das ferramentas utilizadas para coleta de dados pessoais devem estar aptas a consultar bases de dados nacionais (Ex. Receita Federal) visando validar a titularidade das contas criadas (passivo) ou a serem criadas. A possibilidade de cruzamento dos dados envolvendo o CPF de menores aos respectivos pais ou responsáveis possibilita a confirmação da filiação ou tutela. A avaliação dos riscos envolvendo as bases e seus eventuais compartilhamentos devem ser objeto de análise visando ações mitigatórias previstas em instrumento contratual ou de convênio.","708745":"Considerando que a autonomia progressiva é um princípio que reconhece às crianças a faculdade de decidir quando e como querem exercer um direito, sua concessão deve ser entendida como uma alteração cadastral a ser registrada na base de dados da Receita Federal. As ferramentas de Ouvidoria podem utilizar-se dessa mesma base (atualizada) para considerar o caso em seus processos de coleta e tratamento de dados, não condicionando o acesso ao consentimento de pais e responsáveis. ","705539":"O Governo do Distrito Federal vem buscando a devida adequação de seus processos de trabalho que envolvam a coleta e uso de dados pessoais (inclusive de menores) tendo como base os princípios da LGPD. A consecução dessa adequação está condicionada à correta execução de ações previstas em um planejamento, elaborado a partir do mapeamento da situação atual (diagnóstico) e de um plano de gestão de riscos que inclua as ferramentas (plataformas,

aplicativos e participação em redes sociais) utilizadas nos processos de trabalho. As medidas escolhidas para mitigar riscos que dependam do trabalho da área de Tecnologia da Informação devem estar contempladas no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) de cada órgão/entidade. ","708762":"A construção de uma boa prática se dá a partir da aplicação, monitoramento e aperfeiçoamento. Nesse contexto, no âmbito da Ouvidoria, entendeu-se que a base de dados da nossa plataforma “Participa-DF” deveria ser “limpa” a partir da verificação dos nº de CPF constantes da base da Receita Federal. A identificação de cadastros com dados inconsistentes, inexistentes ou de pessoa falecida levou à aplicação de ações tanto na ferramenta como nas rotinas desenvolvidas pelas pessoas (rede SIGO-DF) e abriu espaço para ideias de melhoria (ver respostas 1 e 2 do item CONSENTIMENTO).","708764":"A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece em seu artigo 14, § 4º da LGPD que os controladores não devem condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. No caso das Ouvidorias, entendemos que cada assunto constante da tabela armazenada na ferramenta de registro deva conter campos complementares, de preenchimento obrigatório, que ajudarão no tratamento do mérito. Além disso, a LGPD estabelece outros princípios e regras importantes: • O princípio do “melhor interesse”, que deve sempre ser observado no tratamento de dados pessoais de crianças e adolescentes. (Não aplicável no setor público). • O consentimento específico e em destaque, a ser obtido dos pais ou do responsável legal pela criança, quando necessário ao tratamento de seus dados pessoais. • O fornecimento pelos controladores de informações de maneira simples, clara e acessível sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares. Além disso, a LGPD permite a coleta de dados pessoais de crianças sem o consentimento quando as informações forem necessárias para garantir a proteção delas ou para contatar os pais ou o responsável legal. No entanto, essas informações devem ser utilizadas uma única vez e sem armazenamento, e em nenhum caso podem ser repassadas a terceiros sem autorização. Portanto, ao coletar e tratar dados pessoais de crianças e adolescentes, as plataformas digitais devem observar essas limitações e garantir que estão agindo no melhor interesse da criança ou do adolescente. Isso inclui considerar a natureza dos dados coletados e a finalidade do tratamento, como a formação de perfis comportamentais.","708768":"No contexto de Ouvidoria, considerando o conteúdo das respostas 1 e 2 do item “II - CONSENTIMENTO” entendemos que uma forma adicional de controle pode ser o envio automático, aos pais ou responsáveis, de respostas concedidas aos menores. Dessa forma, o Estado concede a possibilidade de acompanhamento das questões postuladas pelo menor e facilita o exercício do controle social.","708772":"1. Informações claras e acessíveis: As informações sobre o tratamento de dados devem ser fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário. Isso pode incluir o uso de recursos audiovisuais quando adequado. 2. Transparência: As plataformas digitais devem fornecer informações claras, simples e acessíveis sobre a coleta e uso de dados, considerando as características físico-motoras, sensoriais, intelectuais e mentais das crianças e adolescentes. Portanto, é importante que sejam transparentes sobre quais dados estão coletando, porque

estão coletando esses dados e como eles serão usados. Isso pode ser feito por meio de políticas de privacidade claras e facilmente acessíveis, podendo ainda incluir o uso de recursos audiovisuais para facilitar a compreensão. 3. Consentimento dos pais ou responsáveis: Quando necessário, as plataformas devem obter o consentimento dos pais ou responsáveis antes de coletar ou usar dados pessoais de crianças. 4. Limitação da coleta de dados: As plataformas não devem coletar mais dados do que o necessário para a atividade em questão. Isso é especialmente importante quando se trata de dados de crianças. 5. Segurança dos dados: As plataformas devem implementar medidas de segurança adequadas para proteger os dados pessoais de crianças e adolescentes. 6. Direitos do titular: As plataformas devem fornecer meios para que os titulares dos dados (ou seus pais ou responsáveis) possam exercer seus direitos sob a LGPD, como o direito de acessar, corrigir e excluir seus dados.","708775":"Nada mais a acrescenta. Contudo, gostaríamos de destacar que as respostas foram apresentadas em nome da Câmara Técnica (CT) da Rede Nacional de Ouvidorias (Renouv), prevista no Decreto nº 9.492/2018, a qual trata da aplicação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, no âmbito das ouvidorias públicas. A CT-LGPD se configura como instância de caráter orientativo e não vinculante, observando a dinâmica colaborativa e o respeito às especificidades dos membros da Rede. Sendo assim, os esclarecimentos prestados são resultado do trabalho em grupo com os 17 (dezessete) membros da CT-LGPD, quais sejam: Ouvidoria Geral do Município de Londrina/PR, Instituto Brasileiro do Meio Ambiente e dos Recursos – IBAMA, Controladoria-Geral da União – CGU, Supremo Tribunal de Justiça – STJ, Prefeitura de Igrejinha/RS, Dataprev, Prefeitura Municipal de São José do Rio Preto/SP, Ministério das Cidades, Ministério do Desenvolvimento, Indústria, Comércio e Serviços – MDIC, Prefeitura Municipal de Três Marias/MG, Centro Federal de Educação Tecnológica de Minas Gerais – CEFET/MG, Ouvidoria-Geral do Município de Vitória da Conquista/BA, Controladoria-Geral do Distrito Federal – CGDF, Superintendência do Desenvolvimento do Centro-Oeste – SUDECO, Controladoria-Geral do Estado do Amazonas – CGE/AM e Universidade Federal de Mato Grosso – UFMT.

Contribuinte: Rede Nacional de Ouvidorias

Número: OP-752757

Data: 15/08/2024 - 12:39

Resumo: :"[Contribuições feitas em nome da Telefônica Brasil S.A.] Entendemos que o Enunciado CD/ANPD Nº 1, de 2023 (“Enunciado”) corretamente já regulamentou o aspecto mais importante sobre o tema e, neste sentido, deve ser reforçado, exemplificado e complementado pela Autoridade a partir das manifestações recebidas da sociedade por meio desta Tomada de Subsídios. Importante ressaltar, desde já, sugerimos que os exemplos e esclarecimentos sejam feitos necessariamente a título exemplificativo e não taxativo, especialmente considerando a diversidade de mercados no cenário brasileiro, bem como - naturalmente - dos titulares envolvidos nos diversos cenários práticos atuais. A orientação da ANPD sobre o tema deve ser especialmente voltada para o esclarecimento do que é entendido

como "melhor interesse do menor", preferencialmente por meio de exemplos não exaustivos considerando diversos mercados, abarcando desde o conceito ou entendimento técnico do que é o "melhor interesse do menor" a ações práticas educativas destinadas aos Titulares. Partindo destes esclarecimentos e rol exemplificativo prático, entendemos que a qualidade e precisão de informação aos titulares, bem como a avaliação de riscos e proporcionalidade das atividades envolvendo o tratamento de dados de menores pelas empresas serão mais precisas e atenderão melhor às necessidades aplicáveis a cada caso. Os exemplos também serão direcionadores essenciais para a sociedade como um todo, de forma que possa exigir - como titular - e desenvolver - como empresa atuante - suas próprias medidas educativas na proximidade adequada para o seu serviço ou fornecimento em atendimento à LGPD. ","708725":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Não entendemos que há um contexto ou uma situação específica que demande atenção especial da ANPD, mas sim um direcional relativo à premissa inicial no contexto do tratamento de dados de menores, que é a presunção prévia do melhor interesse. Isto é, o entendimento de que as atividades envolvendo tratamento de dados de menores consideram, desde sua etapa inicial, o melhor interesse do menor. Note-se que nossa sugestão aqui é que o princípio do melhor interesse seja uma premissa inicial e não uma condição a ser comprovada ou superada sempre e previamente a toda atividade de tratamento que envolva dados de menores em alguma medida. Do contrário, - isto é, exigir que o melhor interesse seja comprovado e superado constantemente – pode trazer potenciais impactos e prejuízos dos titulares na medida em que a sustentabilidade probatória para algumas atividades tornaria alguns serviços e produtos do mercado insustentáveis ou inviáveis o que, por sua vez, poderia impactar indireta e diretamente na evolução e desenvolvimento social. ","705523":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Entendemos como essencial esclarecer nesta resposta o aspecto da representação e/ou assistência tácita para adolescentes inserida no contexto atual da sociedade. A capacidade civil tem sido amplamente discutida recentemente, especialmente porque o Código Civil Brasileiro em vigor e´ de 2002, época em que o uso da internet e de plataformas digitais não era tão comum como atualmente. Neste sentido, acadêmicos e doutrinadores têm defendido uma abordagem mais flexível para "atos corriqueiros" dos adolescentes em algumas situações, como no caso de uso de plataforma projetada para criação de conteúdo, consumo de vídeos e interação com outros usuários. Isto considerando 2 aspectos: a) Estes atos não impõem ou exigem consequências significativas ou compromissos para os adolescentes; e b) É necessário retornar a institutos desatualizados para adaptá-los a` nova realidade social. Conforme as interações online se desenvolvem, é natural que discussões para que as legislações se adaptem às realidades do uso moderno das plataformas digitais, especialmente considerando que as atividades online dos adolescentes são frequentemente reconhecidas como rotineiras. Nessa mesma linha, a Federal Trade Commission ("FTC") se pronunciou sobre o tema em razão do Children's Online Privacy Protection Act ("COPPA"). Primeiramente, a FTC explorou o conceito de consentimento parental verificável e listou alguns métodos e informações possíveis como evidência desse consentimento. O COPPA, assim como a FTC, não especifica o método que uma empresa deve usar para obter o consentimento parental. Em vez disso, exige que a empresa responsável escolha um método razoavelmente adequado, considerando a tecnologia

disponível, e o implemente a fim de garantir que a pessoa que concede o consentimento ou exerce direitos em nome do menor seja de fato a pessoa competente para tanto. Esclarecemos melhor sobre os métodos e mecanismos ao longo da Resposta para a Pergunta 2. Por fim, vale ressaltar que a FTC analisa e dispõe continuamente sobre diversos métodos e padrões de verificação de consentimento, em muitos casos apresentados pelo próprio mercado. Um deles, compatível com a realidade do Brasil, já aprovado e mencionado no website da FTC como possível, é o uso de cartão de crédito, cartão de débito ou outro sistema de pagamento online pelo menor. Complementarmente à premissa de consentimento tácito dos responsáveis, entendemos que - nos casos em que o Consentimento for aplicável - há uma diversidade de medidas e ferramentas disponíveis no mercado que podem ser consideradas pelas empresas. Nesta mesma linha, estas empresas independentes deverão selecionar e implementar a medida mais adequada para o seu negócio, visando a preservação dos direitos dos seus Titulares e garantindo o consentimento pelos representantes legais competentes. Neste sentido, é importante para a cultura e harmonia de condução no mercado brasileiro que os mecanismos e métodos com o objetivo de verificar o consentimento parental sejam indicados pela ANPD a título de rol exemplificativo. ","708742":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Ainda em linha com os comentários na Pergunta 1 deste bloco, entendemos que os “esforços razoáveis” pelas empresas devem ser avaliados individualmente e conforme seu negócio/mercado. Indiscutivelmente, é essencial que as empresas mantenham medidas e mecanismos que permitam a verificação de idade do Usuário no momento do primeiro acesso, mas também de forma contínua. Desta forma, não só fica preservado o consentimento tácito anteriormente fornecido por meio do aceite dos Termos de Adesão das plataformas pelo Usuário menor, bem como garante que eventuais consentimentos fraudados pelo menor sejam mapeados e que o responsável legal tenha condições de retirar o consentimento. Abaixo, mencionamos 2 exemplos de mecanismos e medidas que entendemos como adequados e são comumente praticados no Brasil e exterior:

a) Age Gate: é o mecanismo melhor aceito atualmente pela sociedade e pelas plataformas digitais das mais diferentes naturezas. No age gate, a empresa confia na declaração inicial do Usuário, mas mantém ferramentas operando que permitem a detecção de inveracidade/fraude de informações posteriormente. Isto é, a empresa mantém um processo de verificação/moderação de conteúdo. A partir de uma suspeita de fraude no age gate, a empresa inicia um processo de apuração e – caso confirmado – bloqueia/revoga a conta do Usuário na plataforma. É muito importante nesta medida, que as empresas efetivamente confiem/partam da boa-fé sobre a veracidade da informação, não solicitando dados adicionais com o objetivo de confirmar a idade indicada (como documento de identidade), mas sim estabelecendo mecanismos reativos aplicáveis após o cadastro. Isto porque essa coleta incialmente bem-intencionada pode mais expor o Usuário do que o proteger na medida em que pode se comprovar desnecessária ou mesmo motivar o Usuário a incluir documento de terceiro. Outro ponto importante aqui é que o age gate seja, de fato, uma espécie de portão de controle no caso em que o Usuário indicar idade abaixo da permitida para acesso na plataforma – hoje comumente a idade limite de 13 anos. Caso a informação incluída signifique idade inferior a 13 anos, é essencial que a plataforma impeça ou bloqueie a alteração da informação instantaneamente de forma que a criança seja impedida

de prosseguir – seja “corrigindo” ou alterando a informação indicada. b) Canal de Denúncia: disponibilizar um canal de denúncia para suspeitas ou fraude confirmadas dentro das plataformas. Assim, as empresas terão condições de rever as denúncias de forma centralizada e manterão canal aberto para com os representantes/responsáveis legais que precisarem entrar em contato por qualquer motivo relacionado aos menores de sua responsabilidade. É essencial que os mecanismos e métodos com o objetivo de verificar o consentimento parental sejam indicados pela ANPD a título de rol exemplificativo. ","708745":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Reforçamos o exposto na resposta à Pergunta 1: o Código Civil Brasileiro não define especificamente a representação ou assistência. A ausência de diretrizes específicas sobre a forma da representação ou assistência sugere que a aceitação dos termos de serviço por meio de acordos de clique é um acordo implícito dos responsáveis. Assim, é razoável confiar na autorização tácita dos pais ou responsáveis considerando a prática de alguns atos mais simples por adolescentes, resguardada a responsabilidade da empresa na implementação de medidas que permitam ações posteriores para eventual mitigação de risco. Há uma compreensão implícita de que os menores se envolvem em atividades online com algum nível de conhecimento ou autorização dos pais e/ou responsáveis, embora não exija aprovação explícita destes, e sequer é necessária, estando de acordo com as interpretações legais atuais. Adicionalmente, importante notar que o entendimento contrário – isto é, que os responsáveis devem consentir expressamente para toda e qualquer situação envolvendo adolescentes – pode prejudicar uma série de contratações e produtos rotineiros e seguros para estes Usuários e já comumente praticados via contrato verbal, inclusive com a ciência e acompanhamento dos responsáveis ainda que de forma tácita - como a compra de uma pizza ou a entrada de um cinema. Por fim, entendemos como correta a aplicação da autonomia progressiva dos adolescentes, em consonância tanto com o melhor interesse do menor quanto com o próprio Código Civil. ","705539":"[Contribuições feitas em nome da Telefônica Brasil S.A.] O Information Commissioner’s Office (“ICO”) tem disponível em seu website um Guia considerando o Children’s Information. Referido guia tem servido de referência nas práticas visando a proteção no tratamento de dados de crianças e adolescentes, devendo servir da mesma forma no Brasil. Dentre diversas práticas, algumas mencionadas: a i) Transparência na Coleta de Dados, considerando que as plataformas devem fornecer informações claras e acessíveis sobre como os dados pessoais de crianças e adolescentes serão usados, incluindo os propósitos da coleta, o uso pretendido e quaisquer compartilhamentos de dados com terceiros e ii) o Acesso e Retificação pelos pais ou responsáveis, bem como a correção de informações imprecisas ou desatualizadas. ","708762":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Primeiramente, reforçamos mais uma vez que atualmente dezenas de boas práticas e técnicas disponíveis considerando a verificação de idade estão disponíveis no mercado e que eventual rol ou lista de boas práticas ou técnicas a ser apresentada pela ANPD seja meramente exemplificativa e não impositiva/taxativa. As medidas e técnicas aqui, são semelhantes àquelas mencionadas na Resposta à Pergunta 2 do bloco de Consentimento com uma adicional considerando verificação de conteúdo: a) Age Gate: a empresa parte da boa-fé social e confia na declaração inicial do Usuário, mas mantém ferramentas operando que permitem a detecção de inveracidade/fraude de informações posteriormente, ou seja, a

empresa deve manter um processo de verificação/moderação de conteúdo. O age gate deve ser efetivamente uma espécie de portão de controle, impedindo que o Usuário prossiga com o acesso/criação de conta apenas “corrigindo” ou alterando uma informação inicialmente incluída com o objetivo de burlar o limitador determinado pela plataforma. Neste cenário, é cristalina a preservação do melhor interesse do menor pela própria plataforma considerando o seu impedimento de acesso aos serviços como potencialmente inadequados para sua faixa etária. b) Verificação/moderação de conteúdo: é a verificação das atividades consumidas pelo Usuário com o objetivo de entender se ele fraudou a informação relativa à idade no momento de acesso/criação de conta na plataforma. Essa moderação consiste basicamente na verificação do conteúdo consumido pelo Usuário motivada pela inconsistência quando comparado com o conteúdo consumido por outros Usuários da mesma faixa etária indicada. Por vezes, a suspeita ou confirmação de fraude no age gate se dá na moderação de conteúdo, quando a empresa verifica que este não é aquele habitualmente consumido pelo público da faixa etária originalmente indicada. Por exemplo, no momento da criação de uma conta ou do primeiro acesso na plataforma, o Usuário indica que tem mais de 18 anos. Porém ao conectar/acessar a plataforma, ele inclui na foto de perfil a de um adolescente e consome o conteúdo de páginas comumente famosas nesse público e não no público com idade igual ou superior a 18 anos. Identificada essas inconsistências pela empresa, ela iniciará uma apuração. A partir desta verificação, a empresa tem condições de revisar as informações indicadas no momento do cadastro em conjunto com a atividade do Usuário na plataforma e analisar se necessário a tomada de ação na conta – seja de bloqueio, banimento ou outro - a fim de preservar o melhor interesse do menor. c) Canal de Denúncia: disponibilizar um canal de denúncia para suspeitas ou fraude confirmadas dentro das plataformas, disponibilizando canal aberto entre a plataforma e a sociedade. Entendemos que o movimento atual de validação de idade no Brasil é correto e coerente, além de bem aceito – inclusive pelo FTC e ICO. Por meio das medidas mencionadas, acreditamos que o melhor interesse do menor é preservado de forma transparente e proporcional, garantindo seu acesso e inserção na sociedade de forma controlada e segura conjuntamente pelos seus responsáveis e as empresas fornecedoras dos serviços. Este fluxo é importante na medida em que não inviabiliza o acesso de Usuários adolescentes às plataformas adequadas para sua faixa etária, bem como controla e evita a permanência de menores naquelas potencialmente ou sabidamente inadequadas. ","708764":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Sobre os perfis comportamentais, é importante esclarecer e considerar os perfis comportamentais em 2: (i) aqueles com a finalidade exclusiva de marketing/publicidade e (ii) aqueles para fins outros que não publicidade digital. Partindo dessas possibilidades, é relevante que a ANPD considere que a formação de perfis comportamentais isoladamente e de forma neutra pelas empresas podem não só estar aliada ao melhor interesse do menor, como colaborar e garantir sua preservação. Vejam, a formação de perfil comportamental considerando a adequação na apresentação de conteúdos conforme seus gostos e desenvolvimento humano e social pode ter alto impacto positivo. Exemplificando, um Usuário muda o perfil de conteúdos nos últimos meses diminuindo o volume consumido de desenhos animados e séries e aumentando o de vídeos educacionais ou de uma matéria em específico (como exatas, humanas, etc). Neste cenário, o perfil comportamental visando a

oferta de conteúdos educativos mais lúdicos, com melhores avaliações por outros Usuários, contribui e preserva o melhor interesse do menor. Assim, entendemos que proibir ou restringir a formação de perfis comportamentais pode prejudicar – e não preservar - os interesses dos menores, podendo impactar no seu desenvolvimento social e humano. A finalidade e formação dos perfis comportamentais, do ponto de vista prático, são essenciais para a análise tanto de benefícios e prejuízos, bem como possíveis danos, decorrentes dessa prática. ","708768":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Entendemos que mecanismos e boas práticas, considerando o controle dos pais e responsáveis, devem ser escolhidos e aplicados exclusivamente a critério destes pais e responsáveis. Ou seja, é da livre escolha destes Usuários quais programas e medidas serão utilizados para seu controle parental dos conteúdos dos menores de sua responsabilidade e mais, entendemos essencial essa prática social prosseguir como habitual nos dias de hoje. Vale relembrar aqui que o Marco Civil de Internet ("MCI") acertadamente determinou em seu Art. 29 , amplamente debatido à época do seu processo legislativo, a liberalidade e responsabilidade exclusiva dos pais e responsáveis quanto a forma e programa de computador a ser utilizado para o seu adequado controle parental. Com isto, entendemos como desnecessária a regulamentação e implementação de medidas estatais adicionais à previsão em vigor feita pelo MCI. Apenas a título de debate, caso a ANPD entenda contrariamente, importante considerar que eventuais boas práticas e medidas objetivando ampliar o controle dos pais e responsáveis sejam exclusivamente exemplificativas e não impositivas tendo em vista a diversidade de formação, status econômico e cultural das famílias brasileiras. ","708772":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Entendemos que o essencial a esclarecer nesta Pergunta é que as boas práticas considerando transparência e fornecimento de informações de forma assertiva e eficaz varia conforme o mercado objeto de análise e que, considerando nosso país, é extremamente diverso e regionalizado. Assim, do nosso ponto de vista, não existe uma fórmula única ou um modelo específico para apresentar informações sobre a proteção de dados de menores. Essa comunicação pode ser, e deve, considerando (i) o público-alvo de destino e (ii) o melhor formato para este público – seja por meio de vídeos, jogos, textos curtos e claros ou qualquer outro meio avaliado pelas empresas. O importante é garantir que a comunicação seja compreensível, e verificar se uma criança ou adolescente - o público-alvo - pode entender a mensagem. Adicionalmente, é crucial distinguir se o destinatário é criança ou adolescente. Adolescentes, devido à maior autonomia e capacidade, tendem a conseguir ler e interpretar informações essencialmente. Enquanto no caso das crianças, muito provavelmente o público-alvo das empresas são os pais e/ou responsáveis que lerão e entenderão as condições e responsabilidades indicadas. É necessário cuidado ao simplificar e personalizar a linguagem e conteúdo considerando plataformas direcionadas ou disponíveis para crianças, visto que na prática o Usuário responsável por avaliar as comunicações é, em verdade, os pais ou responsáveis e não a criança propriamente dita. Ainda sobre o ponto anterior, uma abordagem possível e adequada seria orientar através da própria comunicação que os pais ou responsáveis devem ler e entender a sessão relativa à proteção e tratamento de dados. Por exemplo: "Veja esta seção com um adulto" ou "Leia com um responsável". Esse direcionamento e interação conjunta, garante que os responsáveis possam explicar os conceitos e cuidados necessários as crianças, assegurando que elas utilizem a plataforma de

forma segura e informada. ","708775":"[Contribuições feitas em nome da Telefônica Brasil S.A.] Entendemos que o Enunciado da ANPD acertadamente estabeleceu a possibilidade de aplicação de qualquer base legal para o tratamento de dados de menores, desde que observado seu melhor interesse. Isto foi crucial para evitar retrocessos. Considerando desdobramentos e o processo natural de maturidade deste ponto, entendemos que é essencial que a ANPD esclareça e reforce este posicionamento em materiais oficiais a fim de evitar interpretações equivocadas no sentido de que o consentimento é a regra geral, colocando as demais bases previstas na LGPD como exceções ou inferiores. Assim, nossa sugestão é para que a ANPD inclua tal informação em outros materiais da ANPD, bem como referencie o Enunciado em seus diversos documentos que oportunamente venham a ser desenvolvidos como resultado da presente tomada de subsídios.

Contribuinte: Karen Scarpel Araújo Forte

Número: OP-752803

Data: 15/08/2024 - 14:19

Resumo: :"A doutrina especializada em direitos fundamentais de crianças frequentemente caracteriza o princípio do melhor interesse como indeterminado e dinâmico, o que muitas vezes causa confusão sobre os contornos da sua aplicação. A sua indeterminação e dinamicidade advêm, porém, da sua característica de princípio geral da Convenção sobre os Direitos da Criança (daqui pra frente, Convenção). Isto quer dizer que ele deve ser utilizado na interpretação e aplicação de outros direitos previstos na Convenção (Lundy & Byrne, 2017). Sendo um mandado de otimização com caráter procedimental, não é possível definir o que é de melhor interesse de uma criança ou grupo de crianças em abstrato. O conteúdo do princípio do melhor interesse será sempre o resultado de um exercício de balanceamento no caso concreto. Isso não quer dizer que decisões tenham de ser tomadas a nível individual e o próprio Comitê reconhece a possibilidade de uma análise coletiva do melhor interesse de um grupo de crianças (como a nível de legislação, políticas públicas ou mesmo em uma plataforma digital). A fim de auxiliar a determinação do conteúdo do melhor interesse, o Comitê apresenta alguns parâmetros não exaustivos que devem ser utilizados: a) A natureza universal, indivisível, interdependente e inter-relacionada dos direitos das crianças; b) Reconhecimento das crianças como titulares de direitos; c) A natureza global e o alcance da Convenção; d) A obrigação dos Estados Partes de respeitar, proteger e cumprir todos os direitos na Convenção; e) Efeitos de curto, médio e longo prazo das ações relacionadas ao desenvolvimento da criança ao longo do tempo. Estes parâmetros mostram que este não é um exercício subjetivo. Assim, o primeiro critério aponta para a necessidade de um balanceamento dos impactos negativos e positivos do tratamento de dados em todos os direitos previstos na Convenção, considerando a sua indivisibilidade e interdependência. Esse balanceamento para a identificação do melhor interesse deve ser feito através da realização dos chamados Children Rights Impact Assessments – CRIAs, que podem ser holisticamente integrados nos Relatórios de Impacto de Proteção de Dados (RIPD). Os outros princípios gerais da Convenção devem ser considerados neste exercício também, em especial o direito

de crianças a serem ouvidas, que deve ser implementado sempre que possível na tomada de decisão. Destaca-se, também, que, dentre os parâmetros de determinação apresentados pelo Comitê, está a necessidade de considerar os efeitos de curto, médio e longo prazo das ações relacionadas ao desenvolvimento da criança. Decisões que levem em consideração o princípio do melhor interesse devem ser sempre baseadas em evidências científicas, incluindo o conhecimento das necessidades de desenvolvimento de crianças e os impactos de inovações tecnológicas (Livingstone et al., 2024). Além dos impactos em seus interesses atuais, é crucial que os controladores considerem os impactos do tratamento de dados em seus interesses futuros. Assim, o princípio do melhor interesse também deve ser entendido como um princípio de precaução, que requer a avaliação da possibilidade de risco e dano futuros e outras consequências da decisão para os direitos da criança (Committee on the Rights of the Child, 2013, parag. 74). Essa compreensão nos obriga a agir com cautela, mesmo quando o potencial perigo de uma determinada tecnologia não está totalmente estabelecido, mas há indicações de que não agir neste momento poderia causar danos. Isso é especialmente importante no caso de tecnologias cujos benefícios não são confirmados por evidências científicas (Lievens, 2021). Após a identificação do que é de melhor interesse da criança em determinado caso concreto (1º passo), é preciso ainda contrapô-lo com outros interesses e direitos de terceiros (2º passo). Nesta segunda etapa, o que foi determinado como o melhor interesse da criança no caso deve ser considerado com absoluta prioridade na decisão, inclusive em relação aos interesses dos pais (Brochado Teixeira & Rettore, 2024).","708725":"A fim de direcionar os agentes de tratamento a tratarem dados de crianças e adolescentes de acordo com o seu melhor interesse, para além das considerações elaboradas na resposta anterior, seria de extrema valia caso a ANPD determinasse, a priori, situações claras em que o melhor interesse da criança sempre prevalecerá, além de exemplos de situações limítrofes. Um exemplo claro de situação em que o melhor interesse da criança deve sempre prevalecer é o caso de interesses comerciais, que muito frequentemente não coincidem com os interesses e direitos de crianças. Destaca-se que um dos direitos previstos na Convenção, em seu art. 32(1), é o direito à proteção contra a exploração econômica. Devemos entender "econômico" como qualquer interesse material, como a busca de ganho ou lucro através da produção, distribuição ou consumo de bens e serviços. Já o conceito de "exploração" se refere a aferir vantagem injustamente de outros em benefício próprio. Isso abrangeria ações como manipulação, uso indevido, abuso, vitimização, opressão ou maus-tratos (Verdoodt, 2020, p. 98). Estes dois elementos podem ser identificados no ambiente digital e, de forma específica, nos principais modelos de negócio online. No seu Comentário Geral 25 (2021), o Comitê destacou como os interesses comerciais podem impactar negativamente os direitos das crianças à informação independente (para. 53), a liberdade de expressão (para. 61) e o direito das crianças de brincar (para. 110). Outros exemplos de direitos afetados pelo tratamento de dados para fins comerciais incluem direito à não discriminação, ao desenvolvimento, à saúde e à educação (Van Der Hof et al., 2020). Isso não significa que as empresas não devam obter retorno financeiro sobre os seus produtos, mas isso não deve basear-se em dados, uma vez que não devem ser vistos como uma mercadoria, especialmente no caso de crianças. No âmbito da Global Privacy Assembly, em sua Resolução sobre os Direitos de Crianças no Ambiente Digital, as Autoridades de Proteção de

Dados destacaram que os Estados deveriam promover regulações que proibissem a transmissão de dados de crianças para terceiros para fins comerciais, assim como práticas de publicidade que encorajam crianças a fornecer dados pessoais (Global Privacy Assembly, 2021). No âmbito da União Europeia, o Regulamento de Serviços Digitais (DSA, na sigla em inglês) proibiu, em seu art. 28(2), que plataformas perfilassem crianças a partir de seus dados pessoais com a finalidade de publicidade direcionada (o mesmo sendo aplicado para qualquer dado sensível, segundo o art. 26(3)) (União Europeia, 2022). Isso está diretamente ligado ao impacto do melhor interesse na caracterização do que é considerada uma finalidade legítima, a partir do art. 6º, I, da LGPD. O critério de legitimidade vai além da mera existência de base legal na LGPD e deve considerar a legalidade mais ampla do processamento de dados pessoais. Isso inclui, além do art. 14, da LGPD, todo o arcabouço jurídico de proteção de crianças e adolescentes. Assim, só deve ser considerada legítima a finalidade caso ela leve primordialmente em consideração o melhor interesse da criança. A ANPD pode ter um papel fundamental na definição de situações em que o melhor interesse sempre prevalecerá (como em relação a interesses comerciais), gerando interpretações proibitivas específicas. Ademais, também pode auxiliar agentes de tratamento a partir da elaboração de ferramentas práticas que ajudem controladores a realizar o exercício de balanceamento destacado na pergunta acima, como já feito, por exemplo, pela autoridade do Reino Unido após a elaboração de seu Age Appropriate Design Code (Information Commissioner's Office (ICO), 2024). Por fim, a discussão acerca do uso comercial de dados de crianças está diretamente ligada à necessidade de se regular de forma restrita o uso da base legal da proteção ao crédito para o tratamento de dados destes sujeitos (art. 7º, X, LGPD). Considerando que a função primordial desta base legal é a proteção de credores e interesses financeiros, não é possível imaginar cenários em que estes superariam a proteção do melhor interesse.","705523":"Assim como o consentimento exigido para o tratamento de dados sensíveis, o consentimento para o tratamento de dados de crianças mencionado no art. 14, §1°, LGPD, não deve apenas apresentar as mesmas características do consentimento para dados pessoais "comuns" (livre, informado e inequívoco), mas também ser específico e em destaque. Isso evidencia a intensão do legislador de incluir medidas adicionais de tutela na obtenção do consentimento para o tratamento de dados de crianças. Para que o consentimento seja específico, ele dever não somente estar ligado a uma finalidade determinada, o que já é um requerimento do art. 5º, XII, LGPD, mas, mais restritamente, a uma atividade de processamento de dados específica e bem definida. Assim, no caso de múltiplas operações de tratamento de dados para diversos fins, pais ou responsáveis legais deverão fornecer consentimento separadamente para cada uma dessas operações, possibilitando uma maior granularidade e implementação da autodeterminação informativa. Por outro lado, o requerimento de o consentimento ser em destaque está relacionado à necessidade de chamar a atenção do usuário de forma mais intensa acerca da decisão que ele está prestes a tomar. Isso pode ser feito através de recursos visuais, como cores diferentes, caixas de seleção destacada, pop-ups, ícones ou etiquetas virtuais que podem, inclusive, ser objeto de regulamentação da ANPD. Destaca-se a necessidade, por parte da ANPD, de esclarecer os requerimentos para o consentimento de adolescentes. Embora o legislador tenha permitido que os adolescentes consentissem sem representação ou assistência dos pais, como será defendido abaixo, essas duas salvaguardas

adicionais presentes no art. 14, §1º, LGPD, para o tratamento de dados de crianças não parecem ser, em um primeiro momento, aplicáveis a eles. Considerando que o princípio do melhor interesse deve ser aplicado a toda e qualquer pessoa de até 18 anos incompletos (isto é, a crianças e adolescentes na linguagem do ECA), é indispensável que os adolescentes também contem com essa proteção adicional. Isso é especialmente o caso considerando que eles terão apenas iniciado a sua jornada de maior autonomia na proteção de seus dados pessoais e é preciso considerar que decisões equivocadas poderão ser tomadas ao longo deste caminho. Portanto, considerando a intenção do legislador de oferecer mais proteção a crianças e adolescentes, não faz sentido tratar adolescentes como menos necessitados dos requisitos de um consentimento específico e destacado do que os pais ou responsáveis legais que consentem em nome de crianças. Por fim, em qualquer caso, é importante ressaltar que o consentimento não deve ser entendido como um mecanismo de legitimação do tratamento de dados de crianças e adolescentes como se adultos fossem. O consentimento é apenas uma das bases legais possíveis e todas as outras regras da LGPD, inclusive o caput do art. 14 continuam sendo aplicados. Ademais, sempre que possível uma análise individual da capacidade da criança poderá ser feita como melhor prática, a fim de verificar as suas capacidades para consentir de forma informada no caso concreto (DPC, 2021). ","708742":"De maneira geral, as diversas autoridades de proteção de dados ao redor do mundo têm interpretado o conceito de esforço razoável a partir de uma abordagem de proporcionalidade baseada em risco (cf. EDPB, 2020; Global Privacy Assembly, 2021). Assim, agentes de tratamento devem analisar todas as opções tecnológicas disponíveis no momento em questão e comparar os riscos e benefícios que elas apresentam com os riscos relativos ao tratamento de dados inicial que requer o consentimento. Esse processo deve estar sempre alinhado aos princípios da LGPD interpretados a partir do princípio do melhor interesse, como o princípio da necessidade. Caso o tratamento de dados para a atividade em questão gere um risco pequeno aos direitos fundamentais de crianças, os esforços podem se restringir a uma caixa de verificação de idade a partir, por exemplo, da requisição do ano em que o titular de dados nasceu. Após a verificação da faixa de idade, poderia ocorrer uma segunda etapa de envio de e-mail para o pai ou responsável para que este possa fornecer o consentimento. Exemplo claro seria o tratamento de um endereço de e-mail estritamente para o envio de newsletter acerca de um artista que a criança acompanha. Por outro lado, quando o tratamento de dados envolve riscos mais altos para os direitos da criança, os esforços de verificação da idade e, em seguida, do consentimento dado pelo pai ou responsável deve seguir parâmetros mais restritos (para mais detalhes, verificar abaixo a resposta à pergunta 2 da seção “III - Jogos e aplicações de internet”). Este é o caso, por exemplo, da necessidade de tratamento de dados sensíveis em uma situação relacionada à saúde da criança. Assim como na pergunta anterior, destaca-se a necessidade de a ANPD esclarecer que as mesmas regras se aplicam para adolescentes. Defende-se que os mesmos esforços razoáveis devem ser aplicados para a obtenção do consentimento do adolescente, quando este tiver mais de 12 anos, tendo em vista a sua vulnerabilidade. ","708745":"O art. 14, §1°, afirma que dados de crianças devem ser tratados com base no consentimento específico e em destaque dado por pelo menos um de seus pais ou representante legal. Essa regra também deve ser interpretada de acordo com o sistema jurídico brasileiro, em especial com o ECA e o regime das

incapacidades presente no Código Civil (CC). O CC apresenta dois níveis de capacidade legal: a chamada capacidade de direito (consequência da personalidade e inerente à condição de ser pessoa) e a capacidade de fato (ligada à capacidade de exercer validamente atos da vida civil por si só, sem a necessidade de um representante ou o assentimento de um assistente). O CC, define os indivíduos com menos de 16 anos como absolutamente incapazes (art. 3º) e indivíduos com idades entre 16 e 17 anos como relativamente incapazes (art. 4º). Assim, apesar de a Convenção reconhecer as capacidades em evolução e a autonomia progressiva da criança, um modelo estático puramente baseado na idade prevalece no sistema brasileiro. Todavia, ao longo do tempo, outros dispositivos buscaram mitigar a rigidez do CC, apresentando exceções ao regime geral de incapacidade civil, especialmente quando se trata de direitos da personalidade. Considerando a existência de outras exceções no sistema jurídico brasileiro e o fato de que a LGPD é posterior ao CC, é possível argumentar que o legislador de fato introduziu uma nova exceção, via lex specialis, permitindo que pessoas com 12 anos ou mais consintam para o processamento de seus dados pessoais sem representação ou assistência. Apesar de se defender que a LGPD introduziu uma exceção ao regime das incapacidades e que permite que adolescentes deem seu consentimento para o processamento de seus dados pessoais, é preciso recordar que isso se dá ao se privilegiar a autonomia e o desenvolvimento progressivo das capacidades da criança e do adolescente. Ao se desenvolver e adquirir novas capacidades, crianças adquirem, também, mais responsabilidade e autonomia para lidar com os seus próprios direitos e matérias relativas à sua vida. Isso é extremamente importante no ambiente digital e o envolvimento de crianças com matérias de proteção de dados pessoais, paulatinamente, é essencial para o desenvolvimento de sua literacia digital. Todavia, é destaca-se que este deve ser enxergado como um processo que beneficia a própria criança e não como uma justificativa para o tratamento de dados que seja contrário ao seu melhor interesse. Nesse sentido, com o reconhecimento que adolescentes podem consentir com o tratamento de seus dados pessoais, métodos de verificação da idade para a introdução de regras mais rígidas e padrões de design específicos para a sua navegação online se tornam ainda mais importantes. Por fim, importa destacar que a exceção ao regime das incapacidades disposta no art. 14, §1º, da LGPD, deve ser entendida restritivamente e aplicada exclusivamente ao consentimento fornecido para o processamento de dados pessoais. Assim, isso não deve impactar a análise de legalidade e o regime de consentimento dado para a celebração de contratos eletrônicos (incluindo Termos de Uso) ou consentimento ético quando, por exemplo, de processamento de dados para finalidade de pesquisas científicas (Teffé & Fernandes, 2022). Isso demonstra a importância de momentos separados, na experiência do usuário, para o consentimento fornecido em contrato eletrônico e o consentimento fornecido para o processamento de dados pessoais. Isso deve ocorrer não apenas pela necessidade de transparência e para que o consentimento seja considerado livre e em destaque, mas também porque pode haver situações em que pais ou responsáveis devem assistir ou representar o adolescente no consentimento para a celebração de contrato, mas em que o adolescente já pode dar consentimento para o processamento de dados pessoais (quando o este tem, por exemplo, entre 12 e 18 anos).","705539":"O especial estágio de desenvolvimento de crianças e adolescentes os caracterizam como uma maior vulnerabilidade e demanda que todos os atores da sociedade estejam ativamente envolvidos

na promoção (e não apenas proteção) de seus direitos, assim como definido pelo art. 227, CRFB. Muitos dos riscos do ambiente online são apenas o resultado de crianças e adolescentes utilizando tecnologias que não foram desenvolvidas para eles (5Rights Foundation, 2021b; Kidron & Rudkin, 2017). Isso faz com que medidas específicas sejam necessárias por design e por padrão não apenas para proteger crianças de riscos, mas para fornecer a elas um ambiente saudável e empoderador para o seu desenvolvimento em todas as áreas. Apesar da importância da agência de crianças e adolescentes, assim como de seus pais e responsáveis, a ubiquidade e complexidade das tecnologias atuais faz com que medidas individuais sejam extremamente insuficientes para o controle de dados pessoais. Essa proteção deve ocorrer de forma coletiva e agir diretamente na arquitetura das plataformas. Nesse sentido, propõe-se segmentar potenciais ações como medidas de restritivas de proteção, que proíbem ações específicas por parte de agentes de tratamento e medidas proativas de proteção, que estão diretamente relacionadas às configurações práticas da aplicação. Embora os limites entre essas categorias não sejam rigorosamente definidos, essa distinção pode ser útil na criação de uma checklist de medidas e salvaguardas a serem implementadas. Em ambos os casos, essas medidas podem ser incorporadas no design ou configuradas por padrão, diretamente no código da aplicação. Dentre as medidas restritivas de proteção encontram-se proibições específicas de tratamento de dados que são sempre contrários ao princípio do melhor interesse, como para fins de manipulação comercial ou política; publicidade direcionada; exploração da vulnerabilidade e atenção da criança (especialmente através de padrões abusivos e dark patterns); direcionamento de conteúdo danoso etc. Também inclui limitações severas ao perfilamento; à vigilância; à coleta de dados específicos como dados sensíveis ou de geolocalização; ao compartilhamento de dados com terceiros; e à retenção de dados pessoais. Dentre medidas proativas de proteção pode-se citar a implementação por padrão das configurações de privacidade mais protetivas; a anonimização ou pseudoanonimização sempre que possível; a minimização extrema do uso de dados pessoais (ver interpretação ao art. 14, §4º, infra); a criação de interfaces inclusivas e seguras; a implementação de sistemas de monitoramento de atividades suspeitas ou alertas para controle dos pais; e o ajuste do design de acordo com as idades e capacidades da criança e do adolescente. Estas medidas podem ser consideradas como um resumo do estado da arte existente e já exigido em prática por autoridades e instituições ao redor do mundo (Nesse sentido, cf. Australian eSafety Commissioner, 2024; CNIL, 2021; D4CR Association, 2024; Digital Futures Commission, 2023; DPC, 2021; ICO, 2020; IEEE, 2021; International Telecommunication Union, 2020; Ministerie van Binnenlandse Zaken en Koninkrijsrelaties et al., 2021; Nordic Data Protection Authorities, 2024; Perrino, 2022). ","708762":"Os processos de verificação da idade em três categorias e cada uma possui níveis de efetividade e riscos aos direitos fundamentais diferentes. A declaração da idade pode incluir diversos métodos como clicar em uma caixa em que o usuário declare que possui mais de “x” anos, informar que está em determinada faixa etária (entre “x” e “y” anos) ou fornecer diretamente sua data de nascimento. Esse é o método menos intrusivo, mas a possibilidade de contorna-lo ou burlá-lo é alta e crianças podem mentir a idade. Isso pode ser evitado, por exemplo, através de um segundo fator de verificação como envio de e-mail para pais, social vouching (quando um terceiro confirma a idade do usuário), uso de cartão de crédito etc. Ademais,

medidas de design ou controle parental podem fazer com que essa modalidade seja mais segura. A estimação da idade tem como função estimar a idade do usuário através de métodos como perfilamento de comportamento online, análise de dados biométricos, ou testes de capacidade. Exceto quando se adota o método de teste de capacidade, a estimação de idade necessariamente demanda a coleta de mais dados do usuário (Sas & Mühlberg, 2024). Na resposta à próxima pergunta, será discutida, de forma específica, a problemática relativa ao perfilamento de crianças e adolescentes, que deve ser evitado e utilizado apenas quando indispensável para a realização do seu melhor interesse. Isso inclui não apenas a mera necessidade (o que poderia ser argumentado no caso da verificação de idade), mas também a proporcionalidade deste benefício em relação aos riscos que este método impõe a outros direitos fundamentais. O tratamento de dados biométricos para a estimação de idade apresenta ainda mais desafios devido à sua alta sensitividade. Ademais, esse é uma modalidade ainda falha, podendo ser contornada facilmente, funcionando inadequadamente para pessoas negras (European Digital Rights (EDRi), 2023) e não fornecendo uma estimativa precisa da idade do usuário (métodos atuais anunciam uma margem de erro de aproximadamente 1,5 ano — cf. Pôle d'Expertise de la Régulation Numérique (PEReN), 2022). Por fim, há ainda a possibilidade de verificação da idade por documento oficial. Este é o método mais acurado e geralmente é levado à cabo através do scan ou imagem digital do documento (podendo ser integrado com chamada ao vivo com participação de humanos para confirmação — European Commission et al., 2024). Todavia, esse método também apresenta diversos desafios. Isso inclui a exclusão digital daqueles que não possuem acesso a documentação oficial, assim como o fim da anonimidade neste ambiente e da normalização de age gates em qualquer interação online. Ademais, também cria riscos de vazamento de dados, roubo de identidade e utilização dos dados para outros fins. Ao menos em teoria, já existem métodos que buscam solucionar alguns dos problemas identificados acima, como os baseados em "zero-knowledge proof". Neste modelo, é possível que indivíduos provem a acurácia de certa informação (que possuem certa idade, por exemplo, sem revelá-la ou revelar sua identidade. Isso é idealmente feito através de um sistema independente fornecido por terceiros. Esse modelo ideal já foi, por exemplo, discutido pela autoridade francesa de proteção de dados em 2022 (CNIL, 2022). Ainda não há ainda uma solução perfeita e universal para o problema. Todavia, já é possível argumentar que certos modelos são extremamente invasivos e não acurados, devendo ser rechaçados. Esse é o caso por exemplo, de métodos de estimação de idade. Ademais, métodos tradicionais de verificação através de documentos oficiais devem ser utilizados apenas quando extremamente necessários, devido ao grande risco imposto a todos os usuários. A declaração de idade continua sendo o método menos invasivo e os seus desafios podem ser contornados, em certos casos, através de verificação em duas etapas. Por fim, é preciso incentivar o desenvolvimento de métodos seguros e protetivos à proteção de dados pessoais baseados em zero knowledge proof, algo que no Brasil poderia ser feito, por exemplo, através da parceria da ANPD com o sistema gov.br.","708764":"O art. 6º, III, da LGPD, determina que o tratamento de dados pessoais deve ser restringido ao mínimo necessário, relevante, proporcional e não excessivo para alcançar os fins especificados pelo controlados. No entanto, além de reforçar esse princípio, é possível argumentar que o art. 14, §4º, vai além ao utilizar a expressão "estritamente

necessário para a atividade" (grifo nosso). De maneira geral, princípio da necessidade disposto no art. 6º está intrinsicamente relacionado ao princípio da finalidade e não existe por si só. Isto é, o que é considerado necessário sempre dependerá da finalidade para o tratamento de dados pessoais (que, como discutido acima, deve estar alinhada ao melhor interesse da criança e do adolescente para ser legítima). Assim, caso a finalidade seja legítima e o controlador tenha uma base legal para tratar os dados necessários para essa finalidade, basta que a anuncie em sua política de privacidade e esteja em conformidade com o restante da LGPD. Todavia, o art. 14, §4º, LGPD, apresenta regra mais restritiva para o tratamento de dados de crianças (titulares de que se trata o §1º do art. 14). Este dispositivo dispõe que os controladores não deverão condicionar a sua participação em jogos, aplicações de internet ou outras atividades ao fornecimento de informações para além das estritamente necessárias à atividade. O legislador cita jogos e aplicações de internet como exemplos de atividades (tendo em vista os ter inserido logo antes da expressão "ou outras atividades"). Assim, entende-se que não se trata de dados necessários a determinada finalidade de tratamento de dados, mas sim de dados necessários para a aplicação prática ou funcional específica, para o serviço ou produto mais amplo que requer o tratamento de dado pessoal. Embora essa atividade possa envolver diversas finalidades de tratamento, os dados coletados, observados ou inferidos devem ter uma relação direta com a atividade em questão. Apenas mencionar outras finalidades não é suficiente para coletar dados além dos principais objetivos da aplicação. Pode-se pensar na situação de tratamento de dados pessoais em uma aplicação com fins educacionais. O tratamento deve ser reservado estritamente para possibilitar o funcionamento básico da aplicação para os fins educacionais, não sendo possível tratar dados, por exemplo, para direcionamento de publicidade, melhoramento de outros serviços ou treinamento de sistemas de inteligência artificial, seja por parte do controlador, seja de terceiros. Isso deve ocorrer mesmo que a finalidade seja legítima, pois a análise da conformidade com os diferentes princípios deve ocorrer de forma separada. Esta é uma regra extremamente importante no âmbito da LGPD, que protege os dados das crianças desde o momento da coleta e impede que sejam acumulados em larga escala para fins não relacionados ao propósito principal da aplicação ou jogo em que a criança está envolvida. Portanto, os dados pessoais coletados devem aderir estritamente ao que é indispensável e justificável (Zanatta et al., 2021), o que também está alinhado ao princípio da boa-fé. Por fim, o perfilamneto pode ocorrer para diversos fins. Ele não seria compatível com o melhor interesse quando é realizado para fins comerciais. Todavia, ele pode ocorrer para outras finalidades, como no caso de tecnologias de educação que buscam aplicar metodologias de ensino personalizado. Neste caso, é essencial que o agente de tratamento demonstre que este perfilamento de crianças é indispensável para alcançar uma finalidade consistente com o seu melhor interesse. Ademais, essa indispensabilidade deve ser baseada em evidências científicas claras e no princípio da precaução. Isso, pois o perfilamento em si, independentemente da finalidade de tratamento, pode afetar diretamente diversos direitos fundamentais de crianças. Riscos dessa automaticidade vão desde o vazamento de dados e roubo de identidade, até a limitação de oportunidades devido a erros e vieses (Van Der Hof et al., 2020). Nesse sentido, em seu Comentário Geral Nº 25, o Comitê (2021, parag. 42) defende que Estados Membros proíbam o uso de perfilamento de crianças e adolescentes para

fins comerciais.","708768":"O controle parental pode ser entendido como qualquer medida utilizadas por pais ou responsáveis legais para adaptar a experiência online de crianças e adolescentes. Isso pode ser feito, por exemplo, através de mecanismos de imposição de limites de uso, como temporizadores e bloqueios de determinados sites, ou então do controle de acesso a informações da criança ou adolescente por determinado website. Esta é uma forma extremamente importante de incluir pais e responsáveis na proteção de direitos de crianças e adolescentes online, assim como demandado pelo art. 227, da CRFB. Todavia, é preciso reconhecer, também, os seus limites. O primeiro limite a ser reconhecido diz respeito à relação estabelecida entre as partes envolvidas. Crianças e adolescentes também precisam de um espaço de privacidade em relação aos seus pais ou responsáveis para que possam desenvolver sua identidade de maneira saudável. Portanto, qualquer medida adotada nesse sentido deve ser sempre necessária e proporcional, levando em consideração o princípio do melhor interesse. Essas medidas devem ser transparentes, de modo que crianças e adolescentes estejam cientes de que suas experiências estão sendo monitoradas ou moldadas de alguma forma. A comunicação sobre essas medidas também deve ser adequada à idade e às capacidades da criança ou adolescente, respeitando sua autonomia progressiva. O segundo limite refere-se à própria função do controle parental. A existência de controles parentais ou a possibilidade de ajuste das configurações de privacidade por pais ou responsáveis não deve servir como justificativa para padrões de design que não estejam alinhados com o melhor interesse da criança, nem para transferir aos pais a responsabilidade de decidir sobre questões complexas de tratamento de dados. Assim, as decisões tomadas por pais ou responsáveis devem ser sempre secundárias a designs que protejam, por padrão, os interesses da criança e do adolescente.","708772":"A disponibilização de informações de maneira clara e acessível para crianças e adolescentes sobre o tratamento de seus dados pessoais desempenha um papel crucial no reconhecimento desse grupo como sujeitos de direitos, que, desde o início, foi o principal objetivo da Convenção. Embora esses direitos muitas vezes sejam exercidos com a representação ou assistência de pais ou responsáveis legais, eles continuam a pertencer, em essência, às crianças e adolescentes. Adaptar a comunicação sobre o tratamento de dados pessoais é o primeiro passo para empoderar esses indivíduos no ambiente digital, auxiliando-os a desenvolver a literacia digital, a compreender o impacto negativo e positivo do tratamento de dados em seus direitos e, em última análise, a exercê-los de forma consciente. De toda forma, porém, é preciso enxergar essa realização do princípio da transparência como a base mínima para a proteção dessas pessoas no ambiente digital, sem que isso signifique transferir de forma completa a responsabilidade pela proteção de dados para as crianças ou seus pais e responsáveis. Diversas instituições ao redor do mundo já se debruçaram sobre o tema e a ANPD pode se beneficiar de trabalhos que buscaram estudar a compreensão de crianças e adolescentes sobre informações acerca do tratamento de seus dados pessoais. Isso não quer dizer, porém, que os resultados dessas análises possam ser aplicados, diretamente, à realidade brasileira, o que demandaria, por parte da autoridade, estudos empíricos específicos com crianças do país para confirmar a eficácia destes métodos. De toda forma, acredita-se que muitos dos princípios básicos possam ser aproveitados. Tendo em vista a complexidade do tema e a falta de espaço adequado para a discussão de todas as suas nuances, indica-se como ponto de partida o trabalho recente realizado por Sas, Denoo e Mühlberg (2023), que

mapearam as diversas estratégias de comunicação apropriada à idade sugeridas por autoridades de proteção de dados, organizações de proteção à criança e adolescente, assim como a literatura científica. Essas estratégias são classificadas em sete categorias que fazem parte de uma matriz de avaliação: linguagem, tamanho, formato de comunicação, acessibilidade, técnicas de nudge, momento e envolvimento parental. Apesar de nem todas as estratégias serem específicas para crianças, estas podem se beneficiar enormemente de sua implementação. Por fim, é essencial lembrar que todas essas estratégias devem levar em conta a diversidade dentro do grupo de crianças e adolescentes, reconhecendo que diferentes faixas etárias possuem entendimentos e necessidades distintas. Assim, a comunicação deve ser adaptada de acordo com o público-alvo. Por exemplo, crianças de até cinco anos têm um nível de compreensão e necessidades específicas, dependendo muito mais de seus pais ou responsáveis do que adolescentes de 15 anos, que já possuem maior autonomia e capacidade de lidar com questões relacionadas à própria vida. Portanto, é crucial que a abordagem seja ajustada para atender adequadamente às diferentes etapas de desenvolvimento, garantindo que todos recebam a informação de maneira eficaz e apropriada.","708775":"Para além das questões já discutidas acima, indica-se uma atenção especial à regulação dos seguintes temas: • O exercício dos direitos de titulares por crianças; • A realização do RIPD e a sua relação com o CRIA; • A regulação de bases legais específicas, como a interpretação do que significa tratar dados para a proteção da criança, conforme art. 14, §3º, LGPD; • A regulação do uso de bases legais do art. 7º, LGPD, como execução de contrato ou proteção ao crédito; • O tratamento de dados em situações específicas, como no âmbito da educação (incluindo regras sobre a inclusão de medidas de proteção de crianças por design em processos licitatórios); • Medidas especiais de cyber segurança para a proteção de dados de crianças e adolescentes; • Medidas de educação digital para pais e responsáveis para a sua conscientização dos problemas relacionados à divulgação excessiva de dados e da imagem de crianças e adolescentes (over-sharenting).

Contribuinte: ELORA RAAD FERNANDES

Número: OP-752923

Data: 15/08/2024 - 21:21

Resumo: :"É importante que a ANPD reconheça que não existe uma regra única para a aplicação do princípio do melhor interesse, mas depende de uma análise contextual a depender das atividades do controlador. É recomendado que a ANPD reconheça a pluralidade de agentes e forneça orientações suficientemente flexíveis para que os controladores possam avaliar a aplicação do princípio do melhor interesse dentro de seus modelos de negócios. É preciso considerar que as crianças e adolescentes possuem desenvolvimento diverso, sendo primordial a observação de que há diferenças entre crianças e adolescentes, em termos de desenvolvimento psicológico, pedagógico, educacional, físico e biopsíquico. Assim, a ANPD deve fornecer orientações capazes de endereçar de maneira apropriada as diferentes etapas de desenvolvimento desses diferentes públicos, que não podem ser tratados de maneira indistinta sob pena de contradizer a própria natureza de melhor interesse. Tal análise deve ser pautada

pela multidimensionalidade, pois não envolve apenas a proteção dos dados, mas também outros direitos, como a segurança. Deve-se também levar em conta as diferentes características e experiências de um grupo heterogêneo tendo flexibilidade suficiente para ser adaptável ao desenvolvimento dos vários indivíduos que o compõem. As regulamentações devem refletir a crescente maturidade dos adolescentes, permitindo-lhes maior autonomia e acesso aos benefícios online sem restrições desnecessárias. O princípio da autonomia progressiva sugere que os adolescentes devem poder dar consentimento para o tratamento de dados, quando esta for a base legal mais adequada, sem a assistência dos pais, uma vez que requisitos de consentimento excessivamente restritivos podem excluí-los de serviços online valiosos. Portanto, métodos regulatórios mais flexíveis e inclusivos são recomendados para garantir experiências online seguras e apropriadas para cada faixa etária, protegendo crianças e adolescentes na internet, enquanto permite que eles aproveitem ao máximo a tecnologia. Devendo, assim, ser considerados os seguintes pontos em especial: a)Autonomia Progressiva: À medida que os adolescentes amadurecem, deve-se permitir que eles tenham mais autonomia na gestão de seus dados pessoais, respeitando sua capacidade crescente de tomar decisões informadas; b)Consentimento pessoal pelo adolescente: Nos casos em que a base legal do consentimento for utilizada, oferecer aos adolescentes a oportunidade de dar seu próprio consentimento, com a orientação e o apoio dos pais ou responsáveis, para ajudá-los a entender as implicações. Ressalta-se que, nos termos do Enunciado nº 1/2022 da ANPD, o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base em todas as bases legais previstas na LGPD, desde que observado e prevalente o seu melhor interesse, a ser avaliado no caso concreto; c)Equilíbrio entre segurança e privacidade: É preciso proporcionar um equilíbrio entre a necessidade de segurança e a importância da privacidade, permitindo que os adolescentes compreendam e gerenciem suas próprias informações pessoais de maneira responsável; d) Ferramentas de gerenciamento de dados: Devem ser fornecidas ferramentas e recursos que permitam aos adolescentes gerenciar seus dados de forma eficaz, incluindo a capacidade de visualizar, corrigir e excluir informações pessoais. Uma perspectiva contextual e flexível do melhor interesse permite que o princípio seja responsivo à condição peculiar de pessoa em desenvolvimento das crianças e adolescentes, destacada acima. Além disso, outros elementos poderão ser considerados pelo controlador para determinar o melhor interesse de forma concreta como, por exemplo, quais dados são tratados, finalidade do tratamento, possíveis benefícios e danos decorrentes do tratamento, dentre outros. De toda forma, seria relevante que a Autoridade consolidasse entendimento no sentido de que a determinação do melhor interesse exige, necessariamente, uma análise do caso concreto e suas circunstâncias específicas, bem como de outros direitos e interesses envolvidos.","708725":"De acordo com o Comentário Geral 14 do Comitê sobre os direitos da Criança, o princípio do melhor interesse é “um conceito dinâmico que requer uma avaliação adequada do contexto específico”. O princípio e o conceito do melhor interesse são complexos e, por si só, demandam uma análise contextualizada. Além disso, alguns contextos específicos que já receberam atenção da Autoridade no Guia de Legítimo Interesse demandam cautela, como por exemplo, o tratamento de dados pessoais para publicidade. Vale destacar que a publicidade online para menores é uma atividade lícita e regulamentada: o Código de Defesa do Consumidor (“CDC”), em seu artigo 37, veda a publicidade enganosa

ou abusiva, estabelecendo que seria abusiva aquela publicidade que se aproveita da deficiência de julgamento e experiência da criança. Em complemento, o Código Brasileiro de Autorregulamentação Publicitária CONAR conta com dispositivo voltado especialmente a estabelecer parâmetros éticos que devem ser considerados em anúncios voltados a este público (artigo 37). Entende-se que no cenário de tratamento de dados pessoais para publicidade, o princípio do melhor interesse deve considerar os diferentes níveis ou fases de maturidade ao longo da infância e da adolescência. Essa visão é corroborada pelo Comitê sobre os Direitos da Criança em seu Comentário 20, no qual afirma que as abordagens adotadas para concretizar os direitos dos adolescentes distinguem-se significativamente daquelas adotadas para crianças e que, mesmo dentro de cada nicho, existem diferentes fases de desenvolvimento. Por tal razão, a adoção de práticas genéricas para crianças e jovens são inadequadas e os colocam num grande nicho impreciso e vago. Justamente por esse motivo, algumas plataformas digitais desenvolvem serviços personalizados com políticas diferenciadas para tratamento de dados pessoais para publicidade de crianças e adolescentes. Outra que demanda atenção é a interação do princípio do melhor interesse com o legítimo interesse do controlador ou terceiro quando analisados diante de novas práticas, como a coleta de dados para treinamento de sistemas de Inteligência Artificial. De acordo com o Enunciado CD/ANPD 1/23, o tratamento de dados pessoais de crianças e adolescentes pode ser realizado nas hipóteses legais dos artigos 7° e 11° da LGPD, entre elas o tratamento de dados poderá ser feito “quando necessário para atender os interesses legítimos do controlador ou terceiro [...]”. Dentre os argumentos favoráveis para o tratamento de dados pessoais com fundamento no legítimo interesse está a maior flexibilidade e o aumento das hipóteses de acordo com a diversidade de situações concretas e complexas que surgem com as novas tecnologias. Assim, diante das novas situações surgidas nos últimos anos, sobretudo questões envolvendo o tratamento de dados para treinamento de sistemas de IA por plataformas digitais e a relevância da base legal do legítimo interesse para este cenário, torna-se crucial que não se adote uma perspectiva restritiva sobre o uso dessa base legal. As plataformas digitais e a legislação local devem garantir a transparência e compreensibilidade das crianças e adolescentes e de seus pais e responsáveis sobre o tratamento de seus dados pessoais. Isso também envolve a discussão e um melhor esclarecimento sobre o consentimento informado. Recomendações personalizadas são essenciais para fornecer conteúdo apropriado para a idade, pois ajudam a garantir o acesso a materiais adequados, permitindo que os desenvolvedores criem produtos mais seguros e apropriados para diferentes faixas etárias. Regulamentações excessivamente restritivas neste campo podem limitar a capacidade das empresas de inovar e aprimorar essas ofertas, potencialmente prejudicando o apoio aos jovens usuários. Ainda merece destaque questões envolvendo tratamento de dados para prevenção de riscos e segurança on-line de crianças e adolescentes. Algumas plataformas digitais utilizam dados pessoais com a finalidade de proteger crianças e adolescentes em situação de cyberbullying, abuso sexual e outros riscos on-line. O tratamento de dados pessoais nessas situações demonstra como, por vezes, o tratamento é necessário.
","705523":"Preliminarmente é importante salientar que o consentimento detalhado pelo §1º do artigo 14 da LGPD diz respeito às crianças, isto é, não se estende aos adolescentes. Além disso, é relevante rememorar que o consentimento não é a única base legal disponível para o

tratamento de dados pessoais de tal público, entendimento esse que inclusive corresponde àquele firmado por esta Autoridade no Enunciado nº 1 de 2023. No Estudo Preliminar que embasou tal entendimento, a Autoridade trouxe uma série de argumentos que contrariam o entendimento de que o consentimento seria sempre a base legal mais apropriada ou adequada, são exemplos: o consentimento pode ser fornecido em contrariedade ao melhor interesse; atribuição de ônus excessivo aos pais ou responsáveis legais; inviabilização de certos tratamentos; etc. A questão envolvendo a obtenção do consentimento dos usuários é complexa não apenas em contextos que envolvem dados de crianças. A obtenção do consentimento assumiu um papel central nas discussões sobre segurança e privacidade e é, muitas vezes, tratado como o principal mecanismo para a proteção dos dados pessoais. Ocorre que o processo de obtenção do consentimento atualmente possui diversas insuficiências, por tal razão, é necessário reavaliá-lo e repensá-lo para funcionar de maneira mais eficaz. Inicialmente, cabe destacar que é preciso que haja a apresentação clara e completa do aplicativo, seus objetivos, funcionalidades e como os dados pessoais serão utilizados para que os pais e responsáveis tenham clareza do que estão consentido. Após, podem ser disponibilizados diversos e variados mecanismos e procedimentos para que o consentimento seja fornecido de forma clara e responsável. Caso haja uso de formulários, este deve ser detalhado e acessível, evitando jargões técnicos que possam confundir os pais ou responsáveis. A obtenção do consentimento específico e em destaque de pais ou responsáveis legais deve observar alguns critérios e parâmetros para que se garanta uma proteção efetiva. Tais critérios e parâmetros devem ser desenvolvidos tendo como foco a correção das insuficiências na obtenção do consentimento, que são: a) Limitações cognitivas do titular dos dados pessoais e dos pais ou responsáveis na ponderação entre custo-benefício: A obtenção do consentimento deve ser informada, ou seja, os pais/responsáveis somente poderão tomar a decisão de consentir ou não se com conhecimento sobre tratamento dos dados pessoais. Essa obtenção informada e consciente também pode ser concretizada por meio de critérios adicionais, como o fornecimento de informações educativas visuais, cartilhas, manuais e outros documentos sucintos que discutam a importância da privacidade e o papel dos pais e responsáveis, bem como a adoção de uma linguagem clara, simples e compreensível. b) Manifestação de vontade livre: A obtenção do consentimento específico e em destaque dos pais ou responsáveis deve incorporar parâmetros que reforcem e/ou melhorem a privacidade, devendo ser pensadas e desenvolvidas sempre considerando a privacidade e a segurança das crianças e dos adolescentes (Privacy by Design). Citamos alguns critérios e parâmetros para a obtenção do consentimento que se mostram adequados: • Destacamento e visibilidade: deve-se garantir que o pedido de consentimento esteja explícito e separado de outros assuntos gerais. • Melhores esforços para verificação da identidade e autoridade dos pais/responsáveis: Outro critério deve estar relacionado ao emprego dos melhores esforços para a verificação da identidade e autoridade dos pais e responsáveis legais por meio de técnicas não invasivas como a disponibilização do e-mail ou a realização de perguntas apropriadas. Essas perguntas incluem informações pessoais que apenas os pais e responsáveis seriam capazes de responder. ","708742":"Salientamos que os métodos para verificação do consentimento parental são realizados de acordo com as limitações técnicas para a sua aplicação e o estado da técnica da tecnologia disponível. Os

mecanismos de verificação da idade podem ser adotados normalmente são usados para averiguar se o consentimento foi realmente fornecido pelos pais ou responsáveis em conjunto com outras medidas. Para isso, podem ser usados formulários com questionamentos que crianças de determinada idade não conseguiriam responder, de forma que são capazes de determinar se o consentimento está sendo fornecido por um adulto. O mecanismo pode ser utilizado no primeiro acesso, autorizando os acessos subsequentes. O controle pode ser aplicado no momento do cadastro do usuário, na própria página do primeiro acesso ou enviada para o e-mail do responsável para apurar a autenticidade da informação - ideal para casos que envolvem dados sensíveis ou conteúdos específicos. Outra ferramenta que pode ser utilizada é a inclusão de campos para que os pais ou responsáveis leiam e assinem digitalmente o consentimento, confirmando que compreenderam todas as informações fornecidas. O uso de código de autorização também pode ser uma ferramenta mais simples e confiável para que o consentimento dos pais seja explícito e confiável. Neste sentido, a plataforma envia um código único para o e-mail ou telefone dos pais ou responsáveis, que deve ser inserido no aplicativo ou serviço para concluir o processo de consentimento. Em caso de aplicativos mais complexos ou que possam envolver a comunicação ou interação dos usuários, existe a possibilidade de que juntamente com o código, seja enviada uma explicação detalhada sobre o aplicativo ou serviço e as razões para a necessidade do consentimento. Os códigos únicos garantem que apenas os pais ou responsáveis autorizados possam conceder consentimento. Todas as ferramentas acima elencadas são aplicadas, como regra, em cada um dos serviços ou aplicativos, o que exige múltiplas ações dos pais ou responsáveis. Por isso, pode se mostrar interessante uma solução que possa ser amplamente adotada pelo setor privado, promovendo a colaboração entre os diferentes atores do ecossistema digital. Apontamos a possibilidade de a verificação ser realizada no momento da habilitação do telefone ou computador e a configuração de contas ou IDs de usuários no nível do sistema operacional ou da loja de aplicativos. Ao utilizar deste mecanismo para a verificação e o registro da permissão e consentimento dos pais ou responsáveis, já restam definidos os parâmetros para o uso do dispositivo, utilizando ferramentas de controle e supervisão parental. Essas informações poderiam ser comunicadas e repassadas aos demais participantes do ecossistema, como desenvolvedores e fornecedores de aplicativos, para garantir que sejam implementadas e observadas na oferta de produtos e serviços no nível dos aplicativos. Seria um ponto de partida comum, proporcionando maior eficiência e uniformidade na verificação da idade. É importante ressaltar que, de acordo com as características específicas de cada aplicativo e ferramenta disponível, níveis adicionais de controle e supervisão parental podem ser desenvolvidos especificamente. Essa ação permite uma atuação transversal contribuindo para a privacidade e minimização do tratamento de dados, ao reduzir a coleta de informações em vários aplicativos. De toda forma, assim como vem se consolidando na prática internacional, sugere-se que a ANPD reconheça que a escolha do mecanismo a ser usado para a verificação do consentimento parental deve se guiar por uma análise de risco e considerar as tecnologias existentes. Além disso, é preciso reconhecer que não existe uma solução única para a verificação do consentimento parental e que certas ferramentas podem ser mais ou menos adequadas a depender da plataforma que a emprega. Ainda, é relevante admitir que não existe solução infalível e que todas as ferramentas existentes terão prós e contras e

estarão sujeitas a falhas. ","708745":"A obtenção do consentimento de adolescentes para o tratamento de seus dados pessoais no ambiente digital é um tema complexo, que envolve o equilíbrio entre a proteção dos direitos dos jovens e o respeito à sua autonomia progressiva. Aplicar o princípio da autonomia progressiva, especialmente em consonância com o princípio do melhor interesse, traz benefícios significativos para o desenvolvimento dos adolescentes. A perspectiva mais adequada é aquela baseada em diversos fundamentos e áreas, que vão desde a visão da psicologia e da pedagogia, até a visão integral e holística do adolescente. Os adolescentes, especialmente na fase da adolescência média (entre 14 e 17 anos), começam a desenvolver habilidades cognitivas avançadas, incluindo pensamento abstrato, raciocínio lógico e capacidade de tomar decisões informadas. De acordo com o Comentário Geral 20 do Comitê sobre os direitos das Crianças, esse processo de desenvolvimento cognitivo e físico na adolescência é, na maioria das vezes, influenciado e exacerbado pelo ambiente digital. Ao permitir que esses adolescentes forneçam consentimento para o tratamento de seus dados pessoais, estamos reconhecendo e valorizando essas capacidades cognitivas emergentes, o que contribui para o fortalecimento de sua autoestima e senso de responsabilidade, entre outros benefícios na formação de sua personalidade. A autonomia progressiva é fundamental para o desenvolvimento de indivíduos críticos e conscientes. A educação moderna defende a ideia de que os adolescentes devem ser incentivados a participar ativamente nas decisões que os afetam, o que inclui o consentimento para o uso de seus dados pessoais. Esse envolvimento não apenas promove o aprendizado sobre direitos e responsabilidades digitais, mas também prepara os jovens para a vida adulta, onde tomarão decisões independentes e informadas. A autonomia progressiva e a consideração integral do indivíduo, que trata o adolescente como um ser em desenvolvimento, com capacidades e direitos que evoluem ao longo do tempo proporciona mais autonomia na medida em que o adolescente amadurece, reconhecemos a importância de sua participação ativa em questões que impactam sua vida. De acordo com o Comentário Geral 20 do Comitê sobre Direitos das Crianças, os adolescentes estão na vanguarda dos ambientes digitais e as plataformas digitais têm um papel formador essencial para sua educação, cultura e envolvimento político. Isso não significa ausência de orientação, mas sim uma transição gradual onde o papel dos pais ou responsáveis passa de controlador para orientador, permitindo ao adolescente exercer sua autonomia em contextos apropriados. O princípio do melhor interesse do adolescente, consagrado em diversos instrumentos legais e diretrizes internacionais, inclusive pela ANPD e a LGPD, reforça a ideia de que as decisões devem ser tomadas considerando o bem-estar e o desenvolvimento integral do jovem. Permitir a autonomia progressiva no consentimento para o tratamento de dados pessoais não apenas respeita esse princípio, mas também promove um ambiente onde os adolescentes se sentem valorizados e respeitados como indivíduos capazes. A autonomia progressiva, conforme positivada pela legislação brasileira, deve levar a uma redução gradual da interferência parental, respeitando a crescente capacidade dos adolescentes de exercerem seus direitos de forma independente. Portanto, é possível que adolescentes forneçam consentimento no ambiente digital sem a necessidade de representação ou assistência expressa dos pais, alinhando-se ao princípio do melhor interesse. Implementar a autonomia progressiva requer a criação de diretrizes claras que definam os contextos e as idades apropriadas para que os adolescentes possam fornecer consentimento

sem a necessidade de representação ou assistência. Isso pode incluir, por exemplo, um sistema escalonado de controle e supervisão parental. Os controladores no ambiente digital devem aplicar em suas políticas, termos de uso ou diretrizes a serem seguidas normas claras neste sentido. Além disso, devem criar mecanismos de verificação da progressividade da idade e, consequentemente, da autonomia aplicável ao caso concreto.","705539":"Para garantir o tratamento adequado de dados pessoais de crianças e adolescentes no ambiente digital, alguns princípios basilares da LGPD se tornam ainda mais relevantes, de forma que devem estar presentes em todas as aplicações da internet. O artigo 6º, I, II e III da LGPD traz a previsão dos princípios da finalidade, necessidade e adequação que limitam o tratamento ao mínimo necessário para fins específicos, legítimos e informados, vedando posterior utilização incompatível. O princípio da transparência, previsto no Art. 6º, VI, exige que se forneçam informações claras, precisas e acessíveis sobre o tratamento, utilizando recursos audiovisuais quando adequado para facilitar a compreensão por pais ou responsáveis. O princípio da segurança, abarcado no Art. 7º, exige a adoção de medidas técnicas e organizacionais adequadas à proteção dos dados contra acessos não autorizados, modificações, destruição ou perda. Todos os princípios elencados acima devem ser considerados em comunhão com o princípio da boa-fé. As plataformas digitais em seus termos e políticas da comunidade parecem aplicar os princípios elencados. Quanto à abordagem a ser realizada, entendemos que as plataformas digitais devem adotar abordagens específicas para o tratamento de dados pessoais de crianças e adolescentes, como de fato o fazem. Deve-se levar em consideração as diferenças existentes em cada faixa etária, suas vulnerabilidades e capacidades específicas, que demandam parâmetros e salvaguardas distintas. A política de privacidade para jovens e adolescentes deve ser projetada com observância do princípio da transparência, o que exige o fornecimento de informações claras e acessíveis sobre a coleta, uso, compartilhamento e armazenamento dos dados pessoais. As plataformas também devem adotar o consentimento informado, quando aplicável, como princípio de desenvolvimento do espaço e das políticas de proteção das crianças e adolescentes. Isso permitirá estabelecer um canal de diálogo aberto entre a plataforma, a criança e seus pais ou responsáveis. Ainda, devem utilizar como parâmetro para coleta de dados a minimização, ou seja, coletar apenas os dados estritamente necessários para a finalidade a que se destinam. Contudo, é preciso que a Autoridade esteja atenta à necessidade de equacionar esse princípio com a garantia de outros princípios e a aplicação do melhor interesse no caso concreto, visto que existem situações nas quais uma coleta mais significativa de dados é necessária como, por exemplo, para a implementação de mecanismos de detecção de idade. A adoção de medidas de design e salvaguardas para a educação e conscientização sobre o tratamento de dados pessoais e a privacidade digital direcionada aos pais e responsáveis, à criança e ao adolescente também é prioridade das plataformas digitais e aplicações de jogos digitais. Medidas que incorporem um design que desperte a curiosidade da criança e do adolescente para os benefícios do uso seguro da internet podem atingir uma maior eficácia do que políticas de privacidade extensas. Isso também deve incluir medidas adicionais de conscientização dos benefícios da privacidade da conta. O monitoramento contínuo e a realização de avaliações de impacto de privacidade também podem ser mecanismos eficientes para proteção do tratamento de dados pessoais de crianças e adolescentes. Processos contínuos de monitoramento e revisão das políticas de

privacidade garantirão sua conformidade com a legislação local e com os padrões esperados pelos usuários. ","708762":"A resposta desta questão já foi amplamente trazida nas respostas anteriores, devendo haver acolhimento dos argumentos supramencionados para esta indagação. De qualquer forma, reforçamos que os dados pessoais de verificação de idade de crianças e adolescentes hoje são obtidos normalmente pela declaração pessoal no preenchimento do cadastro ou no momento do acesso, ou seja, medidas que solicitam que a própria pessoa autodeclare sua idade. Essa técnica pode abranger uma série de ferramentas, como o preenchimento de formulários de declaração de idade, no qual a plataforma incorpora caixas para preenchimento da data de nascimento ou perguntas explícitas sobre a idade. A técnica de declaração da idade também pode estar incorporada na aceitação dos termos e condições de uso da plataforma, através do preenchimento de campos que confirmem que o usuário tem a idade mínima para usá-la. Contudo, essa técnica depende da declaração verídica e, portanto, está sujeita a falhas. Por isso, cada vez mais são utilizadas perguntas que para serem respondidas exigem conhecimento e maior raciocínio, de forma que, na maioria das vezes, apenas adultos seriam capazes de respondê-las. De outro lado, alternativas mostram-se possíveis, como por exemplo, o uso de métodos de estimativa de idade, que são aqueles que geralmente funcionam utilizando dados sobre o usuário, combinados com análises preditivas (como análise facial ou outras ferramentas baseadas em IA), para adivinhar a idade. Isso pode ser baseado na aparência do usuário, em suas preferências online ou no histórico de navegação na internet. A inteligência artificial (IA) e o aprendizado de máquina estão sendo empregados também para analisar padrões de comportamento. Esses sistemas podem se adaptar e aprender ao longo do tempo, melhorando sua precisão e reduzindo o risco de serem contornados, embora atualmente ainda estejam em desenvolvimento e aprimoramento. Uma boa prática a ser citada é a obrigatoriedade de sincronização de contas de crianças à conta de seus pais ou responsáveis (recurso de pareamento familiar), de forma que os acessos de crianças são controlados pelos pais, ou seja, a responsabilização do controle de acessos e de comprovação de idade recai aos pais, que são os maiores interessados na segurança e proteção dos filhos. Na medida em que as crianças vão crescendo, os pais vão alterando as informações possibilitando o acesso a diferentes páginas, conteúdos e acessos, justamente por isso, essa técnica deve ser combinada com boas práticas pelas plataformas digitais, com a adoção de uma abordagem centrada na proteção da privacidade e segurança da criança, restrições de conteúdo, ferramentas de conscientização das crianças e adolescentes e dos seus pais e responsáveis. A verificação da idade em plataformas digitais é um desafio complexo que exige a implementação de soluções adequadas e proporcionais que estão sendo estudadas e elaboradas por diversos profissionais. É preciso mencionar que a autoridade deve reconhecer que as finalidades do processamento (como criação de perfil/formação de perfis comportamentais, personalização de anúncios para fins de segmentação, etc.) não devem ser limitadas por sua natureza, pois podem constituir atividades de processamento importantes, inclusive para garantir os melhores interesses de menores. além disso, é preciso considerar que as finalidades do tratamento só devem ser limitadas se envolverem o tratamento de dados de menores de uma forma que afete negativamente os seus interesses superiores. Por fim, assim como vem se consolidando na prática internacional, sugere-se o reconhecimento de que a escolha do mecanismo a ser

usado para a verificação de idade deve se guiar por uma análise de risco e considerar as tecnologias existentes. Além disso, é preciso reconhecer que não existe uma solução única para a verificação de idade e que certas ferramentas podem ser mais ou menos adequadas a depender da plataforma que a emprega. Ainda, é relevante admitir que não existe solução infalível e que todas as ferramentas existentes terão prós e contras e serão sujeitas a falhas. ","708764":"O § 4º, art. 14 da Lei 13.709/2018 determina que não seja exigido o fornecimento de informações pessoais além das estritamente necessárias sobre as crianças para que possam participar de jogos, aplicações da internet ou atividades online. Neste sentido, acreditamos que algumas limitações específicas devem ser observadas na coleta de dados pessoais de crianças a fim de proteger sua privacidade e segurança. Inicialmente, as plataformas digitais devem observar restrições quanto à natureza dos dados coletados. Isso inclui considerar que não deve haver o tratamento indiscriminado de dados pessoais, especialmente de dados pessoais sensíveis, como aqueles relacionados à saúde, religião, orientação sexual, origem étnica, eventuais opiniões políticas etc.. Além disso, a coleta de dados de localização, metadados e informações de uso da plataforma devem observar os princípios aplicáveis na prestação dos serviços, mantendo observância ao princípio da transparência. A coleta de dados para formação de perfis comportamentais do menor deve sempre observar o princípio do melhor interesse do menor, ou seja, as plataformas devem assegurar que a formação do perfil seja compatível com o melhor interesse da criança ou adolescente, como para personalização da sua experiência e melhor segurança. Outra limitação específica para os dados de crianças e adolescentes refere-se à limitação na retenção dos dados. As plataformas digitais devem estabelecer parâmetros claros em suas políticas de privacidade e segurança sobre a retenção dos dados pessoais e dados pessoais sensíveis. ","708768":"A Convenção sobre os Direitos da Criança afirma que as plataformas de comunicação são importantes para a criança, pois garantem o acesso a “informações e materiais procedentes de diversas fontes nacionais e internacionais, especialmente aqueles que visam à promoção de seu bem-estar social, espiritual e moral e de sua saúde física e mental”. A utilização de mecanismos e boas práticas para o tratamento dos dados pessoais é capaz de reduzir os riscos de exposição, violação da privacidade e vigilância. Dentre essas boas práticas, destacam-se aquelas adotadas para ampliar o controle ou supervisão de pais e responsáveis sobre o tratamento de dados pessoais. De acordo com o Fundo das Nações Unidas para a Infância (UNICEF), o pleno desenvolvimento da criança e do adolescente nos dias atuais depende diretamente da criação de um ambiente digital seguro. Os pais e responsáveis têm o dever legal de proteger os seus filhos, mas devem respeitar a personalidade e as liberdades reconhecidas nacional e internacionalmente para crianças e adolescentes. Portanto, o controle realizado pelos pais deve ser adequado à idade. Para plataformas digitais que permitem o acesso de crianças menores de 13 anos a ambientes projetados para sua idade, mostra-se adequado o controle parental, permitindo que os pais e responsáveis personalizem as configurações da conta da criança quanto à privacidade e ao conteúdo. Já no tocante aos jovens, mostra-se mais adequado a adoção de ferramentas de supervisão da conta, que preservem a autonomia do adolescente para gerir sua conta. A supervisão pode incluir um conjunto de mecanismos relacionados ao monitoramento da atividade online, como a possibilidade de receber relatórios da atividade com os serviços

acessados e interações realizadas ou o recebimento de alertas quando ocorrerem atividades que ponham em risco a privacidade e segurança do jovem. Importante ressaltar que a supervisão parental deve ser realizada mediante o consentimento dos filhos a fim de preservar sua autonomia e identidade pessoal e incentivar o diálogo aberto entre pais e responsáveis. ","708772":"O princípio da transparência é essencial para a criação de uma relação de confiança entre a plataforma digital e o usuário. A transparência permite a compreensão dos processos de tratamento de dados pessoais e é um pré-requisito para a contestabilidade e a responsabilização dos sistemas. Dentre as boas práticas relacionadas à transparência, as plataformas digitais devem garantir que os usuários sejam informados quando da atualização ou alteração material das suas políticas de privacidade e diretrizes da comunidade. Isso deve ser feito de forma clara e compreensível, incluindo postagens em seus sites, garantindo a ampla divulgação. A localização dos termos e condições de uso deve estar disponibilizada em local acessível, em destaque. Além disso, a compreensibilidade das informações relativas à coleta, ao uso, ao tratamento e ao armazenamento dos dados pessoais de crianças e adolescentes é um aspecto importante para as plataformas digitais. Isso demanda a utilização de uma linguagem simples, clara e adaptada ao contexto local. Ainda, como medida de boa prática, é possível que seja utilizado, adicionalmente à disponibilização clara e simples das informações, outras formas de divulgação, como por meio de vídeos sobre a política de segurança e privacidade das crianças, tornando-as atrativas e despertando a curiosidade sobre o texto integral. ","708775":"Sinalizamos que a legislação usa muitos termos vagos, com possibilidades interpretativas diversas. Além disso, faz-se necessária uma mudança de perspectiva em relação ao uso das plataformas digitais por crianças e adolescentes, trazendo a perspectiva dos benefícios do uso da tecnologia e das plataformas digitais no desenvolvimento das crianças e dos adolescentes. É preciso que a política aplicável seja capaz de fomentar também os aspectos positivos das plataformas. É claro que há desafios e questões a serem consideradas em relação ao impacto e à formação de crianças e adolescentes nas plataformas digitais. Contudo, é preciso que se considere que elas oferecem um universo ilimitado de informações e conteúdos educativos, permitindo que crianças e adolescentes explorem seus interesses, desenvolvam novas habilidades e ampliem seus horizontes. Através de vídeos, jogos educativos, aplicativos interativos e cursos online, jovens podem aprender sobre diversos temas, desde ciências e matemática até história, artes e idiomas, de maneira lúdica e envolvente. Essa autonomia no aprendizado contribui para a formação de indivíduos críticos, criativos e proativos, preparados para os desafios do século XXI. Além disso, é preciso que se considere que as plataformas digitais permitem que crianças e adolescentes se conectem com amigos e familiares, mesmo que estejam distantes. Redes sociais, grupos de bate-papo e plataformas de comunicação possibilitam a troca de experiências, o compartilhamento de ideias e a construção de relacionamentos significativos. Essa interação social contribui para o desenvolvimento da comunicação, da empatia e da colaboração, habilidades essenciais para a vida em sociedade. As plataformas digitais oferecem ainda o acesso a um vasto leque de informações e conteúdos culturais, como livros, músicas, filmes, museus virtuais e exposições online. Essa riqueza cultural contribui para o desenvolvimento do senso crítico, da apreciação artística e da compreensão de diferentes culturas, elementos essenciais para a formação de indivíduos completos e preparados para viver em um mundo

globalizado. No artigo de Laura Bitto Urbanova e outras, que traduzindo livremente tem o seguinte título: “A tecnologia me apoia: Percepções sobre os benefícios da tecnologia digital em adolescentes”, as autoras concluem: “Nossas descobertas mostram que a tecnologia digital pode apoiar adolescentes em vários domínios de suas vidas e que eles são conscientes das oportunidades relativas à sua utilização. Isso demonstra que colocar os adolescentes e suas opiniões no centro da políticas digitais nacionais e até globais podem ser muito úteis, não apenas na redução da sua exposição aos riscos associados ao tecnologia, mas também na exploração de como ela pode ser útil em concretizar o seu potencial (UNICEF para Todas as Crianças, 2017).Além disso, a nossa investigação sugere que a tecnologia digital pode permitir crescimento pessoal positivo, autopercepção e desenvolvimento mental saudável em adolescentes. Embora mais pesquisas estejam focadas sobre os riscos da tecnologia digital, a presença dos adolescentes no mundo online também pode apoiar uma adaptação positiva a este período de desenvolvimento, bem como sua socialização em oposição ao isolamento.” - BITTO URBANOVA, Laura et al. Technology supports me: Perceptions of the benefits of digital technology in adolescents. Frontiers in Psychology, v. 13, p. 970395, 2023. É preciso que seja enaltecido e considerados os pontos positivos, as possibilidades efetivas de melhorias na vida de milhares de crianças e adolescentes. As empresas do setor da tecnologia investem quantias extremamente elevadas no desenvolvimento de ferramentas e sistemas que ampliem e efetivem a segurança e a preservação da intimidade e privacidade das crianças, dos adolescentes e de seus usuários em geral. É preciso que se ressalte que a coleta e o tratamento de dados pessoais permitem uma série de benefícios relativos à segurança. O trabalho conjunto das plataformas e da ANPD é essencial. A parceria entre estes atores mostra-se imprescindível na efetivação de políticas de proteção de dados de crianças e adolescentes.

Contribuinte: Conselho Digital do Brasil

Número: OP-752978

Data: 16/08/2024 - 08:25

Resumo: :"Contribuição do Idec - Instituto de Defesa de Consumidores: O Enunciado nº 1/2023 possibilitou que os dados de crianças e adolescentes possam ser tratados com base no legítimo interesse. No entanto, o próprio enunciado reitera a necessidade de observância e prevalência do princípio do melhor interesse (art. 227 CF/88 c/c art. 14 LGPD). Já o Guia traz algumas orientações interpretativas sobre a priorização do melhor interesse na aplicação do legítimo interesse. No Projeto Regulatório, a ANPD deve aprofundar a interpretação do melhor interesse no Tratamento de Dados de Crianças e Adolescentes. Nos termos do Comentário Geral n° 14, de 2013, do Comitê dos Direitos da Criança da ONU, o melhor interesse pode ser compreendido como um (i) direito substantivo, que determina que uma criança deve ter seu melhor interesse apreciado e levado em consideração de forma prioritária; (ii) um princípio fundamental e interpretativo, de maneira que deve ser privilegiada a interpretação que melhor atenda de forma mais eficaz aos interesses da criança e (iii) uma regra processual, para que o processo de tomada de decisão deve incluir uma

avaliação dos impactos (positivos ou negativos) sobre as crianças envolvidas. Ou seja, o tratamento de dados que atenda o princípio do melhor interesse deve privilegiar o interesse e os direitos das crianças e adolescentes. A aplicação do melhor interesse à proteção de dados pessoais deve ser holística, exigindo que os controladores apliquem esse princípio em todos os momentos do tratamento de dados. Dessa forma, a aplicação do melhor interesse deve ser utilizada para harmonizar o tratamento de dados visando como finalidade a garantia dos direitos das crianças e adolescentes. 1. Um Guia deve discorrer sobre a escolha de bases legais para o tratamento de dados de crianças e adolescentes e, enquanto isso, o Enunciado deve ser interpretado de maneira restritiva Seguindo boas práticas internacionais, o Enunciado deve ser interpretado de maneira a aplicar o melhor interesse na escolha das bases legais para o tratamento de dados de crianças e adolescentes. Considerando a proteção constitucional superior a essa população, a interpretação de que qualquer base legal do art. 7º e do art. 11 seriam aplicáveis a crianças e adolescentes é esvaziar o comando legal de sua proteção. Desta maneira, espera-se que a ANPD restrinja a interpretação do Enunciado em futuro guia sobre o tema. 2. Um aspecto do melhor interesse que deve ser regulamentado pela ANPD é a aplicação dos direitos dos titulares para crianças e adolescentes. É necessário que a ANPD proponha um design apropriado para que esses titulares possam exercê-los apropriadamente. Assim como o direito à informação (art. 14, §6º da LGPD), o exercício dos direitos dos titulares também devem ser fornecidos de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado. Uma criança não deve ser impedida de exercer seus direitos de titular em razão de sua idade, maturidade ou capacidade. É fundamental que os agentes de tratamento, diretamente ou com assistência/representação, possibilitem que a criança compreenda e exerça seus direitos. Para isso, é necessário que a ANPD regulamente um Código de Design direcionado a produtos e serviços online, que contemple, entre outros, os direito dos titulares. ","708725":"Contribuição do Idec - Instituto de Defesa de Consumidores: 1. Vedação à exploração comercial de crianças e adolescentes A ANPD, enquanto agente do Estado, tem o dever de proteger crianças contra ações de agentes sociais e econômicos que as coloquem em risco e/ou as explora comercialmente. Nesse sentido, é direito das crianças a proteção contra a exploração comercial infantil, incluindo o direcionamento de comunicação mercadológica aos menores de 12 anos. A exploração comercial infantil já é rechaçada por diversos marcos normativos, inclusive pela Constituição Federal de 1988 (art. 227), além de um grande arcabouço contra a publicidade de crianças e adolescentes, como pelo Estatuto da Criança e do Adolescente (art. 4 do ECA), pelo Código de Defesa do Consumidor (art. 36, CDC), Marco Legal da Primeira Infância (Art. 5º), a Convenção dos Direitos da Criança (Art. 32, par. 1º) e Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) (Res. 163/2014 e Res. 245/2024). No Guia sobre Legítimo Interesse a ANPD analisa um caso envolve a exploração comercial, concluindo que a legítima expectativa e os direitos das crianças devem prevalecer, o que impossibilitaria o uso desta base legal no caso analisado. Assim, o Projeto Regulatório que se pretenda significativamente garantir direitos a crianças e adolescentes no ambiente digital deve vedar a exploração comercial para uma população que não tem discernimento necessário para tanto. Crianças e adolescentes são sujeitos hipervulneráveis e, portanto, estão

mais expostos aos aspectos negativos do ecossistema digital, tendo em vista a etapa específica de desenvolvimento biopsicológico que atravessam. Ao vedar todas as formas de exploração comercial infantil, a ANPD dará um passo à frente para que as crianças e adolescentes possam usufruir de plataformas e dispositivos digitais sem riscos aos seus direitos e garantias individuais. Isso porque não há razões para crer que a obtenção de vantagens econômicas por parte do setor privado deva prevalecer sobre os direitos das crianças e adolescentes no ambiente digital. Em razão do melhor interesse, o Projeto Regulatório no Tratamento de Dados de Crianças e Adolescentes deve vedar o uso da hipótese legal do legítimo interesse para fins comerciais e igualmente espera-se que a ANPD contribua para projetos de lei nesse sentido, como o PL 2628. Não há razões para crer que a exploração comercial de crianças cumpre o melhor interesse e é de sua legítima expectativa. ","705523":"N/a","708742":"N/a","708745":"N/a","705539":"N/a","708762":"N/a","708764":"N/a","708768":"N/a","708772":"N/a","708775":"N/a

Contribuinte: Marina Fernandes Bispo de Siqueira

Número: OP-753018

Data: 16/08/2024 - 10:25

Resumo: :"O princípio do melhor interesse da criança e do adolescente busca garantir a proteção integral dos direitos fundamentais de crianças e adolescentes de forma a garantir que seus interesses sejam vistos como prioridade no tratamento de dados pessoais. Neste sentido, é fundamental que seja realizada uma avaliação específica do tratamento dos dados pessoais pelo controlador, justificando a necessidade do tratamento de dados de crianças e adolescentes e as medidas de segurança adequadas para a proteção dos dados, garantindo a segurança das operações não apenas em fluxos em que a hipótese legal de tratamento seja o legítimo interesse. ","708725":"Considerando as próprias determinações apresentadas pela Lei Geral de Proteção de Dados (LGPD), há demanda de maior atenção no tratamento de dados pessoais que envolva dados sensíveis de crianças e adolescentes como informações sobre origem racial ou étnica, convicções religiosas, dados referentes à saúde ou dados genéticos ou biométricos, e quanto o tratamento de dados for baseado na hipótese legal do legítimo interesse. Além dessas hipóteses já apresentadas pela LGPD, são situações que poderiam demandar maior atenção e detalhamento o tratamento de dados pessoais em redes sociais, plataformas digitais e jogos pelo potencial exposição de crianças e adolescentes e possíveis implicações para a sua privacidade e segurança, e o tratamento de dados para publicidade e marketing direcionado para crianças e adolescentes por haver um tratamento de dados para fins comerciais. Outros pontos que remetem atenção também estão em serviços educacionais, sejam de escolas regulamentadas comumente pelo MEC, ou outros meios de aprendizagem, como no caso de plataformas de ensino e demais formas de formação de conhecimento. Esses agentes processam dados de crianças e adolescentes em alto volume. Ademais, o uso de dados de crianças e adolescentes em decisões automatizadas, inferências e na utilização de inteligência artificial merecem ser observados em relação ao princípio do melhor interesse. ","705523":"Para que seja obtido o consentimento específico e destacado

dos pais e responsáveis de forma adequada, de acordo com o estabelecido pelo GDPR (Regulamento Geral sobre a Proteção de Dados) na União Europeia em seus artigos 4(11), 6(1)(a), 7 e considerando 32, é fundamental que este seja apresentado de forma clara e transparente por meio de linguagem acessível, destacado visualmente de forma a ser facilmente identificado pelos pais e responsáveis e separado de outros termos e condições. No mais, podem ser utilizadas formas verificação de autenticidade do consentimento, garantindo assim que a pessoa que está consentindo efetivamente é um pai ou responsável, e não a criança. Esta verificação pode ocorrer por autentificação multifator, confirmação por e-mail ou SMS, ou até mesmo prova de identidade a depender dos dados tratados e sensibilidade da operação de tratamento.","708742":"Controladores podem utilizar de formas de verificação de autenticidade do consentimento, especialmente no ambiente digital, viabilizando identificar que o consentimento de fato foi fornecido por pais e responsáveis. Esta verificação pode ocorrer por autentificação multifator com a implementação de mais de um método para a verificação de identidade do usuário, confirmação por e-mail ou SMS, ou até mesmo prova de identidade a depender dos dados tratados e sensibilidade da operação de tratamento. Meios já existentes e centralizados no âmbito público também podem ser utilizados, como o caso de logins únicos, exemplo: gov.br.","708745":"Cumpre a observação das disposições do Direito Civil referentes às capacidades civis, seguindo a regra geral de representação e assistência de pais ou responsáveis estabelecida pela legislação vigente. Caso a Autoridade Nacional de Proteção de Dados considere possível a concessão de consentimento por adolescentes para o tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais ou responsáveis legais, isso deve ser abordado por legislação específica adequada ao caso.","705539":"Assim como descrito pela própria Autoridade Nacional de Proteção de Dados, cumpre a observância dos princípios apresentados pela legislação em seu artigo 6º, em especial o da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais restringem o tratamento de dados pessoais ao mínimo necessário para o atingimento das finalidades específicas, legítimas e informadas aos titulares de dados. Quanto aos parâmetros e salvaguardas adicionais aos já descritos, é relevante que seja estabelecida uma idade mínima adequada para o uso das plataformas digitais, especialmente jogos on-line com conteúdo sensível ou com inserção de propagandas publicitárias não adequadas ao público-alvo das aplicações. Sobre as medidas de design a serem adotadas, é fundamental o fornecimento de informações claras e acessíveis quanto ao tratamento de dados incluindo políticas de privacidade e termos de uso redigidas em linguagem simples e acessível, contendo, sempre que possível, elementos gráficos adequados para a idade à qual a comunicação é destinada, o que auxilia na compreensão do conteúdo disponibilizado e garante maior transparência.","708762":"Existem diversas técnicas disponíveis para a verificação de idade de usuários em plataformas digitais, cabendo aos agentes de tratamento a avaliação de qual o método mais adequado a depender da plataforma utilizada, orçamento a ser despendido, e esforços necessários para a implementação e razoabilidade das práticas utilizadas. Dentre as boas práticas, destacamos a verificação por data de nascimento declarada pelo próprio titular de dados ou seus pais e responsáveis legais no momento da obtenção do consentimento ou a solicitação do fornecimento de documento de identidade válido. É viável o uso tecnologias como algoritmos para verificação de idade

em bancos de dados disponíveis, no entanto é fundamental que seja respeitado sempre o melhor interesse do menor e avaliada a razoabilidade desta operação.","708764":"Considerando o disposto no art. 14, § 4º, da LGPD e demais aspectos apresentados pela legislação, resta claro que o tratamento de dados pessoais de crianças e adolescentes por plataformas digitais especificamente para jogos digitais deve se limitar ao mínimo necessário para a execução da atividade pretendida. Tal disposição está em conformidade com os princípios normativos apresentados pela lei (art. 6º LGPD), em especial o princípio da necessidade, que sugere a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.","708768":"Para a ampliação do controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes é fundamental que o consentimento seja obtido de forma adequada, de acordo com o estabelecido pelo GDPR (Regulamento Geral sobre a Proteção de Dados) na União Europeia em seus artigos 4(11), 6(1)(a), 7 e considerando 32, sendo apresentadas informações de forma clara e transparente por meio de linguagem acessível sobre como os dados serão tratados antes mesmo do fornecimento do consentimento, garantindo maior autonomia na tomada de decisões. Também são boas práticas para a ampliação do controle de pais e responsáveis a disponibilização de mecanismos facilitados para a revogação do consentimento, garantindo a retirada do acesso ou eliminação de dados pessoais coletados a qualquer momento, além do oferecimento de controles que permitam o gerenciamento e monitoramento das atividades executadas pelas crianças e adolescentes. ","708772":"Dentre as boas práticas relacionadas à transparência e ao fornecimento de informações, destaca-se como boa prática o aprimoramento da estratégia de comunicação a ser utilizada pelas plataformas digitais, adequando o design ao público alvo. Neste sentido, é fundamental que o fornecimento de informações quanto ao tratamento de dados pessoais se dê de forma clara e acessível, incluindo políticas de privacidade e termos de uso em linguagem simples e acessível e contendo, sempre que possível, elementos gráficos adequados para a idade à qual a comunicação é destinada, o que auxilia na compreensão do conteúdo disponibilizado e garante maior transparência. ","708775":"Voltar a atenção para questões de inferência e inteligência artificial.

Contribuinte: JOSE LUCAS SILVA GALDINO

Número: OP-753021

Data: 16/08/2024 - 10:33

Resumo:
:"abc","708725":"abc","705523":"abc","708742":"abc","708745":"abc","705539":"abc","708762":"abc","708764":"abc","708768":"abc","708772":"abc","708775":"abc

Contribuinte: KARINE LOPES DA CRUZ SOUSA

Número: OP-753027

Data: 16/08/2024 - 10:48

Contribuinte: VIVIAN DE LIMA ALVES

Número: OP-753038

Data: 16/08/2024 - 11:31

Resumo: :"Contribuições da Associação Nacional de Hospitais Privados - Anahp Para assegurar a privacidade e a proteção de dados das crianças, é essencial definir de forma clara e assertiva o conceito de "melhor interesse da criança". Este conceito, embora fundamental,ainda não possui uma definição consensual na doutrina. Ele é fundamentado em diversas fontes, como a Constituição, o Estatuto da Criança e do Adolescente, além de Convenções e Tratados Internacionais. Normalmente, o melhor interesse da criança é determinado caso a caso, o que complica a identificação de referências claras em relação aos dados pessoais. A natureza dinâmica das atividades de tratamento de dados, especialmente na internet, torna inviável a análise individual do tratamento de dados de cada criança. Portanto, é necessário estabelecer um conceito geral que defina claramente as limitações e proibições aplicáveis ao tratamento de dados pessoais de crianças. É importante o estabelecimento de um conceito central e objetivo, a fim de diminuir interpretações subjetivas sobre cada caso.","708725":"Contribuições da Associação Nacional de Hospitais Privados - Anahp O uso de imagens de menores no ambiente escolar requer diretrizes claras, pois cada instituição de ensino age de acordo com seu nível de governança de dados. Alguns pais não se opõem à divulgação de fotos de seus filhos pelas instituições e até desejam receber essas imagens. No entanto, outros pais têm uma posição contrária. Como as crianças frequentemente interagem entre si, é comum que apareçam em fotos ou vídeos com colegas de turma. Diante dessa situação, como a instituição de ensino deve proceder? Excluir alunos das fotografias, seja digitalmente ou isolando-os durante a captura, pode criar um sentimento de rejeição nas crianças. Por outro lado, fotos coletivas poderiam ser inviabilizadas para compartilhamento com pais ou em mídias devido à falta de autorização do uso da imagem de uma criança específica. Outro problema é o compartilhamento de dados pessoais de menores por canais não oficiais e com baixo nível de segurança. Muitos pais ou responsáveis solicitam o tratamento de dados pessoais de menores por aplicativos como WhatsApp e similares. Nas instituições de ensino, é comum que os pais prefiram essa praticidade ou não tenham a facilidade e o grau de instrução necessários para acessar canais mais seguros de compartilhamento. Assim, os aplicativos se tornam as ferramentas mais simples e acessíveis para esse tipo de tarefa. Até onde vai a responsabilidade da instituição em casos como estes? Seria o responsável autoridade máxima para decidir sozinho sobre o melhor interesse da criança no tratamento de dados pessoais?","705523":"Contribuições da Associação Nacional de Hospitais Privados - Anahp A obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais para o tratamento de dados pessoais de crianças e adolescentes é um processo que demanda a estrita observância de uma série de critérios e parâmetros,

conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD). Tal exigência visa assegurar a proteção integral dos menores, garantindo que seus direitos fundamentais sejam plenamente resguardados. Primordialmente, a clareza e simplicidade das informações são elementos essenciais. De acordo com o artigo 14 da LGPD, as informações fornecidas aos pais ou responsáveis devem ser redigidas em linguagem acessível e de fácil compreensão, evitando termos técnicos ou jurídicos que possam gerar confusão. A comunicação deve ser direta e transparente, assegurando que os responsáveis compreendam completamente as implicações do consentimento que estão prestes a fornecer, à exemplo do estudo realizado pela UNICEF, em 2017, o qual já destacava a importância de formular comunicações claras e compreensíveis para garantir que os responsáveis entendam os riscos e benefícios do tratamento de dados. Além disso, é importante que o pedido de consentimento esteja destacado, separado de outros termos e condições, de modo a não passar despercebido. É essencial que os responsáveis entendam claramente que estão consentindo com o tratamento de dados pessoais da criança e as finalidades específicas para as quais esses dados serão utilizados. Ainda, a finalidade determinada do consentimento também pode ser considerada como um ponto importante. Segundo a LGPD, o consentimento deve ser solicitado para uma finalidade específica e determinada, que deve ser claramente explicada aos pais ou responsáveis. Dessa forma, dentre os critérios essenciais para obtenção do consentimento, está o fato de que os controladores de dados precisam fornecer informações detalhadas sobre os tipos de dados que serão coletados, a forma como serão utilizados, armazenados e compartilhados, trazendo transparência suficiente para garantir que os responsáveis possam tomar uma decisão informada e consciente sobre o consentimento. A verificação da autenticidade do consentimento é outro aspecto crucial. Os controladores devem realizar todos os esforços razoáveis para verificar que o consentimento foi realmente fornecido pelos pais ou responsáveis legais. Isso pode incluir métodos de autenticação adicionais, como o uso de documentos de identidade ou, até mesmo, confirmações por meio de ligações telefônicas. A utilização de tecnologias adequadas que garantam a segurança e a confidencialidade das informações também é recomendada. Além disso, os responsáveis devem ser informados sobre a possibilidade de retirar o consentimento a qualquer momento, e o processo para fazê-lo deve ser simples e acessível, na medida em que a facilidade de retirada do consentimento é um direito garantido pela LGPD e deve ser respeitado pelos controladores de dados. A educação e a conscientização dos pais ou responsáveis sobre a importância da proteção de dados pessoais e o impacto do tratamento desses dados nas crianças são igualmente fundamentais, considerações já ponderadas pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a educação digital é crucial para garantir que os responsáveis possam tomar decisões informadas sobre a privacidade e a segurança online de seus filhos. Pode-se concluir, então, que a clareza, a transparência, a verificação da autenticidade, a facilidade de retirada do consentimento e a educação dos responsáveis são elementos essenciais nesse processo. Além dos critérios exigidos pela LGPD (art. 8º), é importante que haja a verificação da identidade dos pais ou responsáveis legais, para a certificação de que são as pessoas corretas fornecendo o consentimento. Também devem ser estabelecidos parâmetros objetivos de como deverá ser feita a gestão desse consentimento (se será coletado de modo físico ou digital, onde será armazenado, e o tempo de manutenção do

documento adequado ao tempo necessário para o tratamento).","708742":"Contribuições da Associação Nacional de Hospitais Privados - Anahp A Lei Geral de Proteção de Dados (LGPD) estabeleceu requisitos mais rigorosos para a coleta e tratamento de dados pessoais de crianças e adolescentes, reconhecendo a necessidade de proteção especial em razão da vulnerabilidade deste grupo de titulares. Por isso, segundo o artigo 14 desta lei, o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado considerando o seu melhor interesse. Além disso, o consentimento em que se baseará o tratamento de dados pessoais de crianças e adolescentes deve ser específico e destacado, dado por um dos pais ou responsáveis. Dito isso, algumas medidas de segurança devem ser implementadas para que a coleta do consentimento para o tratamento de dados pessoais de crianças e adolescentes sigam as diretrizes estabelecidas na LGPD. Inicialmente, podemos sugerir a implementação de mecanismos que sejam capazes de identificar a idade da criança ou do adolescente para que o tratamento em questão seja realizado considerando o grau de vulnerabilidade e maturidade do titular (criança ou adolescente) e a fim de entender o grau de participação dos pais e/ou responsáveis do menor de idade na obtenção do consentimento. Atrelada a esta implementação, é interessante que o controlador tenha o cuidado de alertar os pais e/ou responsáveis pelo menor de idade sobre o tratamento em questão, principalmente se a utilização dos dados pessoais do menor não for adequada a uma faixa etária específica. Outra medida de segurança interessante pode ser a confirmação de identidade do pai e/ou responsável pela criança ou adolescente que está dando o consentimento para o tratamento dos dados. Aqui, além de confirmar que o pai e/ou responsável é, de fato, quem ele(a) diz ser, é importante certificar-se de que ele(a) detém a competência para dar tal consentimento. Para esta medida de segurança, podem ser utilizados métodos como a confirmação de e-mail, autenticação por documento ou a verificação telefônica, por exemplo. Em caso de dúvidas sobre a identidade do responsável legal ou a relação com a criança, o controlador deve adotar medidas cautelosas, como solicitar documentos comprobatórios ou suspender o tratamento de dados até que a situação seja esclarecida. Por fim, após a coleta do consentimento prestado pelos pais e/ou responsáveis, é de extrema importância que o controlador implemente algumas medidas para que na constância do tratamento tal segurança seja garantida. Por isso, deverão ser mantidos registros sobre a obtenção do consentimento e, ainda, os responsáveis pelos titulares menores de idade deverão ter acesso facilitado às informações claras e transparentes sobre os processos de tratamento e às ferramentas de revogação do consentimento prestado. ","708745":"Contribuições da Associação Nacional de Hospitais Privados - Anahp A Lei Geral de Proteção de Dados Pessoais (LGPD) prevê em seu artigo 14 que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado considerando o melhor interesse destes titulares. Com relação ao consentimento, de forma geral, este precisará ser concedido pelos pais e/ou responsáveis da criança ou do adolescente (até 16 anos), visto que são titulares sem capacidade civil, conforme Código Civil. Contudo, há que se considerar os ditames do Estatuto da Criança e do Adolescente (norma específica sobre o tema), que em seu artigo 16 prevê que o direito à liberdade de expressão da criança e do adolescente deverá ser exercido de acordo com a sua capacidade de discernimento. Isto é, o ECA prevê em seu texto o princípio da autonomia progressiva e por isso considera que crianças e adolescentes poderão praticar alguns atos da vida civil sem a necessidade de

representação ou assistência de seus pais e/ou responsável, desde que o ato em questão esteja de acordo com a sua capacidade de discernimento. Para corroborar com esta ideia, o Comentário Geral nº 25 do Comitê dos Direitos da Criança da ONU destaca que a interpretação restritiva da capacidade civil poderia trazer dificuldades ou até impedir o acesso de crianças e adolescentes à internet, promovendo exclusão digital. Por isso, partindo do princípio da autonomia progressiva de crianças e adolescentes, é possível afirmar que a depender do tratamento de dados pessoais e do contexto em que está inserido, estes titulares podem fornecer o seu consentimento, sem que seja necessária a representação ou assistência dos pais e/ou responsáveis legais. É recomendável, para que não haja conflito entre as legislações nacionais, que a LGPD observe as disposições do direito civil acerca das capacidades civis, ou seja, o menor de 16 anos, sendo absolutamente incapaz, não poderia conceder o seu consentimento sem a presença de um dos pais ou responsável legal. O Regulamento Geral sobre Proteção de Dados da União Europeia também dispõe nesse sentido (art. 8, 1). ","705539":"Contribuições da Associação Nacional de Hospitais Privados - Anahp Em primeiro lugar, é essencial que o princípio do melhor interesse seja considerado ao definir as finalidades para as quais os dados pessoais de crianças e adolescentes serão tratados. Os agentes de tratamento dificilmente poderão adotar as mesmas práticas usadas para adultos ao lidar com dados de crianças e adolescentes. Ao definir os tratamentos a serem realizados, os agentes de tratamento não devem focar apenas em seus interesses comerciais. É crucial que avaliem se os tratamentos visam proteger e promover o bem-estar e os direitos das crianças e adolescentes. A transparência é outro princípio crucial: os avisos de privacidade devem ter seus textos e formatos adaptados à idade e ao entendimento das crianças e adolescentes. Em alguns casos, pode ser preferível adotar avisos em formatos de animações ou vídeos, por exemplo. Em termos de parâmetros e salvaguardas, é importante adotar a minimização de dados, coletando e processando apenas os dados estritamente necessários para a finalidade pretendida, evitando a coleta excessiva. A segurança dos dados deve ser uma prioridade, com a implementação de medidas robustas para protegê-los contra acessos não autorizados, vazamentos e outras ameaças. Incidentes envolvendo dados de titulares vulneráveis, como crianças e adolescentes, podem aumentar significativamente o risco de danos aos direitos dos titulares, pois eles podem não ter o discernimento necessário para se protegerem contra o uso indevido de seus dados.Técnicas de anonimização e pseudonimização devem ser utilizadas sempre que possível para proteger a identidade das crianças e adolescentes, reduzindo o risco de identificação. As medidas de design e salvaguardas específicas incluem a integração dos princípios de Privacy by Design e Privacy by Default, garantindo que os princípios de privacidade sejam incorporados desde a concepção dos produtos e serviços digitais, com configurações de privacidade ativadas por padrão. A experiência internacional oferece importantes lições a serem consideradas. Boas práticas reconhecidas internacionalmente, como a criação de interfaces amigáveis para crianças e a implementação de restrições de uso voltadas ao público jovem, são essenciais. Entre essas práticas estão a definição de idade mínima para acesso à plataforma, a restrição de conteúdo acessível, a disponibilização de ferramentas de controle para pais e responsáveis, e a proibição do uso de dados de crianças para a criação de perfis com fins de marketing. Todos os princípios do art. 6º da LGPD devem ser observados, especialmente o princípio do melhor interesse e da transparência. Com

relação aos parâmetros e salvaguardas, é importante que as plataformas digitais contenham, minimamente, informações sobre como o tratamento de dados é realizado, além de um canal de comunicação específico para atender questões de privacidade. Internamente, é necessária a implementação de medidas de segurança da informação, e a elaboração de relatórios de impacto à proteção de dados pessoais, caso sejam identificados tratamentos de alto risco. ","708762":"Contribuições da Associação Nacional de Hospitais Privados - Anahp O processo de verificação da idade dos usuários de plataformas digitais, ao mesmo tempo que deve ser realizado com métodos que garantam sua precisão, deve respeitar o princípio da necessidade, evitando a solicitação de dados excessivos. Uma das principais práticas que devem ser adotadas é a garantia da transparência. As plataformas devem informar claramente aos usuários e seus responsáveis sobre a necessidade de verificação de idade, quais dados serão necessários e como os dados serão tratados. Outra boa prática é integrar a privacidade por design desde a concepção dos sistemas de verificação de idade. Isso significa garantir que a coleta de dados seja minimizada e que os dados coletados sejam protegidos. Existem várias técnicas disponíveis para a verificação de idade. Uma das principais abordagens utilizadas é permitir que os usuários façam a autodeclaração da sua idade ou data de nascimento. Embora essa técnica seja fácil de implementar, é recomendável que seja complementada com verificações adicionais para aumentar a precisão, tais como: ¿ Verificação por documento oficial, que envolve solicitar o envio de uma cópia de um documento de identificação, como carteira de identidade ou passaporte. A verificação pode ser realizada manualmente ou através de soluções automatizadas de reconhecimento de documentos. Nesse caso, é importante garantir que esses documentos sejam armazenados de maneira segura e definir prazos de retenção garantindo que esses documentos sejam excluídos quando não forem mais necessários para a finalidade. ¿ Envio de selfies e utilização de tecnologias que faz uma estimativa da idade com base nas características faciais. ¿ Confirmação de outras pessoas. Nessa opção, é possível pedir que os pais ou responsáveis confirmem a idade da criança ou adolescente. ¿ Análise de comportamento através de inteligência artificial. Sistemas baseados em IA podem analisar o comportamento dos usuários para inferir a idade, identificando padrões típicos de interação que correspondem a diferentes faixas etárias. Embora essa abordagem possa ser eficaz, é importante garantir que as análises sejam realizadas de maneira ética e respeitem a privacidade dos usuários. Aliadas a essas medidas, também podem ser disponibilizadas ferramentas de controle parental, as quais permitem que os pais ou responsáveis gerenciem e monitorem o acesso dos menores à plataforma, incluindo a configuração de restrições de idade. ","708764":"Contribuições da Associação Nacional de Hospitais Privados - Anahp O tratamento de dados pessoais de crianças e adolescentes, conforme se extrai do Enunciado n.º 1/2023 da ANPD, pode ser realizado com base em qualquer uma das hipóteses legais de tratamento previstas pelos artigos 7º e 11 da LGPD, desde que sempre no melhor interesse do menor. No âmbito da Política Nacional de Proteção aos Direitos da Criança e do Adolescente, toda operação de tratamento de dados pessoais que envolva, em certo grau, dados pessoais de crianças e adolescentes, deverá se atentar não só às disposições da LGPD (em especial, ao artigo 14), mas também à todo conjunto normativo que compõe esse ecossistema jurídico, como a Constituição Federal (com ênfase no artigo 227), o ECA, o CDC (artigo 37, § 2º), resoluções do CONANDA etc. Nesse sentido, ante a

obrigação de atenção ao melhor interesse da criança e do adolescente, a coleta de dados pessoais desse grupo deve ser estritamente adequado à finalidade para qual o tratamento está sendo realizado, bem como adstrito à necessidade para a qual os dados estão sendo coletados, vedando-se a coleta de dados excessivos. A formação de perfis comportamentais (perfilamento) não é vedada pela legislação pátria, todavia, tratando-se de crianças e adolescentes, pessoas consideradas hipervulneráveis, tal prática deve ser proibida, conforme determina o artigo 15 da Resolução n.º 245/2024 do CONANDA, especialmente se tensionada para o direcionamento de publicidade. Independentemente da base legal escolhida, o Controlador que pretende tratar dados de crianças e adolescentes deve sempre ponderar se os dados que serão coletados estão de acordo com essa sistemática jurídica de proteção a esse grupo, avaliando questões como: (i) os dados coletados são estritamente necessários?; (ii) a finalidade do tratamento é em melhor interesse do titular menor de idade?; e (iii) a operação de tratamento de dados possui as salvaguardas necessárias para mitigar eventuais riscos para esse grupo de pessoas?.","708768":"Contribuições da Associação Nacional de Hospitais Privados - Anahp Como um grupo considerado hipervulnerável, o tratamento de dados pessoais de crianças e adolescentes deve ser norteado pela garantia do melhor interesse dessas pessoas. No ambiente digital, devem ser estabelecidas medidas de segurança e salvaguardas específicas voltadas à proteção desses titulares, sem, no entanto, impedir o acesso deles à internet, bem como o usufruto das aplicações disponíveis - desde que adequadas à idade. Conforme determina a Constituição Federal em seu artigo 227, são deveres do Estado, da sociedade e da família a garantia de que a criança e o adolescente tenham acesso ao lazer, resguardada a sua liberdade e autodeterminação, o que foi reforçado pela Resolução n.º 245/2024 do CONANDA. Nesse sentido, é importante a garantia de que os responsáveis pelos menores tenham toda a dimensão do tratamento de dados pessoais planejado, com o esclarecimento detalhado de todas as implicações e eventuais consequências decorrentes do manuseio desses dados. Seja para a obtenção de consentimento, seja para o cumprimento de obrigações oriundas da LGPD para a legitimação do tratamento por outras bases legais - como os deveres de transparência (artigo 6º, VI) e livre acesso (artigo 6º, IV) -, é importante a exposição de todos os detalhes das operações de tratamento de dados pessoais de crianças e adolescentes aos responsáveis. Práticas como a adoção de controles parentais de privacidade, por exemplo, podem ser úteis para auxiliar os responsáveis no processo de tomada de decisão ou mesmo cientificação acerca das operações de tratamento de dados. Ainda, destacam-se as medidas educativas sobre privacidade e proteção de dados, como forma de conscientização dos pais ou responsáveis quanto à importância desse tema para crianças e adolescentes. Ressalta-se, ainda, a importância de mecanismos de bloqueio de conteúdos proibidos para menores de 18 anos; plataformas de redes sociais, ao validarem que se trata de um adolescente, tornar o perfil obrigatoriamente privado; limitação da coleta de dados para personalização de algoritmos.
","708772":"Contribuições da Associação Nacional de Hospitais Privados - Anahp A LGPD determina que as informações relacionadas ao tratamento de dados de crianças e adolescentes devem ser fornecidas de forma “maneira simples, clara e acessível”, possibilitando a compreensão da operação tanto pelos pais e responsáveis, quanto pelos próprios titulares. Dessa forma, destacam-se como boas práticas ações que possam favorecer a acessibilidade e

a compreensibilidade acerca do tratamento, como: (i) a exposição das informações sobre o tratamento dos dados pessoais por formas além da documental, ou seja, utilizando-se de instrumentos audiovisuais para a exposição das questões principais advindas do manuseio dos dados; (ii) o impulsionamento do letramento digital da população, voltado tanto para as crianças e adolescentes, quanto para os pais ou responsáveis; (iii) o desenvolvimento de documentos como Políticas de Privacidade com linguagem mais acessível, bem como utilizando-se de técnicas de visual law para tornar as explicações sobre Privacidade e Proteção de Dados menos técnicas e mais compreensíveis ao público em geral. Como requisito mínimo, deve ser disponibilizada uma Política de Privacidade e Termos de Uso, dispondo sobre o tratamento de dados realizado, e um canal de comunicação/indicação de um Encarregado (DPO), para o recebimento de demandas de privacidade, conforme determina o art. 14, §2º, da LGPD. ","708775":"Contribuições da Associação Nacional de Hospitais Privados - Anahp Sim, além das questões já abordadas, há outras áreas que requerem esclarecimentos ou regulamentação adicional para assegurar uma proteção adequada dos dados pessoais de crianças e adolescentes. Um ponto crucial é a definição de procedimentos específicos para lidar com vazamentos de dados que envolvam menores. Desta feita, considera-se essencial estabelecer medidas para minimizar os danos e prevenir futuras ocorrências, de forma a garantir uma resposta rápida e eficaz em situações de comprometimento de dados de menores. Outro aspecto importante é a regulamentação da prática de direcionamento de publicidade para menores. É preciso definir claramente as restrições sobre a coleta de dados para fins de marketing, assegurando que as crianças não sejam alvo de publicidade exploratória. Esta proteção é fundamental para evitar a exploração comercial e garantir que o ambiente digital seja seguro e apropriado para o público infantil, respeitando sua vulnerabilidade, especialmente com o ambiente digital em ascensão. Além disso, é necessário, também, um maior foco na educação e conscientização sobre privacidade e proteção de dados, tanto para crianças e adolescentes quanto para pais e educadores. Programas educativos que ensinam sobre os riscos e melhores práticas para o uso seguro da internet são essenciais. A conscientização é uma ferramenta poderosa para capacitar os menores e suas famílias a protegerem seus dados pessoais e navegarem no ambiente digital com mais segurança e confiança. Finalmente, a regulamentação deve abordar o tratamento de dados sensíveis de crianças e adolescentes, como dados de saúde, que demandam um nível de proteção ainda mais elevado. Definir diretrizes claras sobre como esses dados devem ser manejados é crucial para garantir que a privacidade e a integridade dos menores sejam preservadas em todas as situações, criando um ambiente digital seguro e protegido para crianças e adolescentes e garantindo que seus dados pessoais sejam tratados com o máximo de cuidado.

Contribuinte: FLAVIA CRISTINA DE ARAUJO LOPES

Número: OP-753046

Data: 16/08/2024 - 11:52

Resumo: :" Definition and Scope of Best Interest: Clear definitions of what constitutes the "best interest" in various contexts, especially concerning children and other vulnerable groups. Criteria or guidelines for assessing the best interest in data processing activities. Age Verification and Consent: Methods and technologies for verifying the age of data subjects, particularly children; ideally linking these to the best practise work of the global age assurance standards - IEEE 2089.1 Standard for Online Age Verification was published in May 2024, the result of over two years of deliberation by a working group of industry experts from around the world. ISO/IEC 27566 (CD) ISO/IEC 27566 Information security, cybersecurity and privacy protection — Age assurance systems — Framework Part 1: Framework has reached the Committee Draft stage in its development, which means there is a stable document which has been agreed by the relevant global working group (SC27/WG5). Guidelines on obtaining and managing consent from parents or legal guardians for processing children's data. Clarification on situations where consent might not be necessary and the role of legitimate interest in those cases. Data Minimization and Purpose Limitation: Best practices for ensuring data minimization and purpose limitation in the context of children's data. Specific examples or scenarios where data minimization should be prioritized. Transparency and Communication: Requirements for transparency and clear communication with children and their guardians about data processing activities. Development of child-friendly privacy notices (using plain language) and communication strategies. Rights of Data Subjects: Procedures for exercising data subject rights, particularly for children. Guidelines on handling requests from children or their guardians to access, correct, or delete data. Data Security and Protection Measures: Enhanced security measures for protecting children's data. Recommendations for regular security assessments and audits specific to data involving children. Impact Assessments and Risk Management: Guidelines for conducting Data Protection Impact Assessments (DPIAs) with a focus on children's data. Risk management frameworks that include specific considerations for the best interest of children. Educational and Awareness Programs: Initiatives for educating children, parents, and guardians about data protection rights and best practices. Development of educational materials and resources tailored for different age groups. Enforcement and Penalties: Clear consequences and penalties for non-compliance with best interest principles in data processing. Mechanisms for reporting and addressing violations involving children's data. Collaboration with Other Authorities: Guidelines on collaboration with other regulatory bodies, child protection agencies, and educational institutions to ensure a holistic approach to data protection for children. By addressing these issues, the ANPD can provide comprehensive guidance and regulation to ensure that the principle of best interest is effectively applied and upheld in the context of data protection, especially for vulnerable groups such as children. We would signal to the ANPD the work of the ICO in terms of its guidance in the Age Appropriate Design Code; the international regulators working group on age assurance, the work of the EU Consent Project and its deliverables in terms of childs rights, led by Professor Sonia Livingstone which are publicly available. ","708725":"The non profit 5rights produced a publication ’Demystifying the Age Appropriate Design Code’, see the slides below which highlight key elements required by platforms to act in the best interest of the child. Context 30% of people online are minors and minors are not solely to be found on sites designed for

children. Sites aimed at adults may also attract minors - for instance adult content, dating, gambling. Immersive/AR/VR sites may offer blended social and adult or gaming and adult offerings, for instance with gambling or crypto currency provision. In all of these settings the personal data of minors may be being processed, if they are treated as though they are adults and not recognised as minors. This may include location data as well as sensitive age, gender or health data. The context may also lead to a child being offered to set up a contract, under age, to engage with age inappropriate content, witness age inappropriate conduct or contact. Targeted advertising and marketing directed at children and adolescents. A clear issue is preventing the profiling of minors for advertisment purposes, ensuring that marketing content is appropriate and not manipulative, and relying on a valid legal basis for data collection. Limitations are clearly necessary in terms of behavioral advertising targeting minors. IoT and Smart Devices and immersive environments The Use of smart toys, wearables, and other Internet of Things (IoT) devices by children brings the challenges of ensuring device security and data encryption, providing clear information on data collection and sharing practices, and obtaining parental consent for data use. Manufacturers and platforms should conduct regular security assessments and offer easy-to-use privacy controls. Data leakage will be infinitely higher in immersive environments; divulging sensitive age, gender, motor or cognitive delay or acuity. ","705523":"From our experience, obtaining "specific and prominent" consent from parents or legal guardians for processing the personal data of children involves adhering to a number of parameters to ensure that the consent is informed, voluntary, and clearly communicated. Key elements to observe: Plain Language: Use clear, simple, and age-appropriate language to explain what data will be collected, how it will be used, and who it will be shared with. This must avoid tech jargon or ‘legalese’ Transparent, Comprehensive Information: Parents need clear detail about the data processing activities, the types of data collected, the purposes for data collection, and the data retention period, the specific purposes for which consent is being sought. Easy to read - consent requests need to be displayed clearly Specific separate Consent for different data processing activities, eg. consent for collecting data should be separate from consent for sharing data with third parties. Informed & opt-in opt-in mechanisms ensure active and affirmative, informed consent is given More info - additional educational materials or FAQs can help parents or guardians understand the implications of their consent. Voluntary - avoiding any form of coercion or undue pressure. Revocation/Withdrawal Options: Clearly explain that consent can be easily revoked at at any time & show the method Documentation and Record-Keeping - Keeping detailed records of the consent obtained, including the date, the method of obtaining consent, and the specific information provided. Maintain audit trails to demonstrate compliance with consent requirements. User-Friendly Design which is Intuitive Interface: an intuitive consent interface is user-friendly and minimizes the steps required to give or withdraw consent. Clear Actions: Use clear action buttons (e.g., "I Agree" / "I Do Not Agree"). Ongoing Communication: Keep parents or guardians informed of any changes in data processing practices and obtain renewed consent if necessary; reviewing and updating consent forms to ensure continued compliance. Verification of Parent/ Guardian Status: Age assurance: Offer a range of age verification or age estimation mechanisms to ensure that consent is being sought from an age appropriate individual (i.e., an adult who is old enough to be the parent or legal guardian;

typically this is above the age of 25). This may be from a government issued identity document or this may be via checks to sources such as credit card or credit reference agencies. For inclusion, it may also be via an age estimation approach, such as facial age estimation. [Here below, is included data, on the public record from the joint application by Yoti, ESRB, Superawesome to the FTC, with the response letter in footnote; we are able to resubmit following the now complete NIST Benchmark of Facial age estimation. The Commission is aware that Yoti submitted a facial age estimation model to the National Institute of Standards and Technology ("NIST") in September 2023, and Yoti has stated that it anticipates that a report reflecting NIST's evaluation of the model is forthcoming. The Commission expects that this report will materially assist the Commission, and the public, in better understanding age verification technologies and the ESRB group's application. Therefore, rather than staying or extending the deadline for the Commission to make a decision on the application, the Commission is declining the application without prejudice to the applicants refiling in the future. The public would have an opportunity to comment on a refiled application. In declining the application at this time, the Commission is taking no position on the merits of the ESRB group's application.] The following diagram from the Yoti White Paper illustrates the facial age estimation process (shared via email) ","708742":"The method described above, 'Facial Age Estimation' is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. In addition, the method promotes children's privacy, does not present any substantial risk to parents' privacy, and addresses issues of potential bias and discrimination as well as inclusion. Facial Age Estimation preserves privacy by not requiring the parent to produce additional identity documentation or information. Facial Age Estimation is not used to determine that the individual is who they claim to be, but to determine that the individual is the age they claim to be. All the currently approved US VPC methods establish that the person is an adult; none of them definitively authenticates the parent-child relationship. The COPPA Rule, nonetheless, permits these methods in line with the Rule's qualification that new VPC methods be held to the standard of "reasonably available technology," not a requirement of perfect, still-to-be developed, solutions. Moreover, children cannot easily circumvent Facial Age Estimation, which requires the live participation of an adult who is old enough to be the child's parent to submit to the process. A child's 14-year-old sibling or 18-year-old babysitter, for example, would not be able to pass the Facial Age Estimation process. This makes it more likely that the person going through the age estimation flow is the child's parent. Facial Age Estimation also addresses privacy-related issues such as inclusion as well as bias and discrimination. Parents who do not have a social security number or a payment card can use the facial age estimation process. ","708745":"We would advocate the following measures to be observed: Best Interest of the Child: Ensure that the processing of personal data always considers the best interests of the child, prioritizing their well-being, safety, and development. Transparency: Provide clear, understandable, and age-appropriate information about data processing practices, including what data is collected, how it is used, and with whom it is shared. Purpose Limitation: Collect and process personal data only for specific, explicit, and legitimate purposes relevant to the child's use of the platform. Data Minimization: Limit the collection of personal data to what is necessary for

the intended purpose, avoiding excessive or unnecessary data collection. Security: Implement robust security measures to protect personal data from unauthorized access, loss, or misuse. Consent: Obtain verifiable parental / guardian consent before collecting or processing the personal data of children, ensuring the consent process is clear and straightforward. Parameters and Safeguards Age assurance: Implement a range of reliable, independently audited age assurance mechanisms, meeting international standards - eg PAS1296:2018, ISO, IEEE Offering choice to the consumer of age assurance options Ensuring that parental consent is obtained from the appropriate party (parent or guardian) for children under the age of consent. In each instance, a data minimised age attribute can be shared. Parental Controls and Oversight: Provide tools for parents or guardians to monitor and control their child's activities on the platform, including data collection and sharing preferences. Data Subject Rights: Ensure that children and their parents or guardians can easily exercise their data protection rights, such as access, correction, deletion, and objection to data processing. Anonymization and Pseudonymization: Where possible tokenise, anonymize or pseudonymize children's and adults' data to protect their identity and privacy. Data Retention Policies: Establish clear data retention policies, ensuring that personal data is not kept longer than necessary and is securely deleted when no longer needed. Third-Party Data Sharing: Limit the sharing of personal data with third parties and ensure that any third-party service providers comply with the same data protection standards. Behavioral Advertising Restrictions: Avoid using children's data for targeted advertising or profiling purposes Design Measures Privacy by Design and Default: Embed privacy and data protection features into the design of digital platforms from the outset, ensuring that privacy settings are set to high by default. User-Friendly Interface: Design interfaces that are easy to navigate and understand, enabling children and parents to manage privacy settings and understand data practices effectively. Educational Content: Provide educational resources and materials to help children and parents understand online privacy, data protection, and safe internet practices. Regular Audits and Assessments: Conduct regular data protection impact assessments (DPIAs) to identify and mitigate risks related to the processing of children's data. Incident Response Plan: Develop and implement a comprehensive incident response plan to address data breaches promptly, including notifying affected parties and regulatory authorities as required. Monitoring and Compliance Regular Monitoring: Continuously monitor data processing activities to ensure compliance with data protection principles and promptly address any issues. Training and Awareness: Provide regular training for employees on data protection principles, specifically focusing on the processing of children's data. Engagement with Stakeholders: Engage with child protection organizations, regulators, and other stakeholders to stay updated on best practices and regulatory changes. We are happy to provide further detail on the organisations that we engage with as per diagram, shared via email. ","705539":"We would refer to the standards developed for age assurance - PAS 1296:2018, IEEE 2089.1 and ISO/27566 (CD) to detail good practise in terms of tokenised, data minimised age assurance, meeting privacy requirements. Given the word limit, we provide via email a chart here of techniques available; we are happy to provide detailed followup information on each approach, if that is of interest. In terms of facial age estimation, it is key to understand that data is instantly deleted and that there is no unique recognition:

","708762":"We would refer to the standards developed for age assurance - PAS 1296:2018, IEEE 2089.1 and ISO/27566 (CD) to detail good practise in terms of tokenised, data minimised age assurance, meeting privacy requirements. Given the word limit, we provide here a chart here of techniques available; we are happy to provide detailed followup information on each approach, if that is of interest. Working with respected global organisations, expert in child safety, see joint explainer document published by WeProtect Global Alliance & Yoti ","708764":"In each instance, only data minimised age attributes should be shared. Age assurance approaches should meet clear data privacy and security requirements,, meeting recognised standards, eg PAS 1296:2018..
","708768":"NA","708772":"We are happy to provide the ICO Age Appropriate Design Code Audit and ICO Sandbox Exit report from Yoti, link to our privacy notice for children and young adults. The 5Rights Foundation document Age Appropriate Presentation of Published Terms, provides useful suggestions on this topic. Simply deploying plain English and consulting with young people would be straightforward steps to improve the clarity of terms and statements. Examples of improved privacy statements which were developed in this way to meet the AADC include that of 'King', with its cartoon based privacy saga ('Privacy Saga', available at https://tcs.king.com/privacy-saga/level1.html, as detailed in this blog ('King's Award-Winning 'Privacy Saga Makes Terms of Service Playful', available at https://newsroom.activisionblizzard.com/p/king-privacy-saga-awards).","708775":"It is useful to see some visual case studies - we will provide these via email. It is useful to see that age assurance can be used to enable an under 18 year old, to share a data minimised under 18 attribute.

Contribuinte: Julie Dawoson

Número: OP-753069

Data: 16/08/2024 - 13:04

Resumo: :"n/a","708725":"ABRADEE: Em casos de projetos de sustentabilidade que envolvem ações em comunidades carentes, verifica-se uma dificuldade na identificação de responsáveis legais para parte das crianças e adolescentes que poderiam ser beneficiadas por tais projetos, para fins de obtenção de consentimento como hipótese legal. Nestes casos, pensando no melhor interesse desses titulares, entendemos razoável que a hipótese do legitimo interesse seja a mais indicada, mediante teste de balanceamento.","705523":"ABRADEE: Critérios como uso de linguagem de fácil entendimento, documentos divididos em subseções por temas, uso de cor ou letra diferente para destaque das palavras/termos mais importantes. ","708742":"ABRADEE: Verificação de documentação comprobatória do vínculo parental ou de representação legal da criança e do adolescente, quer seja, em base de dados pré-existente ou mediante solicitação de envio/apresentação.","708745":"ABRADEE: Entendemos a primeira opção como a melhor aplicável.
","705539":"n/a","708762":"n/a","708764":"n/a","708768":"n/a","708772":"n/a","708775":"n/a

Contribuinte: Sarah Wallace escalante

Número: OP-753082

Data: 16/08/2024 - 14:00

Resumo: :"É importante entender que, tendo em vista o grau de amplitude e abstração do princípio do melhor interesse - que, vale ressaltar, é natural e faz parte da própria ideia do princípio - o mais relevante é que a ANPD forneça balizas sobre como, em casos concretos, esse princípio será avaliado, tal como em guias orientativos. Evidente que não será possível prever exaustivamente todos os cenários existentes, e nem seria este o objetivo, mas adotar uma lógica como vem sendo feito em outros materiais de exemplificar situações, descrevendo os motivos pelos quais se entende que a situação A é considerada adequada e a situação B, inadequada, já seriam uma grande contribuição. Nesse mesmo sentido, seria importante que, ao levar em conta situações hipotéticas, a autoridade considerasse nuances concretas e esforços tecnicamente disponíveis, mantendo flexibilidade para diferentes contextos e modelos de negócio. A ABRANET reforça que o conceito de "melhor interesse" deve incluir tratamentos que protegem tanto o titular quanto terceiros, como na prevenção de fraudes e na proteção de identidade, mas também deve ser considerado em situações em que o tratamento não gera qualquer prejuízo para as crianças e os adolescentes. Em particular, entende-se ser relevante conferir clareza sobre cenários em que este princípio deve ser sopesado com outros da LGPD. Em particular, citamos o princípio da minimização, na medida em que ferramentas mais acuradas de verificação de idade, por exemplo, frequentemente implicam numa coleta mais expressiva de dados. Para que a ANPD possa direcionar o mercado, seria de extrema relevância que ela buscasse esclarecer em quais contextos esse tipo de conduta será adequada ou mesmo necessária, e em quais contextos será vista como excessiva. Por fim, a ABRANET reforça que é necessário que a ANPD, como autoridade competente, garanta a segurança jurídica ao orientar os agentes de tratamento sobre o “melhor interesse” na seara de proteção de dados pessoais antes que outras entidades menos preparadas o façam, como demonstrado pela Resolução Nº 245/2024 - CONANDA e o Projeto de Lei n° 2628 de 2022. A análise do "melhor interesse" deve considerar várias dimensões, tal como a segurança, acesso à informação e direitos ao lazer e conexão, entre outros aspectos e, principalmente, o respeito à autonomia progressiva, fornecendo orientações sobre como garantir que o “melhor interesse” seja adaptável ao desenvolvimento de cada indivíduo. Como referência internacional no tema, citamos o artigo “Age assurance for the Children’s code” do Information Commissioner’s Office do Reino Unido, que busca definir critérios e balizas específicas a serem considerados em mecanismos de verificação da idade [1]. [1] Disponível em: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/ ","708725":"Como dito, entende-se que os cenários em que o princípio do melhor interesse precisa ser sopesado com outros princípios da LGPD são aqueles que demandam maior esforço de esclarecimento do lado da autoridade. Na medida em que a cultura de proteção de dados pessoais no Brasil é ainda em alguma medida incipiente, não é trivial para os agentes de tratamento concretizar os parâmetros que serão

utilizados pela ANPD para avaliar cenários concretos. Seria de particular relevância indicar balizas nas quais os agentes podem se apoiar para tomar decisões específicas em cenários variados, tendo em vista (i) as especificidades do tratamento de dados de crianças, de um lado, e de adolescentes, de outro, (ii) as particularidades de uso de dados pessoais de crianças e adolescentes para fins de direcionamento de conteúdo, tendo aqui particular atenção ao fato de que a personalização nestes casos não deve ser confundida com a publicidade direcionada, pois trata-se mais propriamente de personalização do próprio conteúdo a ser exibido, o que certamente tem finalidades inclusive protetivas de crianças e adolescentes. Especificamente, o perfilamento para fins de publicidade envolve a coleta e análise de dados para criar anúncios personalizados, enquanto o perfilamento para conteúdo utiliza dados para oferecer conteúdo relevante ao usuário, sem fins publicitários. Assim, enquanto a exposição constante à publicidade personalizada pode influenciar negativamente os jovens, o perfilamento de conteúdo pode fornecer informações educativas e construtivas. Além disso, o perfilamento pode prevenir fraudes, protegendo os jovens de atividades maliciosas e garantindo um ambiente digital mais seguro. Crianças e adolescentes, devido à sua menor experiência, são especialmente vulneráveis a golpes online. O uso de técnicas de perfilamento permite detectar comportamentos suspeitos em tempo real, alertando os jovens e seus responsáveis sobre possíveis ameaças, contribuindo para a segurança digital e educando-os sobre os riscos online. Em particular para a ABRANET, é importante que a ANPD se atente e dê diretrizes sobre a coleta de biometria para acesso a sistemas e aplicativos financeiros. Por fim, seria importante que, ao tratar das bases legais adequadas para o tratamento de dados de menores, a ANPD não afastasse, a priori, o uso de qualquer base legal, inclusive o legítimo interesse – reforçando o que foi estabelecido no Enunciado nº 1/2022, o Guia Orientativo sobre a hipótese legal do legítimo interesse.","705523":"É importante que, sempre que o consentimento parental for requerido, ele esteja adequado ao contexto de relação entre titular, responsável legal e agente de tratamento. Em outras palavras, é preciso ter em vista que há cenários muitos diversos, que podem demandar parâmetros bastante diferentes para que o consentimento seja ofertado. Para ficar em apenas um exemplo, se a relação com o agente de tratamento se dá de forma 100% offline, não seria razoável exigir que o consentimento "específico e em destaque" seja obtido num formato digital, e vice-versa. Cabe também observar que os adjetivos “específico e em destaque” diferem dos adjetivos “livre, informado e inequívoco” mencionados na LGPD. Assim, seria importante que a ANPD esclarecesse a que exatamente se refere a especificidade – ela diz respeito às finalidades do tratamento, diz respeito àquele titular em particular, diz respeito ao conjunto de dados? No que diz respeito ao destaque, o entendimento que parece mais natural é o de que a informação deve ser de alguma forma "segmentada" em relação a eventuais outras informações. Mas seria importante esclarecer se a premissa da autoridade será de que esse destaque deve conter elementos adicionais – por exemplo, pensando na perspectiva de design, se será necessário utilizar cores e fontes que garantam uma diferença visual. Por fim, é importante que este esclarecimento conceitual determine se o consentimento deve variar conforme diferentes faixas etárias, levando em conta a crescente autonomia de crianças e adolescentes.","708742":"Embora o consentimento seja uma base legal importante para o tratamento de dados pessoais de crianças e adolescentes, seu uso deve ser ponderado conforme o contexto específico. Assim, a

ABRANET aponta que uma interpretação restritiva que considera o consentimento como a única opção viável pode resultar em limitações excessivas, mesmo quando o tratamento dos dados está em conformidade com o melhor interesse da criança. A própria ANPD já reconheceu que há outras bases legais para além do consentimento que podem ser adequadas para sustentar tratamentos de dados pessoais de crianças e adolescentes. O Enunciado nº 1/2023 da Autoridade Nacional de Proteção de Dados (ANPD) esclarece que as hipóteses legais previstas no art. 7º da LGPD, incluindo o legítimo interesse, podem ser aplicadas para o tratamento de dados pessoais de crianças e adolescentes, desde que respeitando o princípio do melhor interesse da criança ou adolescente. Essa orientação é reforçada pelo Guia de Legítimo Interesse, que oferece diretrizes claras para os controladores sobre como interpretar e aplicar essa hipótese legal, precedida por uma análise criteriosa de balanceamento de interesses. Se e quando o consentimento for escolhido como base legal adequada para o tratamento de dados, é crucial garantir, como ressaltado por autoridades estrangeiras, que ele será obtido com o menor nível de intrusão possível à privacidade. Por exemplo, o Children's Online Privacy Protection Rule ("COPPA"), administrado pela FTC, estabelece que, embora a regra seja o consentimento dos pais e responsáveis, há exceções claras e objetivas. O European Data Protection Board (EDPB) enfatiza a necessidade de proporcionalidade na verificação do consentimento para tratamento de dados, variando conforme o risco envolvido e a tecnologia disponível, com verificações mais simples para riscos baixos e mais rigorosas para riscos altos. O Information Commissioner's Office e a Data Protection Commission concordam que a adequação dos esforços para verificar o consentimento depende dos riscos e da tecnologia, e que não existe um padrão único para o que constitui "esforços razoáveis", cabendo a cada organização decidir o método mais proporcional. A ANPD deve considerar os esforços razoáveis realizados pelos controladores para obter e verificar o consentimento parental, utilizando métodos acessíveis e proporcionais ao contexto do tratamento. Por exemplo, no caso do setor financeiro, em que já se adota a validação biométrica, seria possível considerar a prática da documentoscopia – a análise de documentos a fim de comprovar a identidade do titular. Esse é um dos métodos sugeridos no COPPA, i.e. verificar uma foto de uma carteira de motorista ou outra identificação com foto enviada pelo pai ou responsável e, em seguida, comparar essa foto com uma segunda foto enviada pelo pai ou responsável, utilizando tecnologia de reconhecimento facial. É essencial também que a autoridade tenha em mente que inexistem mecanismos infalíveis e que todo sistema pode, em alguma medida, ser burlado. A ABRANET destaca a importância de levar esse ponto em consideração ao delimitar a responsabilidade dos agentes de tratamento em casos de falha dos mecanismos. Por fim, exigências desproporcionais e onerosas para os agentes de tratamento podem comprometer a eficácia do processo e acabar sendo ignoradas pelos usuários, o que contradiz os objetivos de proteção de dados da LGPD. Especialmente neste momento em que a cultura de proteção de dados pessoais no Brasil ainda está em desenvolvimento, pode ser mais estratégico que a autoridade não adote parâmetros excessivamente onerosos, cuja chance de efetivo compliance serão reduzidas, o que não significa que tais parâmetros não poderão ser revistos no futuro.","708745":"O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) define "criança" como a pessoa até 12 anos e "adolescente" como aquela entre 12 e 18 anos. Já o Código Civil Brasileiro estabelece que menores de 16 anos são

absolutamente incapazes de exercer pessoalmente os atos da vida civil, devendo ser representados. Aqueles com mais de 16 e menos de 18 anos são relativamente capazes, podendo praticar atos da vida civil desde que assistidos Não há, no entanto, clareza sobre o que exatamente estaria incluído na definição de "atos da vida civil", e essa ambiguidade pode impactar a aplicação do consentimento como base legal. A legislação brasileira já confere aos adolescentes autonomia em cenários da vida civil consideravelmente complexos, como votar nas eleições nacionais, estaduais e municipais, casar-se sem a autorização de um representante legal e viajar pelo território nacional sem a companhia dos pais ou representantes legais, sendo necessário apenas a apresentação de um documento de identificação. Portanto, a ANPD deve levar em conta que adolescentes também poderiam ter a capacidade de fornecer consentimento para o tratamento de seus dados pessoais em alguns contextos - dado que já possuem autonomia para exercer certos direitos e realizar atos da vida civil. Para tal, a complexidade do ato deve ser levada em conta pela autoridade ao orientar os agentes de tratamento, por exemplo, a capacidade de realizar atos simples como comprar um ingresso de cinema para assistir um filme. Na mesma direção, é importante que não se considere que todo e qualquer ato online é impossível de ser levado a cabo por um adolescente e que, portanto, todos equivalem aos parâmetros para é diferente da capacidade de realizar atos mais complexos, como a compra de um imóvel. É importante não equiparar todos os atos online à complexidade de transações imobiliárias. [...] Na visão da ABRANET, em respeito à autonomia progressiva, o desenvolvimento desses titulares adolescentes deve ser respeitado, o que pode tornar desnecessária a representação ou assistência pelos pais ou responsáveis legais para determinados atos. A ANPD poderá detalhar e orientar essas hipóteses de dispensa do consentimento de um dos pais ou responsável legal, o que pode ser uma medida importante para garantir o desenvolvimento pleno da personalidade e a formação cidadã dos indivíduos. É essencial reconhecer outras fontes de apoio além do suporte parental, promovendo a autonomia e o desenvolvimento progressivo das crianças e adolescentes à medida que crescem e adquirem experiências. A ABRANET ressalta que, para que essa autonomia progressiva seja efetivamente considerada e utilizada, é necessário que os controladores de dados adotem medidas que assegurem a compreensão e a clareza do consentimento fornecido pelos adolescentes. Isso inclui a elaboração de políticas de privacidade e termos de uso compreensíveis para essa faixa etária. Por fim, a ABRANET considera essencial que a ANPD esclareça em quais situações o consentimento dos pais ou responsáveis é indispensável. Por exemplo, para que os menores possam exercer seus direitos, é necessário obter o consentimento dos pais ou responsáveis? Isto é, o menor pode exercer esse direito diretamente ou o pai/responsável deve fazê-lo? Esse esclarecimento é relevante para que os agentes de tratamento possam se adequar, criando ou melhorando procedimentos para o exercício dos direitos.","705539":" Entende-se que estas perguntas são focadas alguns setores de forma mais enfática, tais como redes sociais, jogos e outras plataformas de entretenimento ou outras aplicações destinadas ou mais utilizadas por crianças e adolescentes. Ainda assim, a ABRANET destaca a importância de que a ANPD forneça exemplos ou parâmetros que orientem os agentes de tratamento sobre medidas de segurança consideradas adequadas, sem violar os demais princípios da LGPD, em particular no que diz respeito ao setor financeiro e de pagamentos. Essa orientação é essencial devido à possível

dissonância entre a eficácia dos mecanismos de segurança e a observância dos princípios estabelecidos pela LGPD. Ademais, considerando que o setor financeiro já é regulado por normativas específicas, é fundamental que a autoridade leve em conta essas normas ao indicar os parâmetros de privacidade e proteção de dados para menores de idade. Portanto, a orientação da ANPD deve integrar não apenas os princípios da LGPD, mas também as exigências regulatórias já aplicáveis aos variados segmentos. Dessa forma, assegura-se uma abordagem harmonizada e eficaz que respeite a complexidade regulatória existente e proteja adequadamente os dados dos menores. Os conceitos de "privacy by design" e "privacy by default" são especialmente relevantes, principalmente quando se trata de serviços financeiros e de pagamento e, portanto, seria de extrema importância um direcionamento da autoridade sobre esse assunto. Por exemplo, com o objetivo de apresentar parâmetros para que os agentes de tratamento consigam lidar com a tensão entre o melhor interesse da criança e do adolescente e demais princípios da LGPD, seria relevante que a autoridade indicasse como os agentes de tratamento podem balancear a necessidade de implementar medidas de design e, ao mesmo tempo, respeitar o direito positivado à autonomia progressiva da criança e do adolescente. Seria suficiente implementar medidas mais protetivas como padrão, mas oferecer aos usuários a opção de alterá-las? Ressalta-se que, também em consonância com o melhor interesse da criança, a ANPD poderia indicar exemplos de medidas que permitam algum tipo de supervisão parental. Embora a ANPD deva criar seu próprio guia, documentos internacionais podem auxiliar esse processo. Por exemplo, o Age Appropriate Design Code (ou “Children's Code”), - elaborado pelo Information Commissioner's Office (ICO) do Reino Unido, que contém diretrizes para a proteção e privacidade online de crianças e adolescentes -, possui um capítulo destinado à “Configurações Padrão”, cujo início é precisamente a descrição do conceito “privacy by default”. O ICO recomenda que as configurações sejam de "alta privacidade" por padrão, exceto quando houver uma justificativa convincente em contrário, sempre levando em consideração o melhor interesse da criança.","708762":"A implementação de ferramentas de verificação da idade dos usuários apresenta desafios técnicos que podem variar significativamente conforme a natureza do serviço oferecido e novas funcionalidades disponibilizadas. É preciso reconhecer também que nenhum mecanismo é infalível e, dessa forma, a autoridade deve levar em conta os esforços razoáveis dos diferentes agentes de tratamento para implementá-los, levando em conta o estado da arte da tecnologia. Nesse sentido, seria benéfico que a autoridade fornecesse parâmetros de adequabilidade flexíveis, orientando os agentes de tratamento sobre formas adequadas de adaptação das ferramentas, por exemplo, como o já citado guia elaborado pela ICO, Age Appropriate Design Code (ou “Children's Code”), ou o Children's Online Privacy Protection Rule ("COPPA"), que impõe certos requisitos aos operadores de websites ou serviços online direcionados a crianças menores de 13 anos. Ambos os guias apresentam exemplos de mais de um método que pode ser considerado adequado. A ANPD pode seguir esses exemplos e indicar algumas práticas que podem ser avaliadas com bons olhos pela autoridade, tal como a verificação da idade por meio de validação de cartão de crédito; estimativa de idade com base em detecção facial (sem intenção de identificar o indivíduo), análise de documentos de identidade, dentre outros. Além disso, considerando a falibilidade de qualquer mecanismo implementado, a ANPD deve levar em conta que existe a possibilidade de menores e pais

contornarem esses mecanismos offline, por exemplo, quando responsáveis fornecem seus próprios aparelhos para uso pelo menor. Assim, destaca-se a importância de não impor ônus excessivo sobre essa verificação aos controladores. Por isso mesmo, deve ser levado em conta o fato de que métodos de verificação de idade não devem substituir a função de cuidado dos pais e responsáveis. Por fim, conforme já apontado anteriormente, a ANPD deve apresentar parâmetros para que os agentes de tratamento consigam lidar com a tensão entre a eficácia de mecanismos de verificação de idade e demais princípios da LGPD, em especial o princípio da minimização de tratamento de dados pessoais. Como feito em outros guias, sugere-se que algumas situações sejam utilizadas como exemplos, a fim de esclarecer como tal sopesamento deve ser feito pelos agentes de tratamento - indicando, por exemplo, se mecanismos de detecção de menores de idade em plataformas pode ser uma forma de mitigar a coleta de mais dados no momento de acesso à plataforma. Em especial, a ABRANET entende que a ANPD deveria se manifestar sobre a prática de requisição de identidade para os exercícios de direitos dos titulares menores.","708764":"Considerando que a própria LGPD não impõe restrições automáticas ao tratamento de dados de menores, desde que respeitadas as bases legais adequadas e medidas de segurança, a ABRANET destaca que a coleta de dados de crianças e adolescentes não deve ser limitada por padrão, salvo quando necessário para proteger seus melhores interesses. Conforme indicado na pergunta anterior, medidas de segurança são de extrema relevância no setor financeiro e de pagamentos e, portanto, parece ser contra o melhor interesse da criança e do adolescente que se colete menos dados desses titulares se isso prejudicar sua segurança. Ao coletar dados de crianças e adolescentes, deve-se considerar a necessidade dos dados para o modelo de negócio sem comprometer a segurança e privacidade dos usuários. Dessa forma, a ABRANET ressalta que o tratamento desses dados deve ser analisado caso a caso, considerando os riscos específicos. Nesse sentido, reforça-se que não há tratamentos de dados pessoais que sejam maléficos a priori. Especificamente no setor financeiro e de pagamentos, o tratamento de dados pessoais, incluindo a formação de perfis comportamentais e a personalização de anúncios, não deve ser visto de maneira necessariamente negativa, pois pode oferecer benefícios significativos, principalmente no sentido de auxiliar os menores a desenvolverem habilidades financeiras de maneira segura e informada. A formação de perfis comportamentais pode inclusive ajudar a personalizar programas educativos financeiros, adaptando o conteúdo ao nível de entendimento e interesse do jovem. Isso pode tornar o aprendizado mais eficiente e relevante, ajudando a desenvolver habilidades financeiras desde cedo. Um outro exemplo diz respeito à segurança e proteção: perfis comportamentais podem ser usados para identificar padrões incomuns ou riscos de fraude, protegendo assim os menores contra atividades financeiras não autorizadas ou prejudiciais. Assim, a ABRANET entende que a ANPD deve se atentar para esses mecanismos que, se utilizados de maneira responsável e transparente, não são inerentemente maléficos e podem contribuir significativamente para a educação financeira e a segurança dos jovens. Assegurar que essas práticas sejam implementadas com controle parental é fundamental para equilibrar a proteção dos dados pessoais com a promoção da autonomia e do desenvolvimento financeiro saudável dos menores.","708768":"A autonomia progressiva, conforme reconhecida no Estatuto da Criança e do Adolescente (ECA), estipula que crianças e adolescentes devem ter sua capacidade de decisão respeitada e ampliada

conforme crescem e amadurecem. A relação entre a autonomia progressiva da criança e do adolescente é crucial para garantir que jovens possam gradualmente assumir responsabilidades de maneira segura e informada. Nesse sentido, é importante que a ANPD incentive soluções que permitam a participação gradual e supervisionada de jovens que paulatinamente transforme o controle dos pais e responsáveis em uma supervisão, até que se atinja a maioridade já com relevante autonomia digital. Podemos citar como exemplo a criação de plataformas e serviços que ofereçam contas vinculadas ou supervisionadas para menores de idade, permitindo aos pais monitorar e autorizar atividades online. Isso promove a educação digital e o uso responsável da internet enquanto garante a supervisão necessária. Outro exemplo relevante é o controle parental, que pode ser utilizado para proteger os dados e a privacidade dos jovens, garantindo um ambiente digital seguro e educativo. ","708772":"A ABRANET sugere que há algumas práticas que podem garantir a transparência direcionada aos menores, sem, no entanto, desconsiderar o salutar incentivo ao diálogo de pais e responsáveis com os menores de idade. Exemplos incluem: canal de comunicação aberto, sessões de perguntas frequentes e transparência nas atualizações de políticas e termos de uso. No entanto, a ANPD deve reconhecer alguns limites à prestação de transparência pelos agentes de tratamento. Esses limites incluem as limitações técnicas e o estado da arte da tecnologia, o segredo comercial e industrial dos agentes de tratamento, e o fato de que, dependendo da informação oferecida, pode haver risco de uso indevido por atores mal-intencionados, o que poderia potencialmente levar a riscos adicionais para a segurança de menores, em especial no que diz respeito a produtos e serviços financeiros. A ANPD deve reconhecer que algumas práticas de transparência podem ser contraproducentes. Por exemplo, é importante que a Política de Privacidade esteja facilmente acessível na documentação dos agentes de tratamento, mas não há necessidade de ser exibida constantemente ao usuário, evitando assim a fadiga. Retomar informações específicas em momentos diretamente relevantes para o tratamento de dados em questão pode ser uma abordagem mais eficaz.","708775":"A ABRANET destaca a importância de que a autoridade se manifeste em relação à retenção de dados pessoais de titulares após atingirem a maioridade. Essa manifestação é um aspecto fundamental para garantir segurança jurídica aos agentes de tratamento e, ao mesmo tempo, a conformidade com a LGPD, assegurando que os direitos dos indivíduos sejam plenamente respeitados à medida que transitam da infância e adolescência para a idade adulta. Por fim, a ABRANET reforça que seria benéfico que a ANPD implementasse orientações e ações educativas sobre o tratamento de dados pessoais de crianças e adolescentes, principalmente no que tange à introdução de tecnologias inovadoras.

Contribuinte: SILAS CARDOSO DE SOUZA

Número: OP-753092

Data: 16/08/2024 - 14:22

Resumo: :"Contribuição da Câmara Brasileira da Economia Digital: Seria imprescindível que a Autoridade evidenciasse que o melhor interesse não pode ser concebido de forma abstrata e apriorística, sendo necessária uma análise concreta para definir qual é o melhor

interesse da criança e do adolescente em determinada circunstância. Como se sabe, o melhor interesse exige necessariamente um olhar dinâmico, voltado para o caso concreto e para as características do indivíduo ou do grupo de indivíduos afetados. Nesse sentido, cabe referenciar o Comentário Geral nº 14 do Comitê dos Direitos da Criança da Organização das Nações Unidas (ONU): "[...] o conceito de melhor interesse da criança é flexível e adaptável. Deve ser ajustado e definido de forma individual, com base na situação concreta da criança ou crianças afetadas, tendo em vista o contexto e as necessidades pessoais. No que diz respeito às decisões particulares, deve ser analisado e determinado o interesse superior da criança em função das circunstâncias específicas de cada criança em concreto". Ainda no Comentário Geral nº 14, o Comitê dos Direitos da Criança da ONU ressalta que a flexibilidade do conceito de melhor interesse permite que ele seja responsivo à situação de cada menor e que haja progresso no conhecimento sobre o desenvolvimento dos menores. Em outro ponto, a flexibilidade, a dinamicidade e o olhar voltado ao caso concreto permitem que se possa endereçar a interação do melhor interesse com os diversos direitos que podem estar implicados nas situações concretas que envolvem um menor e/ou um grupo de menores. Nessa toada, o Comitê dos Direitos da Criança da ONU ressalta a interação do conceito com múltiplos direitos, são eles: direito à não-discriminação; direito à vida, sobrevivência e desenvolvimento; e direito de ser ouvido. Assim, a análise do melhor interesse deve considerar as diversas dimensões que envolvem a proteção dos interesses da criança e do adolescente. Desta forma, é necessário levar em conta os interesses que podem ser afetados caso a Autoridade opte por uma perspectiva restritiva do melhor interesse. Esses interesses vão além da proteção de dados do menor, incluindo segurança, acesso à informação, direito a brincar e se conectar, entre outros. Portanto, é essencial compreender que avaliar qual é o melhor interesse da criança e do adolescente não se restringe a verificar se o direito à proteção de dados pessoais está sendo respeitado, mas implica também avaliar o impacto ao gozo de outros direitos e considerar o desenvolvimento integral da criança e do adolescente. Este posicionamento está em conformidade com as orientações do Conselho da Europa, que destaca a necessidade de proteção igualitária de direitos como: acesso ao ambiente digital, liberdade de expressão e informação, educação e participação; e da Organização para a Cooperação e Desenvolvimento Econômico (“OCDE”), que destaca que os atores que desempenham um papel ativo na definição de políticas e práticas ou prestação de serviços para crianças e adolescentes no ambiente digital devem considerar suas diferentes necessidades em vista da idade e da maturidade, com medidas proporcionais aos riscos, baseadas em evidências, eficazes, equilibradas e formuladas com uma visão de maximizar as oportunidades e benefícios para as crianças e adolescentes no ambiente digital além de promover a liberdade de expressão das crianças e dos adolescentes e não prejudicar outros direitos humanos e liberdades fundamentais. Resposta na íntegra enviada via e-mail. ","708725":"Contribuição da Câmara Brasileira da Economia Digital: A Câmara-e.net entende que seria relevante que a presente Autoridade esclarecesse que o uso da base legal do legítimo interesse para o tratamento de dados pessoais de crianças e adolescentes não é, prima facie, contrário ao seu melhor interesse. Nesse sentido, é importante destacar que, apesar do entendimento firmado no Enunciado nº 1/2022, o Guia Orientativo sobre a hipótese legal do legítimo interesse trouxe uma perspectiva preocupante sobre o tratamento de dados

pessoais de crianças e adolescentes. Exemplo de afirmativa presente no Guia Orientativo que gerou apreensão foi a de que o uso do legítimo interesse seria mais apropriado em situações específicas como quando há uma relação direta do controlador com os titulares e quando o tratamento visa a proteção de direitos e interesses dos titulares ou a prestação de serviços a ele benéficos. O Estudo Preliminar que embasou o Enunciado nº 1/2022 da ANPD concluiu que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base em todas as bases legais previstas na LGPD, desde que observado e prevalente o seu melhor interesse, a ser avaliado no caso concreto. Para chegar a esta conclusão, diversos argumentos foram considerados: (i) a flexibilidade propiciada pela possibilidade do uso de bases legais distintas, desde que o tratamento respeite o melhor interesse da criança e do adolescente; (ii) a possibilidade de estender a aplicação do melhor interesse da criança e do adolescente para todas as bases legais; (iii) a ausência de proibições jurídicas abstratas em relação a certas hipóteses legais e a necessidade de analisar as situações de forma concreta; e (iv) o tratamento não diferenciado entre as hipóteses legais, mantendo-se a ausência de hierarquia entre elas, como previsto pela LGPD. Assim, a ANPD não deve, a priori, restringir o uso de qualquer base legal, inclusive a do legítimo interesse, para o tratamento de dados pessoais de crianças e adolescentes a situações específicas. Para definir a presença do melhor interesse de crianças e adolescentes, é preciso que a Autoridade olhe para o caso concreto e considere as circunstâncias específicas do tratamento de dados pessoais em questão, como: (a) características gerais dos titulares de dados, (b) quais dados são tratados; (c) qual a finalidade do tratamento; e (d) possíveis benefícios e danos decorrentes do tratamento de dados. Além disso, a ANPD deve equilibrar o legítimo interesse com os demais princípios da LGPD. Quanto a situações que demandam maior atenção, a Câmara-e.net considera que é preciso cautela para não pressupor que o uso de dados pessoais de crianças e adolescentes para direcionamento de publicidade é negativo. No exemplo 3 do Guia do Legítimo Interesse, a Autoridade trata sobre o uso de dados de crianças e adolescentes para publicidade e traz exemplo em que a publicidade pode afetar negativamente os direitos e liberdades fundamentais dos menores. Ocorre que a publicidade online (inclusive para menores de idade) é uma atividade lícita e regulamentada, portanto, é importante que a ANPD reconheça a licitude e possíveis benefícios da atividade no escopo de sua atuação com relação à proteção de dados pessoais de menores. Resposta na íntegra enviada via e-mail.","705523":"Contribuição da Câmara Brasileira da Economia Digital: O §1º do artigo 14 da LGPD estabelece que o tratamento de dados pessoais de crianças deve ser realizado com base no consentimento específico e em destaque (quando essa for a hipótese legal eleita pelo controlador), dado por pelo menos um dos pais ou pelo responsável legal. Primeiramente, é importante destacar que a exigência do consentimento específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal, se aplica apenas às crianças, não se estendendo aos adolescentes. Neste contexto, vale lembrar que o Estatuto da Criança e do Adolescente (ECA) diferencia, em seu artigo 2º, a criança (pessoa de até 12 anos incompletos) do adolescente (pessoas entre 12 e 18 anos) e estabelece, em seu artigo 6º, o dever de interpretar suas normas considerando a condição peculiar de desenvolvimento desses sujeitos. Necessário esclarecer, ainda, que o consentimento não é a única base legal para o tratamento de dados pessoais de crianças e adolescentes e que não há prevalência de

tal base legal em relação às demais hipóteses de tratamento. De modo convergente a este entendimento, esta Autoridade editou o Enunciado nº 1 de 2023, por meio do qual firmou o entendimento de que o tratamento de dados pessoais de crianças e adolescentes pode ser feito com base nas hipóteses legais previstas tanto no artigo 7º quanto no artigo 11º da LGPD. Para trazer maior segurança jurídica nos casos em que a base legal do consentimento será usada para o tratamento de dados pessoais de crianças e adolescentes, é necessário que a Autoridade esclareça o que entende por consentimento "específico e em destaque". Em relação ao consentimento "específico", a Câmara-e.net entende que deve haver flexibilidade na interpretação sobre seu nível de granularidade, desde que o usuário seja informado com um grau razoável de transparência sobre o fluxo de dados, por meio de informações claras, precisas e facilmente acessíveis, capazes de proporcionar clareza ao titular para uma decisão mais informada. Essa perspectiva se justifica em prol de uma transparência eficaz e também para evitar os efeitos negativos da fadiga do consentimento. Quanto ao termo "em destaque", a ANPD deve garantir uma flexibilidade conceitual que considere as diferenças técnicas de cada serviço ou produto, evitando um modelo rígido e padronizado que não leve em conta as diversas naturezas e propósitos. Isso permitirá que os regulados se adaptem aos seus contextos específicos de atuação, com diferentes interfaces. ","708742":"Contribuição da Câmara Brasileira da Economia Digital: Primeiramente, é importante salientar a tensão inerente entre a efetividade dos mecanismos de verificação de consentimento parental e o princípio da necessidade de dados. Mecanismos de verificação mais precisos muitas vezes exigem uma coleta maior de dados, o que pode gerar insegurança para o controlador, haja vista potenciais interpretações restritivas do princípio da necessidade. A ANPD deve, portanto, considerar esse princípio de forma ponderada, reconhecendo que, em alguns casos, é necessário uma maior coleta de dados para confirmar que o consentimento foi realmente dado por um dos responsáveis e que não se trata de uma estratégia para contornar a regra do consentimento parental. Em outro ponto, é preciso que se considere que medidas excessivamente onerosas para obter consentimento, bem como o uso excessivo desta base legal podem dificultar que pais e responsáveis concedam o consentimento de forma efetiva. Assim, é preciso tomar cuidado com a 'fadiga do consentimento' , que na prática pode levar a que pais e responsáveis, especialmente aqueles menos familiarizados com a legislação, consintam excessivamente, gerando um efeito contrário ao pretendido. Isso destaca a necessidade de explorar outras bases legais, conforme já indicado pelo Enunciado nº 01/2023 e pelo Guia de Legítimo Interesse, e enfatiza a importância de que as medidas para obter um consentimento parental válido sejam proporcionais e práticas. Sobre os mecanismos de verificação de consentimento parental em si, é importante salientar que o European Data Protection Board ("EDPB") advoga pela proporcionalidade e destaca que o que é considerado razoável para verificar se o consentimento foi de fato fornecido pelos pais ou responsáveis legais dependerá dos riscos ligados ao tratamento, bem como das tecnologias disponíveis. O EDPB pontua que, em casos de baixo risco, a verificação via e-mail seria suficiente, enquanto em casos de alto risco, poderia ser apropriado solicitar mais provas. No mesmo sentido, o Information Commissioner's Office entende que a análise da adequabilidade dos esforços razoáveis dependerá dos riscos ensejados pelo tratamento e da tecnologia disponível. A Data Protection Commission também endossa a posição do EDPB e

realiza apontamentos relevantes: (i) em vista do princípio da minimização, é preciso cautela para não realizar uma coleta excessiva de dados ao realizar o procedimento de verificação do consentimento; (ii) em última análise, cabe às organizações (como controladoras) decidir quais métodos de verificação são mais apropriados e proporcionais; e (iii) não há um padrão de referência quanto ao que constitui “esforços razoáveis”, tendo em vista a diversidade de estruturas existentes entre os controladores (de modo que aquilo que pode ser considerado um esforço razoável para uma organização pode não ser razoável para outra). Resposta na íntegra enviada via e-mail.","708745":"Contribuição da Câmara Brasileira da Economia Digital: O Estatuto da Criança e do Adolescente faz diferenciação clara, em seu artigo 2º, entre a criança (pessoa de até 12 anos incompletos) e o adolescente (pessoas entre 12 a 18 anos), e estabelece, em seu artigo 6º, o dever de interpretação de suas normas considerando a condição peculiar de desenvolvimento desses sujeitos. A abordagem diferenciada para crianças e adolescentes exige considerar os diferentes estágios de desenvolvimento e autonomia desses titulares, gerando a desnecessidade de representação ou assistência pelos pais ou responsáveis legais no caso dos adolescentes, em respeito ao princípio da condição peculiar de pessoa em desenvolvimento e, em última análise, ao princípio do melhor interesse da criança e do adolescente. Neste contexto, a Lei Geral de Proteção de Dados Pessoais, em seu artigo 14, dispõe especificamente sobre o tratamento de dados pessoais de crianças e adolescentes, que deve ser feito visando o melhor interesse do menor e respeitando a legislação pertinente. Observa-se que, ao não mencionar a necessidade de consentimento por pelo menos um dos pais ou pelo responsável legal no §1º do artigo 14, a LGPD pretende reconhecer a validade do consentimento manifestado pelo próprio adolescente para tratamento de seus dados, atribuindo-lhe maior liberdade para exercer sua personalidade de forma autônoma, o que deve levar, naturalmente, a uma redução gradual da interferência parental. Nesse sentido, a Câmara-e.net entende que, tendo em vista a condição peculiar de pessoa em desenvolvimento, enquanto às crianças devem ser oferecidos mecanismos de controle parental, ou seja, mecanismos que permitam uma maior participação e definição dos pais e responsáveis, e aos adolescentes devem ser reservados mecanismos de supervisão parental, ou seja, mecanismos mais próximos ao monitoramento, que respeitem e promovam sua autonomia e capacidade, de acordo com os seus respectivos graus de desenvolvimento, requerendo, a depender da idade, maior ou menor autonomia. O regime de incapacidades do Código Civil Brasileiro não é o melhor parâmetro para o direito à autonomia progressiva, positivado na legislação brasileira, por tratar as crianças e adolescentes como seres passivos que precisam de controle de um adulto e não como indivíduos em desenvolvimento com capacidade de tomar decisões . Este entendimento não é harmônico com os Comentários Gerais nº 12/2009 e 25/2016 do Comitê da ONU sobre Direitos da Criança e com as recomendações da Comissão Interamericana de Direitos Humanos, que estimulam que os países adaptem suas legislações para reconhecer e efetivar a autonomia progressiva das crianças e adolescentes. O Código Civil Brasileiro não foi criado para o contexto digital, necessitando adaptações para as interações online modernas. É crucial flexibilizar a capacidade civil e a assistência para adolescentes em "atos corriqueiros" online, como criar conteúdo e interagir em plataformas . Presume-se que os pais estão cientes e concordam com essas atividades, uma vez que as plataformas têm proteções e termos conhecidos. A lei

brasileira não exige autorização explícita dos pais para todas as atividades dos adolescentes, mas espera que orientem e monitorem o uso da internet de forma abrangente e não invasiva, permitindo a participação dos jovens em atividades digitais rotineiras sob supervisão indireta. Resposta na íntegra enviada via e-mail.","705539":"Contribuição da Câmara Brasileira da Economia Digital: Em relação aos princípios, é importante considerar que o ordenamento jurídico já os estabelece. Nesse sentido, no artigo 6º, a Lei Geral de Proteção de Dados Pessoais lista uma série de princípios que devem ser considerados para salvaguardar o direito à proteção de dados. Complementarmente, o artigo 14 estabelece que o princípio do melhor interesse deve ser um balizador no tratamento de dados pessoais de crianças e adolescentes. De igual modo, o direito internacional, a Constituição Federal e o Estatuto da Criança e do Adolescente trazem uma série de princípios aplicáveis a crianças e adolescentes, incluindo o princípio da condição peculiar de pessoa em desenvolvimento. Especificamente no que tange a este princípio, a Câmara-e.net gostaria de destacar a importância de considerá-lo no tratamento de dados de crianças e adolescentes. Isso porque, é preciso que haja equilíbrio entre o desejo de proteger as crianças e os adolescentes no ambiente digital com a necessidade de respeitar o desenvolvimento de capacidades e o alcance paulatino de discernimento. Além disso, é preciso evitar perspectivas excessivas que podem afetar o gozo de diversos direitos, como: liberdade, dignidade como pessoa em processo de desenvolvimento, convivência comunitária, educação, cultura, lazer, etc. Nesse sentido, ao estabelecer orientação sobre como respeitar e proteger os direitos das crianças e dos adolescentes no ambiente digital, para além dos direitos à privacidade, proteção e segurança, o Conselho da Europa destaca outros direitos que merecem igualmente proteção, são eles: acesso ao ambiente digital, liberdade de expressão e informação, educação e participação. No mesmo sentido, a Organização para a Cooperação e Desenvolvimento Econômico (“OCDE”) entende que atores desempenham um papel ativo na definição de políticas e práticas ou prestação de serviços para crianças e adolescentes no ambiente digital devem considerar suas diferentes necessidades em vista da idade e da maturidade. No mesmo documento, a OCDE destaca que as medidas adotadas por tais atores devem: (i) ser proporcionais aos riscos, baseadas em evidências, eficazes, equilibradas e formuladas com uma visão de maximizar as oportunidades e benefícios para as crianças e adolescentes no ambiente digital; e (ii) promover a liberdade de expressão das crianças e dos adolescentes e não prejudicar outros direitos humanos e liberdades fundamentais. Assim, entende-se que a condição peculiar de pessoa em desenvolvimento deve ser considerada não só como um princípio, mas também como um parâmetro que guie não só a atuação das organizações como também da própria ANPD. O Age Appropriate Design Code do ICO, por exemplo, trabalha com cinco estágios de desenvolvimento, são eles: pré-alfabetizados e alfabetizados (de zero a cinco anos de idade); anos básicos do ensino fundamental (de seis a nove anos de idade); anos de transição (de dez a doze anos de idade); início da adolescência (de treze a quinze anos de idade); e aproximando-se da idade adulta (de doze a dezessete anos). Além disso, o escritório do Reino Unido fornece um anexo visando trazer clareza sobre os principais aspectos a serem considerados em cada fase. Resposta na íntegra enviada via e-mail.","708762":"Contribuição da Câmara Brasileira da Economia Digital: Como aspecto preliminar, a Câmara-e.net gostaria de destacar que o termo "verificação de idade" abrange

uma gama restrita de mecanismos que visam certificar a idade de um indivíduo. Nesse sentido, conforme documento elaborado pelo Future of Privacy Forum , a expressão "age assurance" é utilizada para englobar uma variedade mais ampla de mecanismos de certificação de idade: declaração, estimativa e verificação. A declaração incluiria mecanismos nos quais o usuário indica sua data de nascimento, ou nos quais o responsável declara a idade da criança ou adolescente. Já a estimativa abrangeria métodos que vão desde a estimativa da idade com base em imagens faciais até métodos que utilizam outros meios (voz, histórico de navegação, etc.). Por fim, a verificação englobaria mecanismos como aqueles que avaliam um escaneamento de documento em relação a uma foto ou vídeo, utilizando reconhecimento facial e aqueles que se utilizam de identidades digitais. No mesmo sentido, o Office of the Privacy Commissioner of Canada , em consulta que está sendo realizada sobre proteção de dados e “age assurance”, adota a terminologia sugerida pelo FPF. Em relação à temática de certificação de idade, é preciso que essa Autoridade considere que não há uma solução única e/ou perfeita. Nesse sentido, a DPC destaca que: (i) a área tecnológica de mecanismos e ferramentas de certificação de idade ainda está em desenvolvimento; e (ii) não existe uma solução única para a questão da certificação de idade, de modo que mecanismos apropriados provavelmente variarão, dependendo, por exemplo, de fatores como o serviço sendo oferecido e a sensibilidade dos dados pessoais sendo tratados. A CNIL salienta que todas as soluções atualmente propostas podem ser, em alguma medida, burladas. Além disso, ao analisar várias soluções existentes para certificação de idade, a autoridade francesa pontuou que nenhuma delas atenderia satisfatoriamente os seguintes requisitos: verificação suficientemente confiável, cobertura completa da população e respeito à proteção dos dados e privacidade dos indivíduos, bem como sua segurança. Como visto, a verificação da idade dos usuários é um desafio técnico que pode variar significativamente conforme a natureza do serviço. Assim, as orientações da ANPD devem reconhecer que não existe um método único de verificação que seja melhor que outros, pois a escolha do mecanismo adequado depende do contexto específico, incluindo a finalidade e a natureza do tratamento dos dados, bem como o modelo de negócios envolvido. Ainda, é crucial considerar que os sistemas de verificação de idade não são infalíveis e que cada método pode apresentar suas próprias limitações e vantagens; A possibilidade de crianças burlarem esses mecanismos, como ao usar o celular dos pais, exemplifica a falibilidade dessas medidas. Nesse sentido, é fundamental que a autoridade enxergue esses esforços com base em melhores esforços; ou seja, mecanismos para que se tente identificar possíveis fraudes e corrigi-las. A Electronic Frontier Foundation (“EFF”) , em 2023, levantou preocupações importantes sobre o equilíbrio dos riscos associados aos mecanismos de verificação de idade. A EFF argumenta que tais sistemas funcionam como formas de vigilância, o que leva a organização a se opor a leis que obrigam a implementação desses mecanismos. Esse debate destaca a complexidade de encontrar um equilíbrio adequado entre a proteção dos dados e a privacidade dos usuários e as preocupações com a vigilância excessiva. Nesse sentido, a avaliação da razoabilidade e a proporcionalidade são essenciais, especialmente considerando que pequenas empresas podem enfrentar custos significativos na implementação dessas ferramentas, enquanto grandes empresas de tecnologia podem ter recursos mais abundantes. Resposta na íntegra enviada via e-mail.","708764":"Contribuição da Câmara Brasileira da Economia Digital:

Inicialmente, é preciso esclarecer o recorte do artigo 14, §4º da LGPD, que dispõe que os controladores não deverão condicionar a participação de crianças em jogos, aplicações de internet e outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. O parágrafo faz remissão clara às disposições do parágrafo 1º, sobre tratamento de dados pessoais de crianças, e não de adolescentes, qualquer interpretação extensiva na tentativa de equiparar crianças e adolescentes poderia gerar violação ao princípio da condição peculiar de pessoa em desenvolvimento, presente nas mais diversas normas protetivas, como na Constituição Federal, no Estatuto da Criança e do Adolescente na Convenção sobre os Direitos da Criança, promulgada pelo Decreto nº 99.710/1990 e com a Doutrina. Como destacado pela Câmara-e.net em outros momentos desta contribuição, é importante considerar o princípio do melhor interesse e a condição peculiar da pessoa em desenvolvimento no tratamento de dados de crianças e adolescentes. É preciso evitar perspectivas excessivas que podem afetar o gozo de diversos direitos, como: liberdade, dignidade como pessoa em processo de desenvolvimento, convivência comunitária, educação, cultura, lazer, etc., para que haja equilíbrio entre o desejo de proteger as crianças e os adolescentes no ambiente digital com a necessidade de respeitar o desenvolvimento de capacidades e o alcance paulatino de discernimento. Qualquer restrição automática ou pré-definida para a coleta de dados pessoais de crianças e adolescentes para além das já explícitas na legislação, pode resultar em maior insegurança para os menores e agentes de tratamento. Além disso, a LGPD não estabelece restrições específicas ao tratamento de dados de crianças e adolescentes, inclusive dados pessoais sensíveis, desde que o agente de tratamento justifique com base legal adequada, implemente medidas necessárias para cumprimento das obrigações estabelecidas pela LGPD e que este tratamento seja alinhado com o melhor interesse dos menores. Em relação à formação de perfis comportamentais, embora exista uma tendência de enxergar a prática com preocupação, estes não devem ser associados automaticamente a práticas prejudiciais. O uso destas tecnologias representa diversos benefícios, principalmente quanto ao tratamento de dados de crianças e adolescentes. Por vezes, é necessário formar perfis comportamentais para cumprimento de obrigações legais, regulatórias e até mesmo para indicar conteúdos adequados à idade do usuário e restringir o conteúdo inadequado. A formação de perfis comportamentais também pode ser usado no combate de ilícitos, para melhorar a precisão da estimativa de idade, além de permitir personalização de serviços para oferecer experiências relevantes e seguras para crianças e adolescentes, dentre outras várias situações nas quais as técnicas de elaboração de perfis comportamentais são utilizadas, justamente, no melhor interesse da criança e do adolescente. ","708768":"Contribuição da Câmara Brasileira da Economia Digital: Aproveita-se o questionamento para reiterar que nem sempre o consentimento será a melhor forma de salvaguardar o melhor interesse de crianças e adolescentes. Esse foi o entendimento esposado pela ANPD no estudo que fundamentou o Enunciado CD/ANPD nº 01/2023. Embora o consentimento possa ser uma ferramenta importante na proteção de dados de crianças e adolescentes, em alguns casos seu uso não será a solução mais adequada. A necessidade de equilibrar a proteção e a autonomia na proteção de crianças e adolescentes no ambiente digital também fundamenta essa perspectiva. Nesse sentido, destaca-se que as medidas de proteção de privacidade para menores devem ser adaptáveis aos níveis de maturidade e

autonomia, em consonância com o princípio da condição peculiar de pessoa em desenvolvimento. As configurações de privacidade não devem ser rígidas, mas sim flexíveis, permitindo ajustes que correspondam à idade e ao estágio de desenvolvimento do usuário. Essa abordagem reconhece que diferentes idades e níveis de compreensão exigem diferentes níveis de proteção e interação, respeitando a autonomia progressiva e o melhor interesse da criança e do adolescente, conforme a legislação brasileira e internacional exigem. Nesse sentido, a Câmara-e.net entende que, tendo em vista a condição peculiar de pessoa em desenvolvimento, enquanto às crianças devem ser oferecidos mecanismos de controle parental, ou seja, mecanismos que permitam uma maior participação e definição dos pais e responsáveis, e aos adolescentes devem ser reservados mecanismos de supervisão parental, ou seja, mecanismos mais próximos ao monitoramento, que respeitem e promovam sua autonomia e capacidade, de acordo com os seus respectivos graus de desenvolvimento, requerendo, a depender da idade, maior ou menor autonomia.". Em outro ponto, é preciso que se considere a diversidade de agentes que atuam no ecossistema digital, diversidade essa que encontra-se refletida nas medidas adotadas por esses atores, são exemplos: ¿

Redes sociais: mecanismos de sincronização familiar, que vinculam a conta dos pais às dos filhos; ajustes do tempo de uso de tela pelos responsáveis; ativação de restrições como: impedimento para iniciar lives, aplicação de filtros a comentários publicados, restrição de quem pode enviar mensagens aos adolescentes; disponibilização de ferramentas que promovem o diálogo entre os pais e os adolescentes; transparência voltada aos pais e responsáveis; mecanismos de limitação de anúncios; acesso as interações com terceiros; possibilidade de edição do perfil; impossibilidade de participação em programas de recompensa, recarga e gratificação, sem assistência; limitação do conteúdo visualizado; possibilidade de denunciar contas de terceiros; ¿ Plataformas de compartilhamento de vídeos: atualizar informações e configurações da conta; excluir a conta; gerenciar os controles de atividades; ¿ Plataformas de streaming: escolher os conteúdos que serão disponibilizados; criar um perfil que terá apenas conteúdo selecionado para crianças e que não terá acesso as configurações da conta; criação de perfis com classificação indicativa; gerenciamento do perfil; ¿ Plataformas de e-commerce: controle das compras feitas; ¿

Jogos: definir permissões para contar de crianças e adolescentes que afetam atividades específicas (jogos multijogador, convites para entrar em jogos de outros jogadores, possibilidade de comunicação, compras); limitação de compras; recomendações de idade que consideram o conteúdo; possibilidade de gerenciamento do conteúdo acessível; e ¿

Lojas de aplicativos: aplicativos e conteúdos de vídeo com classificação indicativa, ferramenta de controle parental que permite selecionar, com base nas faixas etárias, quais aplicativos serão visíveis na loja; organizador pode usar recursos como: “restrições”, “tempo de uso” e “pedir para comprar”; possibilidade de restringir o uso de certas ferramentas e o uso de certos aplicativos; possibilidade de aprovação, pelos pais, do download de aplicativos; e realização de verificação de idade. ","708772":"Contribuição da Câmara Brasileira da Economia Digital: A transparência direcionada aos pais e responsáveis ajuda a garantir uma supervisão eficaz sobre o uso de plataformas por crianças e adolescentes. Guias específicos, com uma linguagem clara e acessível, são importantes para que os pais compreendam as ferramentas e mecanismos disponíveis para o cumprimento de seu dever de supervisão.

Embora a Política de Privacidade (PP) deva conter todas as informações necessárias sobre o tratamento de dados, não é necessário que ela seja exibida continuamente, o que poderia causar fadiga aos usuários e seus responsáveis. Em vez disso, é mais eficiente relembrar as informações específicas sobre o tratamento em momentos pertinentes e diretamente relacionados às ações do serviço. As informações fornecidas aos usuários e seus responsáveis precisam ser relevantes e compreensíveis. A quantidade de informações não garante transparência, especialmente se essas informações forem complexas e menos propensas a serem lidas e compreendidas. Além da PP, outros meios de comunicação, como artigos em centrais de transparência, se disponíveis, ou notícias divulgadas pelos agentes de tratamento, podem complementar a transparência. Esses meios adicionais podem ajudar a assegurar que os dados sejam tratados para finalidades legítimas e informadas ao titular, especialmente durante a utilização dos produtos e serviços, por meio de notificações e outros recursos específicos. A transparência deve ser adaptada às necessidades e às características dos usuários. Isso pode ser alcançado através de portais e outros meios que utilizem elementos visuais, interativos e de linguagem facilitada para tornar a compreensão das informações mais acessível para adolescentes. A adoção de mecanismos que transmitam a informação de forma facilitada (como vídeos lúdicos ou gamificação) pode ser uma alternativa. Além disso, é importante fornecer suporte e informações apropriadas aos pais e responsáveis legais sobre as práticas de tratamento de dados e recursos de supervisão parental. Entretanto, entendemos que não há necessidade de a Política de Privacidade conter uma seção específica dedicada ao tratamento de dados de menores. Em vez disso, uma abordagem positiva é adotar uma Política que utilize uma linguagem clara e acessível, considerando as necessidades específicas deste público e mais compreensíveis tanto para os menores quanto para seus responsáveis. Deste modo, a Política pode oferecer uma proteção robusta e adequada sem a necessidade de uma seção separada. É necessário, ainda, equilibrar a transparência com a proteção dos segredos comerciais e industriais. Informações excessivas sobre ferramentas de tratamento de dados podem facilitar a ação de agentes mal-intencionados que busquem contornar mecanismos de segurança, colocando em risco a proteção dos usuários. Portanto, deve-se estabelecer uma transparência adequada que priorize a segurança e os melhores interesses dos titulares dos dados. Por fim, manter uma colaboração contínua com pais, responsáveis legais e adolescentes ajuda a aprimorar os recursos de transparência disponíveis. Essa parceria é importante para melhorar a compreensão e a gestão das questões de privacidade e segurança, ajustando as práticas para atender às necessidades e preocupações dos usuários. ","708775":"Contribuição da Câmara Brasileira da Economia Digital: A Câmara-e.net gostaria de chamar a atenção desta Autoridade para a crescente importância e complexidade das discussões sobre a proteção de crianças e adolescentes no ambiente digital. Em meio a debates em diversos fóruns e iniciativas de diferentes entidades, há um potencial significativo de conflitos relacionados às competências da ANPD e à integridade da Lei Geral de Proteção de Dados. Assim, para além dos aspectos trazidos ao longo desta tomada de subsídios, a Câmara-e.net encoraja respeitosamente a ANPD a adotar medidas e emitir posicionamentos que fortaleçam não só sua autoridade como órgão competente para regulamentar o tratamento de dados pessoais de crianças e adolescentes, mas também para

evitar conflitos com a própria LGPD e com os entendimentos já consolidados pela própria Autoridade sobre a temática.

Contribuinte: MAIRA LOBO HAYASHIDA BARRETO

Número: OP-753091

Data: 16/08/2024 - 14:23

Resumo: :"PARTE 1: A Associação Latino-Americana de Internet (ALAI) destaca os seguintes pontos: ¿ Definição vaga no Guia de Legítimo Interesse: A ANPD utilizou diretrizes da OCDE e da ONU para definir o "melhor interesse" da criança e do adolescente, mas essas orientações são vagas e insuficientes para que os controladores de dados atuem com segurança no contexto de proteção de dados pessoais. ¿ Papel da ANPD e de outras autoridades competentes na definição do “melhor interesse” no âmbito de proteção de dados pessoais: A ANPD e outras autoridades competentes (que devem considerar o melhor interesse de crianças e adolescentes na interface com suas respectivas áreas) têm a oportunidade de esclarecer o que constitui o melhor interesse desses usuários, assegurando assim a consistência e eficácia na aplicação das normas de proteção de dados. Isso ajudará a manter um equilíbrio adequado entre a proteção efetiva dos titulares e a promoção da segurança jurídica, beneficiando a todos. ¿ O melhor interesse da criança e do adolescente não deve ser considerado um “cheque em branco”, de forma a permitir propostas de regulações esparsas por diferentes autoridades e órgãos. Neste sentido, é importante garantir cooperação entre diferentes atores, para se atingir entendimentos consistentes sobre como alcançar o melhor interesse desses titulares no caso concreto, inclusive considerando os limites e as competências previstas nas legislações e regulações existentes. ¿ Por exemplo - Resolução Nº 245/2024 - CONANDA e Projeto de Lei n° 2628, de 2022 - estabelecimento de regras para proteger crianças e adolescentes no ambiente digital. Além de ser questionável se o CONANDA tem a competência para emitir regulamentações impondo novas obrigações não fundamentadas na Lei Federal, ambos faltam com uma análise técnica adequada sobre os desafios e riscos associados à proteção de dados pessoais. Tal deficiência resulta na proposta de obrigações excessivamente onerosas que, paradoxalmente, podem prejudicar a proteção de crianças e adolescentes. ¿ Necessidade de segurança jurídica: A ANPD e outras autoridades competentes devem parametrizar de forma mais objetiva o "melhor interesse" da criança e do adolescente sob a perspectiva de proteção de dados pessoais. Embora não se trate de um conceito fechado e definido ex ante, seria essencial conferir maior concretude, por exemplo utilizando mecanismos já mobilizados em outras oportunidades, como exemplos e situações hipotéticas que considerem nuances concretas e esforços tecnicamente disponíveis, mantendo flexibilidade para diferentes contextos e modelos de negócio. ¿ Aplicação do princípio da minimização de dados: Considerando que há uma possível tensão inerente entre o princípio da minimização de dados pessoais e a efetividade de mecanismos de verificação e detecção de idade, é essencial estabelecer parâmetros para que os agentes de tratamento possam se orientar. Coletar determinados dados pessoais pode, em certos casos, atender melhor ao interesse da criança e do adolescente, como na eficácia de barrar o acesso a conteúdos ou

plataformas impróprios para a sua idade. Porém, o princípio da necessidade/minimização também determina que a coleta de dados deve contemplar apenas os dados estritamente necessários e não excessivos. Considerando que não há clareza sobre quais dados são considerados “estritamente necessários” neste contexto, e se a existência de salvaguardas pelos agentes de tratamento poderia mitigar eventuais riscos decorrentes dessa tensão, seria importante que a ANPD e outras autoridades competentes enfrentassem esse “trade-off”, para se garantir maior segurança jurídica aos agentes de tratamento. ","708725":"A Associação Latino-Americana de Internet (ALAI) considera que: ¿ Em relação ao princípio do melhor interesse, em certos contextos, há maior facilidade em identificar o que seria o comportamento esperado do lado dos agentes de tratamento. No entanto, sua aplicação pode ser mais complexa em outros contextos, em que é difícil equilibrá-lo com os demais princípios da LGPD. ¿ Exemplo 1 - Perfilamento para publicidade personalizada: há necessidade de equilibrar os benefícios da publicidade personalizada com os riscos à privacidade, afastando-se de um entendimento de que a publicidade personalizada (que não seja abusiva ou ilícita) é negativa em si mesma. ¿ A publicidade personalizada envolve a utilização de dados específicos do usuário, como idade e interesses, para direcionar anúncios relevantes ao perfil individual. ¿ A personalização da publicidade pode proteger menores ao tornar os anúncios mais adequados para eles. Isso evita que anúncios baseados em dados genéricos exponham crianças a conteúdos inadequados. Considerando fatores como idade ou localização, a personalização garante uma filtragem mais precisa e segura, tornando a experiência online mais relevante e segura, e criando um ambiente digital adaptado às necessidades e interesses das crianças. ¿ As diretrizes devem garantir que a publicidade respeite a autonomia progressiva dos adolescentes, assegurando uma experiência online segura e adequada. ¿ Conforme o Guia do LI, o teor da publicidade é crucial para determinar se ela atende ao melhor interesse do menor. Assim, a publicidade personalizada pode ser adequada dependendo de seu conteúdo, destacando a importância de avaliar o tipo de produto anunciado ao considerar o legítimo interesse. ¿ Exemplo 2 - Perfilamento para direcionamento de conteúdo: O perfilamento também pode ser uma prática que atende ao melhor interesse da criança, visto que pode ser utilizado para direcionar conteúdos adequados à idade dos usuários (e vedar que conteúdos inadequados sejam exibidos). ¿ Diferença de conceito: o perfilamento para fins de publicidade refere-se à coleta e análise de dados especificamente para criar anúncios personalizados, enquanto perfilamento para conteúdo envolve a utilização de dados para oferecer conteúdo relevante e apropriado ao usuário, sem fins publicitários. ¿ Exemplo 3 - Processamento de dados pessoais de crianças e adolescentes para protegê-los de interações indesejadas, através do envio de alertas de segurança quando abordados por adultos. Neste caso, a criação de perfis também pode ser uma prática que serve ao melhor interesse. ¿ Novamente, a questão do melhor interesse pode ser menos óbvia nestes contextos e por isso é crucial que a autoridade forneça diretrizes e balizas para avaliar e mitigar esses riscos.","705523":"A Associação Latino-Americana de Internet (ALAI) destaca os seguintes pontos sobre o tema apresentado: ¿ Escopo do termo “consentimento” na presente contribuição: É necessário frisar que a autorização concedida para a utilização de produtos/serviços específicos oferecidos (por meio dos Termos de Serviço, por exemplo) é diferente do consentimento para o tratamento de dados de crianças,

em situações específicas. ¿ As considerações abaixo dizem respeito apenas a este último. Parâmetros para definição de criança e adolescente: Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente): "Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade." ¿ Consentimento parental apenas para crianças: considerando o ponto acima, e em linha com a legislação brasileira (como o artigo 4, §1º da LGPD) e com posicionamentos internacionais sobre o tema, [1] cumpre frisar que, quando o consentimento for a base legal adequada, apenas as atividades de tratamento envolvendo dados de crianças podem exigir consentimento parental. - Conforme explicado mais detalhadamente no item 3 abaixo desta mesma seção, levando em conta a autonomia e o desenvolvimento progressivo de menores de idade, é importante considerar que adolescentes devem ser capazes de fornecer seu próprio consentimento. ¿ Possibilidade da aplicação de outras bases legais: o consentimento nem sempre é a base legal mais adequada para o tratamento de dados pessoais de crianças e adolescentes, conforme os posicionamentos da ANPD, incluindo o Enunciado nº 01/2023 e o Guia de Legítimo Interesse. ¿ No caso de o consentimento parental ser considerado a base legal adequada para o tratamento de dados pessoais de crianças: ¿ ANPD deve esclarecer o conceito de "consentimento específico": O critério de "consentimento específico" deve ser esclarecido, de forma a garantir segurança jurídica aos agentes de tratamento sobre o formato esperado desse consentimento. ¦ Independentemente de como esse consentimento específico poderá ser atingido, é necessário levar em consideração que uma granularidade do consentimento - no sentido de detalhamento de forma extremamente compartimentalizada - não significa necessariamente maior clareza ao titular e/ou uma decisão mais informada. ¦ Ademais, o referido consentimento não deve funcionar como uma ferramenta de "controle" de pais e responsáveis legais sobre as ações de crianças, mas sim como uma forma de consentir com o tratamento dos dados pessoais de crianças para finalidades específicas, conforme informadas aos titulares e seus responsáveis legais, garantindo a legitimidade do tratamento. ¿ ANPD deve esclarecer o conceito de "consentimento em destaque": a autoridade deve garantir que o conceito seja flexível o suficiente para considerar tanto os meios técnicos disponíveis quanto às diferentes naturezas e propósitos dos produtos ou serviços. Assim, deve estabelecer parâmetros mínimos sem impor uma padronização rígida, permitindo que os regulados se adaptem aos seus contextos específicos (e.g., ao seu setor de atuação, à interface utilizada, etc.). [1] Neste sentido, a ICO - Information Commissioners' Office (autoridade de proteção de dados do Reino Unido) entende, por exemplo, que "13 é a idade em que crianças no Reino Unido podem fornecer seu próprio consentimento para o tratamento, se você estiver se baseando no consentimento como a sua base legal para o tratamento no contexto da oferta de um serviço online diretamente para uma criança.","708742":"A Associação Latino-Americana de Internet (ALAI) destaca a possibilidade da aplicação de outras bases legais, por isso considera a importância dos seguintes pontos: ¿ Parametrização contextual: Para definir parâmetros de adoção para viabilizar e verificar que o consentimento foi fornecido pelos pais/ responsáveis, a ANPD deve levar em conta os esforços razoáveis baseados na tecnologia disponível, recursos, nível de risco, naturezas e propósitos dos serviços e produtos. A autoridade não deve estabelecer medidas rígidas, mas diretrizes flexíveis e, em especial, que estejam adequadas à forma como

interagem o titular e o agente de tratamento. Além disso, deve esclarecer parâmetros para que esse consentimento possa ser obtido de maneira que respeite a privacidade, garantindo que os métodos sejam práticos e adequados. ¿ Exemplo - no Guia da ICO Children 's code guidance and resources - age appropriate application: a autoridade deixa claro a consideração de esforços razoáveis para a obtenção do consentimento parental. O Guia também esclarece que o consentimento deve ser obtido de maneira menos intrusiva possível à privacidade, coletando o mínimo de identificadores pessoais. ¿ Exemplo - FTC/EUA “Regra de Proteção à Privacidade Online das Crianças: Um Plano de Conformidade em Seis Etapas para Seu Negócio” - A COPPA permite que se escolha o método de consentimento, desde que ele seja projetado de maneira razoável para garantir sua concessão pelo pai/mãe, tendo em vista as tecnologias disponíveis. ¿ Exemplos: Seria mais produtivo se a autoridade indicasse exemplos de padrões adequados em determinados contextos, ao invés de buscar definir rigidamente os mecanismos mais apropriados. Essa alternativa reconhece a impossibilidade de padronizar mecanismos para serviços tão variados, mas ainda fornece parâmetros claros aos agentes de tratamento, permitindo uma abordagem mais flexível. Assim, facilitaria a implementação em uma ampla gama de produtos, aumentando a eficácia da proteção. ¿

Medidas excessivamente onerosas para obter consentimento podem dificultar que pais e responsáveis concedam esse consentimento de forma efetiva. É preciso tomar cuidado com a “fadiga do consentimento”- na prática pode levar a que pais, especialmente quando menos familiarizados com a legislação, consintam excessivamente, gerando um efeito contrário ao pretendido ¿ Isso destaca a necessidade de explorar outras bases legais, conforme já indicado pelo Enunciado nº 01/2023 e o Guia de Legítimo Interesse, e enfatiza a importância de que as medidas para obter um consentimento parental válido sejam proporcionais e práticas.","708745":"PARTE 1: A Associação Latino-Americana de Internet (ALAI) reforça a necessidade de se diferenciar a autorização para utilizar o aplicativo não deve se confundir com o consentimento enquanto base legal para o tratamento de dados pessoais, por isso considera a importância dos seguintes pontos: ¿ Diferenciar o consentimento enquanto base legal e a concordância relativa a uma relação contratual estabelecida entre o agente de tratamento e o titular. A LGPD não altera a capacidade dos menores de idade de celebrar um contrato legal válido, de modo que o agente de tratamento poderá utilizar qualquer uma das bases legais disponíveis para tratar os dados pessoais de adolescentes. ¿ A autonomia progressiva deve levar a uma redução gradual da interferência parental, respeitando a crescente capacidade dos adolescentes de exercerem seus direitos de forma independente. É possível considerar a autonomia progressiva de adolescentes no ambiente digital sem necessidade de representação ou assistência dos pais, alinhado ao princípio do melhor interesse. Para tanto, podem ser oferecidos mecanismos de supervisão parental que estejam alinhados ao grau de autonomia do adolescente. ¿ O melhor interesse apenas estará corretamente refletido considerando a autonomia e o desenvolvimento progressivo desses titulares, que pode gerar a desnecessidade de representação ou assistência pelos pais ou responsáveis legais: o regime de incapacidades do Código Civil Brasileiro não é o melhor parâmetro para o direito à autonomia progressiva, positivada na legislação brasileira. ¿

Tradicionalmente, a teoria civilista via as crianças como seres passivos, necessitando de controle adulto, mas essa visão está sendo desafiada pela ideia de que os jovens devem ser

vistos como indivíduos capazes de tomar decisões juridicamente relevantes. Essa mudança é reforçada por orientações internacionais [Comitê da ONU sobre Direitos da Criança, nos Comentários Gerais nº 12/2009 e 25/2016 e recomendações da Comissão Interamericana de Direitos Humanos], que instam os países a adaptar suas legislações para reconhecer e efetivar a autonomia progressiva das crianças e adolescentes, alinhada ao princípio do melhor interesse da criança. (Imperiosa revisão do regime de incapacidades pela comissão de atualização do Código Civil) ¿ O Código Civil Brasileiro não foi confeccionado no contexto digital e, portanto, à medida que as interações online evoluíram, é necessário adaptá-lo às realidades do uso moderno de plataformas digitais. ¿ A capacidade civil e as formas de representação ou assistência para adolescentes devem ser mais flexíveis, especialmente em relação às atividades online consideradas "atos corriqueiros" - como o uso de uma plataforma projetada para criação de conteúdo, consumo de vídeos e interação com outros usuários - conforme atualmente defendido por professores e doutrinadores brasileiros (Leal, Sheila do Rocio Cercal Santos. Contratos eletrônicos: validade jurídica dos contratos via Internet; Schreiber, Anderson. "Releitura das Incapacidades". In: Manual de Direito Civil Contemporâneo; Tepedino, Gustavo. "Esboço de uma classificação funcional dos atos jurídicos". Instituto Brasileiro de Direito Civil). ¿ Há, assim, uma presunção de que os pais estão cientes e concordam com os "atos corriqueiros" realizados pelos menores na internet, tal como acesso a uma plataforma (que possui mecanismos de proteção à criança e ao adolescente e é regida por termos os quais, em geral, os pais já conhecem e já validaram). ¿ A lei brasileira não exige a autorização explícita ou expressa dos pais para todas as atividades dos adolescentes. Em vez disso, dentro da lei, há uma compreensão implícita de que os menores se envolvem em atividades online com algum nível de conhecimento ou autorização dos pais. ","705539":"A Associação Latino-Americana de Internet (ALAI) reforça a importância da interpretação contextual do princípio da minimização de dados em relação ao perfilamento como técnica para adequar o conteúdo a menores de idade. ¿ Torna-se necessário parâmetros flexíveis e adaptáveis a diferentes produtos e serviços, considerando a disponibilidade tecnológica, sua natureza e seu propósito, conforme o melhor esforço. Os parâmetros devem considerar a disponibilidade de soluções tecnológicas já existentes em toda a cadeia de valor, incluindo dispositivos e sistemas operacionais. ¿ Em respeito à autonomia progressiva, as ferramentas de privacidade devem também acompanhar o crescimento e maturidade do usuário - há exemplos em que usuários de 13 a 15 anos têm suas contas configuradas como privadas por padrão, permitindo que escolham o que compartilhar, quando e com quem. Além disso, há possibilidade de limitar que o envio de mensagens só esteja disponível para aqueles com 16 anos ou mais, assim como hospedar uma LIVE é limitado aos membros da comunidade que devem ter pelo menos 18 anos. ¿ Há alguns mecanismos que podem ser citados como boas práticas: ¿ Limites diários de tempo de tela: Estabelecimento automático de um limite de tempo de uso diário, que promove a consciência sobre o tempo gasto online. Painéis para manter controle do tempo de tela, bem como a possibilidade de silenciar notificações, também são bons exemplos. ¿ Gerenciamento ativo de tempo: Opções para que os jovens ajustem seus próprios limites de tempo após alcançar o limite padrão, incentivando a tomada de decisão consciente. ¿ Controles parentais expandidos: Ferramentas que permitem aos pais personalizar os limites de tempo de

tela e configurar horários específicos para silenciar notificações, auxiliando na gestão do bem-estar digital, ou que fornecem aos pais informações sobre as interações recentes de usuários menores com outros usuários. Importante que essas ferramentas não invadam a privacidade do usuário menor de idade (como fornecer acesso às mensagens trocadas com outros usuários), mas apenas auxiliem na tomada de decisão. ¿ Notificações programadas: Configuração de horários para silenciar notificações automaticamente, ajudando a minimizar interrupções durante períodos de descanso ou estudo. ¿ Remoção de contas suspeitas de menores de idade a partir de esforços humanos: equipe de segurança treinada para identificar sinais de que uma conta pode ser de um usuário jovem, que esteja burlando os mecanismos de verificação de idade. ¦ Para auxiliar nessa detecção, utilizam-se informações adicionais fornecidas pelos usuários da plataforma, como palavras-chave e denúncias feitas através do aplicativo pela comunidade, ou por meio de relatórios enviados por não-usuários.","708762":"PARTE 1: A Associação Latino-Americana de Internet (ALAI) considera que não há orientações claras por parte da ANPD, o contexto de insegurança jurídica é agravado pela multiplicidade de disposições e atores envolvidos no processo de regulamentação, por isso é importante destacar os seguintes pontos: ¿ O papel da ANPD é fundamental para definir balizas para mecanismos de avaliação de idade, que deverão considerar a natureza do serviço prestado e ponderar interesses conflitantes (e.g., robustez da avaliação de idade vs princípio da minimização). ¿ A ANPD, enquanto autoridade no setor, tem a oportunidade de liderar o estabelecimento de balizas s para mecanismos de avaliação de idade desses usuários, assegurando assim a consistência e a eficácia na aplicação das normas de proteção de dados.. ¿ Com base nas terminologias adotadas pelo Center for Informaiton Policy Leadership (CIPL), a ANPD deve considerar que a avaliação de idade pode envolver diferentes métodos, incluindo: (i) verificação de idade, (ii) estimativa/predição de idade, e (iii) declaração de idade. ¿ Essa interpretação também é adotada pelo Information Commissioner's Office (ICO), que estabelece que "avaliação de idade" se refere coletivamente às abordagens utilizadas para: (i) garantir que as crianças não consigam acessar conteúdo adulto, nocivo ou inadequado ao utilizar determinados serviços; e (ii) estimar ou estabelecer a idade de um usuário, para que os serviços possam ser adaptados às suas necessidades e para que proteções sejam implementadas, de acordo com a sua idade. ¿ Ainda com base no material disponibilizado pelo ICO: "verificação de idade" seria qualquer método projetado para verificar a idade exata de usuários, ou confirmar que um usuário é maior de 18 (dezoito) anos; "estimativa/predição de idade" seria qualquer método projetado para estimar a idade, ou a faixa etária, de um usuário; e "declaração de idade" seria um método de autodeclaração, em que o usuário é solicitado a declarar sua idade, mas nenhuma outra evidência é necessária para confirmar a veracidade da declaração. "Técnicas em cascata" seriam os métodos em que diferentes abordagens de avaliação de idade são combinadas. A ANPD também deve garantir que as medidas de avaliação de idade sejam acessíveis e econômicas para os diversos participantes do mercado, e adequadas ao risco. Outro fator importante a ser levado em consideração pela ANPD são os esforços razoáveis adotados pelos agentes, considerando o estado da arte das tecnologias disponíveis e padrões internacionais. ¿ As orientações da ANPD devem levar em conta que medidas de avaliação de idade representam um desafio para toda a indústria e levantam, entre outros, potenciais

riscos à privacidade. Especificamente: a. A avaliação da idade dos usuários apresenta desafios técnicos que podem variar significativamente conforme a natureza do serviço. ¿

As orientações devem reconhecer que não há um único método de avaliação de idade superior a outros, pois a escolha depende do contexto específico, incluindo a finalidade e a natureza do tratamento dos dados, as limitações técnicas e o estado da arte das tecnologias disponíveis, bem como o modelo de negócios envolvido (já que, dependendo dos serviços/funcionalidades sendo oferecidos, mecanismos de avaliação de idade podem se basear em parâmetros diferentes). b. Há debates importantes sobre a necessidade de equilibrar os riscos dos mecanismos de avaliação de idade. Por exemplo, a Electronic Frontier Foundation (EFF) indicou, em 2023, que “os sistemas de verificação de idade são sistemas de vigilância” e, por isso, a organização é contrária a leis que obriguem a implementação de mecanismos de verificação de idade.","708764":"A Associação Latino-Americana de Internet (ALAI) considera a importância dos seguintes pontos: A coleta de dados pessoais de crianças e adolescentes não deve ser automaticamente limitada por critérios pré-definidos além daqueles já explícitos na legislação (ou seja, finalidades ilícitas). Qualquer restrição imposta deve considerar o melhor interesse desses indivíduos. A definição de diretrizes claras sobre o que constitui o melhor interesse desses titulares de dados ajudaria a clarificar e orientar essas decisões. ¿ Conforme a LGPD e outras legislações, desde que os agentes de tratamento justifiquem uma base legal adequada, implementem as medidas necessárias para cumprir as obrigações estabelecidas pela LGPD e garantam que o tratamento dos dados esteja alinhado com o melhor interesse das crianças e adolescentes, não existem restrições específicas ao tratamento de dados de crianças e adolescentes, inclusive dados pessoais sensíveis. ¿ A formação de perfis comportamentais - ou perfilamento - não deve ser vista como uma atividade de tratamento de dados que apresenta riscos inerentes, especialmente para crianças e adolescentes. Além de personalizar a experiência individual em serviços/produtos oferecidos por agentes de tratamento (permitindo que acessem conteúdos de maior interesse e relevância), a perfilização desempenha papel fundamental na segurança de menores de idade. Dessa forma, o perfilamento pode ser uma prática que atende ao melhor interesse da criança, visto que pode ser utilizado para direcionar conteúdos adequados (e restringir conteúdo inadequado) à idade dos usuários. ¿ Dependendo dos objetivos a que se destinam, as atividades de perfilamento podem ser restringidas conforme as leis do panorama regulatório brasileiro;mas restrições devem ser impostas devido à violação do melhor interesse da criança e do adolescente, e não simplesmente pela realização da atividade em abstrato. o O perfilamento não é exclusivo para publicidade. Note-se que o perfilamento para fins de publicidade refere-se à coleta e análise de dados especificamente para criar anúncios personalizados, enquanto perfilamento para conteúdo envolve a utilização de dados para oferecer conteúdo relevante ao usuário, sem fins publicitários.","708768":"A Associação Latino-Americana de Internet (ALAI) considera a relevância dos seguintes pontos: ¿ Os mandatos sobre controles parentais devem levar em consideração a privacidade dos adolescentes, assim como a importância do acesso à informação e à comunidade. Eles também devem levar em conta a diversidade de serviços e permitir abordagens flexíveis. ¿ Medidas de proteção de privacidade para menores adaptáveis aos níveis de maturidade e autonomia de cada usuário em desenvolvimento: As configurações de privacidade não devem

ser rígidas, mas sim flexíveis, permitindo ajustes que correspondam ao conteúdo apropriado para a idade e ao estágio de desenvolvimento do usuário. Essa abordagem reconhece que diferentes idades e níveis de compreensão requerem diferentes níveis de proteção e interação, levando em conta a autonomia progressiva e, portanto, o melhor interesse da criança e do adolescente, conforme exige a legislação brasileira. ¿ A terminologia “supervisão parental/ de responsáveis” é, neste sentido, mais adequada do que “controle”. ¿ Exemplo - sincronização familiar: deve-se permitir que responsáveis legais e adolescentes decidam em conjunto sobre a ativação de ferramentas com graus distintos de proteção especial, que possibilita a vinculação das contas dos pais às dos filhos adolescentes. Isso facilita a gestão de configurações relacionadas a conteúdo, privacidade e bem-estar. Tais configurações, que devem ser ativadas após diálogo com os pais e responsáveis, incluem tornar a conta privada, gerenciar comentários e mensagens diretas, controlar o acesso a conteúdos através da busca, limitar o tempo de tela diário e ativar o Modo Restrito. De maneira mais específica: ¦

Tempo de Tela: Pais e responsáveis podem vincular suas contas às dos adolescentes para personalizar configurações de segurança, como o tempo de tela diário. Os responsáveis podem ajustar o tempo de uso, aplicá-lo a todos os dispositivos do adolescente e definir um código de acesso para uso adicional após o limite ser atingido. A possibilidade de monitoramento do tempo de tela também é um recurso que promove a segurança das crianças e adolescentes. ¦ Ativação de restrição de funcionalidades específicas, por exemplo: ¿

Modo restrito: funcionalidade que reduz a visualização de conteúdos potencialmente inadequados para certos públicos, como temas maduros ou complexos. Ao ativar este modo, algumas funcionalidades da plataforma são desabilitadas - por exemplo, opções de iniciar LIVEs. ¿ Modo Comentário Moderado: aplicação de filtros a comentários publicados, restringindo, por exemplo, comentários inadequados e ofensivos. ¿ Mensagens diretas: Restringir ou desativar quem pode enviar mensagens ao adolescente. ¿ Promoção da cultura de diálogo dos pais e responsáveis com crianças e adolescentes: ferramentas que incentivem os pais a discutir e explicar a ativação dessas configurações com os adolescentes são bem-vindas, porque é também de responsabilidade da família/dos responsáveis a proteção da segurança, privacidade e autonomia progressiva do menor, cumprindo com seus os direitos e deveres de educar suas crianças - tal como determina o Artigo 5 da Convenção sobre os Direitos da Criança.[1] ¿ Essa medida está alinhada com a lógica de promoção de maior conhecimento e compreensão sobre mecanismos digitais, tanto do lado dos pais, quanto do lado dos adolescentes. ¿ Transparência direcionada aos pais e responsáveis - Guias direcionados especificamente aos pais e responsáveis, com linguagem clara e transparente, facilitam a navegação destes em plataformas de nossas associadas, são ferramentas importantes para ajudá-los a compreender as ferramentas e mecanismos disponíveis para auxiliá-los em seu dever de supervisão. [1] “Os Estados Partes respeitarão as responsabilidades, os direitos e os deveres dos pais ou, onde for o caso, dos membros da família ampliada ou da comunidade, conforme determinem os costumes locais, dos tutores ou de outras pessoas legalmente responsáveis, de proporcionar à criança instrução e orientação adequadas e acordes com a evolução de sua capacidade no exercício dos direitos reconhecidos na presente convenção.”","708772":"A Associação Latino-Americana de Internet (ALAI) considera a importância dos seguintes pontos: ¿ A Política de Privacidade

não precisa aparecer a todo momento ao usuário: informações devem constar na Política de Privacidade ("PP") dos agentes de tratamento e esta deve estar em local de fácil acesso. No entanto, não necessariamente precisa aparecer a todo momento ao usuário e/ou aos seus pais e responsáveis legais, para evitar fadiga. o Em determinados casos, pode ser mais efetivo que informações específicas sejam retomadas na tela em momentos igualmente específicos, relacionados mais diretamente com um determinado tratamento. ¿ As informações fornecidas aos usuários ou pais precisam ser relevantes e facilmente compreensíveis. Meramente aumentar a quantidade de informações disponibilizadas não garante maior transparência, especialmente se essas informações forem complexas ou se houver uma expectativa de que os usuários ou pais provavelmente não as lerão. ¿ Outros meios além da PP são bem-vindos e corroboram com o dever de transparência: em não havendo qualquer tipo de proibição legal (ou determinação) de que a PP deve ser o único meio para o fornecimento de transparência, informações adicionais sobre o tratamento de dados de crianças e adolescentes podem constar em documentos apartados, além da PP, tais como de artigos disponibilizados via central de transparência e ajuda, ou mesmo notícias veiculadas pelos agentes. o A PP não deve ser o único meio de transparência para se aferir se os dados tratados por agentes de tratamento estão associados a finalidades legítimas, específicas, explícitas e informadas ao titular. A "especificidade" da transparência pode ser desenvolvida nestes outros recursos – especialmente durante a utilização de produtos e serviços pelos adolescentes, através de notificações, por exemplo. ¿ A transparência fornecida deve ser adequada/adaptada aos usuários que a utilizam. Para isso, é possível fornecer portais e outros meios específicos, que possuam elementos que facilitem a compreensão das informações por adolescentes (como ícones/apelos visuais, vídeos/áudios, conteúdo interativo, linguagem facilitada, etc). A fim de garantir o melhor interesse, também é importante dar suporte e fornecer transparência apropriada aos pais e responsáveis legais, de modo que tenham acesso a informações sobre as práticas de tratamentos de dados pessoais realizadas, recursos de supervisão parental, dentre outros. ¿ A transparência a ser fornecida deve observar os limites técnicos e os segredos comerciais e industriais dos agentes de tratamento: O fornecimento de informações excessivas sobre as ferramentas de tratamento de dados de menores de idade pode servir de subsídio para que agentes mal-intencionados burlem mecanismos de segurança de websites e plataformas, colocando em risco a segurança desses usuários – portanto, é necessário estabelecer uma transparência adequada, visando os melhores interesses desses titulares. ¿ Por fim, é importante manter uma parceria constante com pais, responsáveis legais e com os próprios adolescentes sobre como melhorar os recursos de transparência disponíveis, a fim de melhorar cada vez mais a compreensão de definições de privacidade e segurança.","708775":"A Associação Latino-Americana de Internet (ALAI) considera importantes os seguintes pontos: ¿ Controladores não devem ser responsáveis por estabelecer bases legais para o tratamento de dados que resultam de menores burlando seus mecanismos de verificação de idade. Considerando que, como dito acima, não há mecanismo de verificação de idade infalível, falhas inevitavelmente ocorrerão. Quando crianças e adolescentes conseguem burlar mecanismos de verificação de idade durante o cadastro em plataformas, é importante que a ANPD determine que não há responsabilidade do controlador em determinar uma base legal apropriada para o tratamento

desses dados pessoais coletados de forma equivocada. ¿ Elaboração de RIPD e de identificação de tratamentos de dados pessoais de alto risco: É necessário que a autoridade se manifeste com relação a requisitos para a elaboração de RIPD e de identificação de tratamentos de dados pessoais de alto risco, tendo em vista que a existência de dados pessoais de crianças e adolescentes é considerada como critério a ser levado em consideração para a aplicação desses requisitos. ¿ Crítica ao critério de alto risco: o estabelecimento de dados pessoais de crianças e adolescentes como um critério de alto risco traz possíveis consequências negativas e ineficiências. Por exemplo, a contaminação de outros tratamentos de dados que poderiam ser inadvertidamente classificados como de alto risco. ¿ : Tratamento de dados para fins de Regulamentação específica para publicidade: Reforça-se a necessidade da ANPD reconhecer a legitimidade do tratamento de dados pessoais de crianças e adolescentes para fins de publicidade, sugerindo a criação de um guia específico que considere a maturidade progressiva do adolescente e diferencie entre publicidade personalizada e não personalizada. ¿ Esclarecimentos sobre controles de escolha: Necessidade de esclarecimentos sobre parâmetros gerais para o formato de centrais de controle das escolhas dos usuários, especialmente quando direcionados para crianças e adolescentes, levando em conta as diferentes tecnologias disponíveis e naturezas e propósitos distintos de diferentes serviços e produtos.

Contribuinte: Wanessa Larissa Silva de Araújo

Número: OP-753096

Data: 16/08/2024 - 14:33

Resumo: :"[TIM S.A.]: Reconhecemos que o Enunciado CD/ANPD Nº 1, de 2023 já regulamentou o aspecto mais crucial sobre a temática. Em qualquer medida, qualquer questão ou exemplo a serem apresentados pela ANPD, devem ser fornecidos apenas de maneira ilustrativa e não exaustiva, para que não engesse as operações executadas pelos agentes de tratamento principalmente considerando o mercado tão diversos e complexo quanto o brasileiro. Além disso, deve-se observar e respeitar o que já está previsto no Estatuto da Criança e do Adolescente, no que diz respeito aos direitos e deveres perante o grupo de titulares afetados.","708725":"Sem considerações.","705523":"[TIM S.A.]: Para garantir a coleta adequada de consentimento, é fundamental observar e respeitar as particularidades sociais do país sendo necessário considerar inclusive a limitação de acesso à educação e à informação. Muitos cidadãos podem não ter pleno entendimento sobre a importância da privacidade e da proteção de dados, o que exige uma abordagem clara e acessível na comunicação sobre esse tema. O aculturamento da população em relação à privacidade contribui para que tema dessa complexidade seja compreensível para todos, independentemente do nível de familiaridade com o assunto, sendo importante que a linguagem utilizada seja adequada de modo que seja simples e direto, evitando jargões técnicos que possam confundir os titulares dos dados. Por fim, é essencial que os processos de coleta de consentimento sejam inclusivos e respeitem a diversidade de mercados e contextos práticos no Brasil. Isso pode envolver a adaptação das práticas de coleta de

consentimento, garantindo que o controle parental seja efetivo.","708742":"[TIM S.A.]: É importante esclarecer que para a adoção dos esforços razoáveis, deve ser considerado pela ANPD, dentre outras questões as especifidades e complexidades das operações para empresas, especialmente aquelas que possuem operações que envolvem diversos departamentos, sistemas e processos. Implementar mudanças ou novas medidas de segurança pode exigir coordenação e integração entre várias áreas. Além disso necessário considerar que as empresas possuem recursos limitados, mesmo as grandes empresas, sejam financeiros, humanos ou tecnológicos. Alocar recursos para cumprir novos requisitos pode significar desviar esforços de outras áreas mais críticas, sem contar na evolução tecnológica e o que é considerado um método razoável hoje pode não ser amanhã. Em qualquer medida, entendemos que a responsabilidade pelo uso seguro e adequado da internet por crianças e adolescentes recai, primeiramente, sobre os pais e responsáveis legais. É fundamental que esses adultos compreendam que o controle parental é uma obrigação intransferível e deve ser exercido com diligência e atenção, isso inclui a supervisão das atividades online, a orientação sobre os riscos e a promoção de um comportamento responsável e seguro no ambiente digital. Embora os agentes de tratamento de dados desempenhem um papel importante na proteção da privacidade e segurança das informações dos menores, sua atuação é complementar. Os agentes de tratamento podem fornecer ferramentas e recursos para ajudar na supervisão, mas não podem substituir a presença e a orientação ativa dos adultos responsáveis. A colaboração entre os responsáveis legais e os agentes de tratamento é crucial para criar um ambiente digital seguro e saudável para crianças e adolescentes.","708745":"[TIM S.A.]: Entendemos que deve ser observado em qualquer medida o ECA, no que diz respeito a balização da idade e sempre em consonância com o princípio do melhor interesse, é possível ser dada a autonomia progressiva ao titular maior de 12 anos, para que o mesmo, em determinados contextos, possa fornecer seu consentimento.","705539":"Sem considerações.","708762":"Sem considerações.","708764":"[TIM S.A.]: Entendemos que as práticas de coleta e tratamento de dados devem estar em conformidade com o ECA, que estabelece direitos e garantias fundamentais para crianças e adolescentes no Brasil. Isso inclui a proteção contra exploração e abuso, bem como a garantia de privacidade e segurança. Ao observar essas limitações, as plataformas digitais podem garantir que a coleta e o tratamento de dados pessoais de crianças e adolescentes sejam realizados de maneira ética, segura e em conformidade com a legislação brasileira.","708768":"Sem considerações.","708772":"[TIM S.A.]: Apesar de não haver uma única forma ou método para garantir a devida transparência, inclusive considerando o cenários brasileiro e limitação de recursos de todos os aspectos nas empresas e, que isso deve ser considerado pela ANPD que os titulares devem ser tratados de maneira isonômica, contudo, considerado o público objeto da consulta, a linguagem precisaria ser mais simplificada e adequada. ","708775":"Sem considerações.

Contribuinte: ANA CLARA ARAUJO MAIA

Número: OP-753101

Data: 16/08/2024 - 14:51

Resumo: :".","708725":".","705523":"O artigo 14, §6º da LGPD é nítido quanto a exposição de dos critérios de informação do tratamento de dados, são eles "[...] maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado [...]", assim, estes elementos devem ser respeitados como condicionante para o reconhecimento do consentimento ao tratamento de dados de crianças e adolescentes. Além deste, reforça-se como parâmetro critérios mínimos de análise sobre a necessidade e co-relação com o serviço prestado. Isto é, não subsiste interesse no manuseio dados sobre altura, peso, idade e medidas de uma criança/adolescente para um serviço relacionado a jogos, por exemplo. É preciso que o balizamento do melhor interesse da criança/adolescente seja visualizado em consonância com estes dois critérios. [Contribuição elaborada pelo Instituto de Referência em Internet e Sociedade]","708742":".","708745":"A legislação no Brasil não segue a classificação universal da Convenção dos Direitos da Criança, em que crianças são todas as pessoas de 0 a 18 anos de idade. De acordo com o art. 2º do ECA, criança é "a pessoa até doze anos de idade incompletos", e adolescente é "aquela entre doze e dezoito anos de idade". Assim, a própria regra legal da LGPD se mostra alinhada com a autonomia progressiva, ao estabelecer regras distintas para o tratamento de dados pessoais de crianças e de adolescentes, com exigências mais rigorosas apenas para crianças, nos termos dos parágrafos do art. 14, que não se referem a adolescentes. Portanto, pode-se afirmar que o princípio do melhor interesse está diretamente relacionado ao princípio da autonomia progressiva, não subsistindo melhor interesse que não amplie as capacidades de adolescentes, por exemplo, para manifestar o próprio consentimento com o tratamento de dados pessoais, desde que respeitados e devidamente aplicados os demais princípios normativos pertinentes. Em todo caso, tal consentimento poderia ser revogado pela pessoa legalmente responsável, à luz da sua capacidade civil relativa, prevista do art. 4º, I, do Código Civil, devendo haver gradação distintiva entre adolescentes de 12 a 16 anos, e aqueles de 16 a 18. É preciso destacar ainda que, seguindo os preceitos legais do art. 14, §6º da LGPD, as informações referentes ao tratamento de dados de crianças e adolescentes precisam seguir alguns elementos de acessibilidade, nitidez, simplicidade, e considerar as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais da pessoa usuária. De modo que a ausência ou desrespeito destes elementos ensejaria em uma obstaculização ao exercício pleno da autonomia do adolescente, fato inclusive destacado no Guia Orientativo da ANPD sobre Legítimo Interesse. [Contribuição elaborada pelo Instituto de Referência em Internet e Sociedade] ","705539":".","708762":"As plataformas digitais não devem encarar a verificação de idade apenas como um meio formal para sua isenção de responsabilidade, mas como um instrumento necessário para a efetivação da proteção integral de crianças e adolescentes. O controle de acesso às aplicações online deve operar mediante ferramentas de autenticação e certificação confiáveis, com tecnologia em constante atualização. Ao mesmo tempo, devem ter o cuidado de não permitir que tal instrumento se converta em mecanismo de vigilância, fragilizando garantias jurídicas e liberdades de crianças e adolescentes. Destaca-se, ainda, que as boas práticas para verificação de idade de usuários não deve ser utilizada como estratégia para captação e manuseio de novos dados, como, por exemplo, a exigência da apresentação de documentos públicos, como o Registro Geral, e seu posterior arquivamento na plataforma

para utilização dos dados ali presentes para perfilamento comercial. Assim, não deve haver vinculação entre a prévia verificação de idade e o posterior tratamento de dados pessoais, de modo que não se viabilize o monitoramento desproporcional das comunicações online ou das informações acessadas durante o uso das plataformas digitais. [Contribuição elaborada pelo Instituto de Referência em Internet e Sociedade]","708764":".","708768":"Em sua condição peculiar de pessoa em desenvolvimento, crianças e adolescentes têm direito a receber a prestação de assistência material, moral e educacional por parte de seus responsáveis. Assim, a supervisão pela família é inerente à proteção integral e ao melhor interesse da criança e do adolescente, servindo como preparação para convivência social e o pleno exercício dos direitos de que é titular. Portanto, o controle de pais e responsáveis não deve ser visto como subterfúgio, e sim como uma garantia em favor das crianças e adolescentes. Logo, por nenhuma razão deve haver qualquer desenho de portas clandestinas para acesso ao banco de dados pessoais. Caso seja adequado que responsáveis tenham acesso aos dados armazenados, incluindo pais ou educadores, esse mecanismo deve ser previsto e implementado de modo aberto e transparente, sem qualquer ocultação ou dissimulação na informação para crianças e adolescentes. Ademais, o reconhecimento da autonomia progressiva infantojuvenil e da sua posição como cidadãos, em contraste com a antiga condição de assujeitamento prevista no Código de Menores dos anos 70, proporciona novas perspectivas para a proteção de crianças e adolescentes, distinguindo claramente o cuidado do mero monitoramento. Assim, as boas práticas na proteção de dados de crianças e adolescentes, em diálogo com seus pais e responsáveis, devem considerar as características da “mediação parental”. Nesse contexto, o adulto responsável não é mais visto como o “detentor” direto da criança ou adolescente, mas sim como um promotor de seus direitos. Dessa forma, as decisões sobre o tratamento de dados infantojuvenis devem ser orientadas não apenas pela concordância dos pais ou responsáveis, mas também pelo melhor interesse da criança e do adolescente envolvidos. [Contribuição elaborada pelo Instituto de Referência em Internet e Sociedade] ","708772":"As plataformas que tenham suas finalidades voltadas ao público infantojuvenil podem e devem articular, a partir do art. 14, §6º da LGPD, modelos distintos do tradicional, para apresentação de seus termos de uso, especialmente dos que dizem respeito ao manuseio de dados. Assim, em termos de boas práticas, deve ser incentivada a adoção de medidas que simplifiquem a linguagem a partir de materiais visuais, e/ou de audiovisual, inclusive animações, que tenham a ver com o contexto da plataforma, e adotem medidas de apresentação dos termos de uso em linguagem acessível. Menciona-se, a título de boas práticas, a possibilidade de utilização de quadrinhos, animes, animações de jogos, dentre outras técnicas lúdicas para apresentar os termos de manuseio dos dados de serviços de tratamento de dados. Essas práticas fortalecem, inclusive, o caráter de autonomia progressiva de crianças e adolescentes, bem como, os preceitos do letramento digital, instigado pelo Marco Civil da Internet. [Contribuição elaborada pelo Instituto de Referência em Internet e Sociedade] ","708775":".

Contribuinte: ANA BARBARA GOMES PEREIRA

Número: OP-753116

Data: 16/08/2024 - 15:20

Resumo: :"Venho, em nome da Associação Brasileira de Planos de Saúde - ABRAMGE e da Associação Brasileira de Planos Odontológicos - SINOG, na figura de sua Advogada e Encarregada de Proteção de Dados, parabenizar esta autoridade pela condução do tema por intermédio de Tomada de Subsídios, possibilitando à sociedade a participação na construção e maturação da cultura de proteção de dados no Brasil, e também pela importância dada ao tema, a ponto de deliberarem pela aprovação de concessão de prazo adicional para participação social. Primeiramente, cabe mencionar que o setor de saúde e odontologia suplementares, especialmente as associadas das entidades ABRAMGE e SINOG, acompanha de perto as atividades desta autoridade, sempre que possível contribuindo com as participações sociais propostas pela ANPD, com a ajuda das construções advindas de Grupo de Trabalho sobre Privacidade e Proteção de Dados. Deste modo, aproveitamos a oportunidade concedida para destacar os principais pontos de preocupação deste setor em relação ao assunto em referência, com foco nas necessidades da operação junto aos titulares de dados pessoais, conforme expomos a seguir. Tendo em vista que o Enunciado autoriza que o tratamento de dados pessoais de crianças e adolescentes seja realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, há a necessidade de tonar a redação clara sobre a aplicabilidade de umas das hipóteses legais previstas nos referidos artigos, além de tornar mais clara também o melhor interesse do titular nessas hipóteses. Com relação ao artigo 14, poderia ser excluído, por consequência, a autorização (consentimento) de um dos pais ou responsável legal, como ocorre com os demais tratamentos de dados quando cabe uma das hipóteses legais, com a observância em todos os casos do melhor interesse da criança. Ainda, com relação ao melhor interesse da criança, cabe à ANPD tonar os critérios mais objetivos ou fazer referência ao que já constam na própria legislação pátria, como os direitos constitucionais, direitos previstos no ECA e demais normas relacionadas existentes e aplicáveis a cada caso concreto. Além disso, no que tange a jogos de azar, apostas e jogos eletrônicos no geral (com compras dentro do próprio jogo); publicidade, marketing e personalização; inteligência artificial, sendo este rol não taxativo, há a necessidade de uma regulamentação específica. ","708725":"Sim, embora jogos de azar sejam proibidos para menores de idade, os bloqueios não são recorrentes e eficientes. A Lei nº 14.852/2024, que cria o marco legal para a indústria de jogos eletrônicos, menciona em seu capítulo III a proteção das crianças e dos adolescentes. Há a promoção de sistemas mínimos de salvaguardas aos direitos e restrição a transações comerciais, porém, não há manual prático no que tange a proteção de dados destes menores. Sobre publicidade, marketing e personalização, embora existam resoluções do Conselho Nacional de Autorregulamentação Publicitária (Conar), do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda), dentre outros, entende-se por orientação de boas práticas e supervisão pela ANPD. Há de se dar especial atenção também, as situações em que há tratamento de categorias de dados de crianças e adolescentes em grande escala ou sem finalidade determinada (em excesso), por ser considerado alto risco, considerando cada tipo de tratamento de dado envolvendo alta escala de dados do mesmo indivíduo (criança/adolescente) e em cada caso concreto, não considerando a operação do agente de tratamento em si. Em relação à inteligência artificial, deve-se aguardar o Projeto de Lei nº

2.338/2023 para eventual futura regulamentação por parte da ANPD. ","705523":"Para que o consentimento seja específico e em destaque, antes do aceite, deve ser explicado cada ponto do termo. Se em aplicativo, pode ser acompanhado através de áudio de leitura, o termo deve ser completo na tela, de fácil escrita e contendo exemplos e demais informações pertinentes, sem se apegar ao "juridiquês", outras possibilidades seriam o consentimento conter os dados mínimos da criança e do autorizador e ocorrer a validação por token ou login/senha, ou ainda de forma manual, através documento privado, e não necessariamente público, assinado pelo representante com o seu reconhecimento de firma. Caso não seja cliente, deve ser realizado contato telefônico e/ou fornecido token para validação pelo responsável legal. ","708742":"Considerando as boas práticas, a forma mais prática e célere de viabilizar o consentimento dos pais seria através de biometria facial. A biometria deve ser validada através do envio de cópia de documento que comprove o relacionamento parental, por exemplo, a identidade do responsável e do menor, a certidão de nascimento com a indicação dos pais ou certidão judicial, com a indicação do tutor. Caso o pai/responsável legal já tenha relação jurídica com a empresa, basta a indicação da informação, sem a apresentação de documentos adicionais. ","708745":"O consentimento previsto na LGPD (artigo 14) faz referência apenas a dados pessoais de crianças, ou seja, até 12 anos incompletos (ECA). Para os adolescentes, de acordo com a LGPD, tal consentimento não se faz obrigatório, o que deve ser descartado. Entretanto, não podemos confundir a autorização de pais e responsáveis considerando as regras gerais aplicáveis no ordenamento jurídico para os atos da vida civil, disponíveis no Código Civil. Tais regramentos são aplicáveis para as pessoas com idade inferior a 18 anos, que possuem a capacidade civil reduzida para os atos da vida civil, o que inclui relacionamento jurídico/negocial desta pessoa natural com uma empresa jurídica em ambiente digital, que pode ter por via transversa o tratamento de dados. O artigo 5º do Código Civil traz, em seu parágrafo único, as possibilidades, para o menor, de ser cessada a incapacidade. Entende-se que, embora a previsão legal para cessar a incapacidade, os direitos daquele adolescente continuam protegidos pelo ECA, bem como a proteção ao melhor interesse. E, neste sentido, a proteção à privacidade e aos seus dados continuará vigorando de forma mais protetiva. Apesar disso, como forma de viabilizar o consentimento – seja aceite, seja recusa – se faz necessário entender a realidade fática para que seja gerada a exceção. Nos casos, por exemplo, da concessão pelos pais ou do casamento (incisos I e II, art. 5º, CC), é possível que a pessoa, agora capaz, não esteja geograficamente próxima de seu outrora responsável legal. Portanto, obrigar a manter o consentimento dado pelos pais pode inviabilizar um consentimento que, se dado, pode ser favorável àquela pessoa e inferir em outras proteções e direitos elencados no ECA. Neste sentido, um estudo específico poderá ser realizado. ","705539":"Devem ser observados os princípios relacionados a respeito à segurança; direitos individuais; qualidade dos dados; transparência; coleta, uso e retenção; compartilhamento e transferências internacionais seguras; responsabilização e prestação de contas. Análise da ferramenta por parte de T.I., arquitetura de dados, engenharia de segurança da informação, governança de dados e obrigatoriedade de manutenção dos documentos de homologação por período de vigência do contrato + 5 anos após rescisão contratual. Além disto, avaliação de cláusulas contratuais e análises de risco vinculadas ao mapeamento de dados. Todos os documentos poderão ser solicitados para análise da ANPD. Em resumo, as

plataformas digitais voltadas exclusivamente para o público em referência poderão conter termos de uso e políticas redigidas de forma clara e didática, a fim de orientar o usuário da plataforma sobre os princípios que estão sendo atendidos, direitos que podem ser exercidos e as respectivas medidas e salvaguardas. ","708762":"Para que seja realmente verificada a validade das informações, existem duas opções: consulta da data de nascimento, nome e CPF (para diferenciação de homônimo) em banco de dados legítimo e legal; ou, caso a consulta seja feita na hora, entende-se que a cópia do documento oficial (registro geral) se faz necessária, a fim de confirmar a validade daquele documento.","708764":"O artigo supramencionado refere-se à obtenção de informações pessoais estritamente necessárias de crianças e adolescentes. Caso a ferramenta apresente conteúdo sensível, que pode ser restringido, entende-se que pode ser feito através de consulta da data de nascimento, nome e CPF (para diferenciação de homônimo) em banco de dados legítimo e legal; ou, caso a consulta seja feita na hora, entende-se que a cópia do documento oficial (registro geral) se faz necessária, a fim de confirmar a validade daquele documento. O ponto de atenção se encontra na foto encontrada no documento oficial, que pode traçar perfil de raça/etnia e deve ser estudado. Todavia, dados sobre geolocalização, cadastro de consumo, dados sensíveis no geral (exceto PCDs para acessibilidade da ferramenta) não devem ser informados. Caso não existam informações a serem restringidas a um público geral, solicitar somente informações básicas para cadastro e recuperação de senha (nome, login, senha, duplo fator de autenticação). As limitações devem se ater às que já estão previstas na Lei, como a atenção aos princípios. ","708768":"As ferramentas podem disponibilizar, a cada período estabelecido (ex. 2x semana em data programada) informações voltadas aos pais, que devem ler e confirmar leitura. Podem ser informações sobre quantidade de uso (número de horas), algum comportamento supostamente indevido da criança/adolescente, ou mesmo dicas práticas (educacionais) de segurança como não registrar a mesma senha para diversas plataformas. Outra opção é o usuário sendo um cliente, recomenda-se o envio de uma notificação por e-mail (ou outro canal digital disponível) para o pai ou responsável legal cadastrado. Quando não for um cliente, deve ser informado pelo usuário em seu acesso. ","708772":"Texto didático e claro em seus termos de uso e política de privacidade, redação de maneira simples, clara e acessível, inclusive com uso de recursos audiovisuais, para fornecer informações necessárias aos pais ou ao responsável legal e para possibilitar o adequado entendimento da criança e do adolescente sobre as informações disponibilizadas, podendo inclusive, solicitar que a cada período estabelecido (ex. 2x semana em data programada) os pais leiam e confirmem a leitura. O texto deve ser curto, interativo, deve contar com opção de áudio de leitura (áudio para acompanhamento do texto), vídeos podem ser apresentados e após finalização do conteúdo abrir um chat para perguntas e respostas.","708775":"Sim, para que novas regulamentações sejam implementadas, por exemplo, código de design voltado especificamente para crianças e adolescentes, estas crianças e adolescentes devem ser voz ativa. Deve-se ouvi-los com intuito de compreender a realidade fática de como a tecnologia tem influenciado suas vidas. Neste sentido há a Convenção sobre os Direitos da Criança da ONU (1989) e o Comentário Geral 25 do Comitê dos Direitos da Criança da ONU (2021). Além disso é importante, a promoção do pensamento crítico sobre o tratamento de dados

pessoais entre crianças e os adolescentes pelo Estado por meio de conscientização em escolas e políticas públicas.

Contribuinte: Camila Castioni Secundino

Número: OP-753118

Data: 16/08/2024 - 15:21

Resumo: :"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Maiores esclarecimentos e/ou framework sobre os parâmetros a serem considerados pelos agentes de tratamento para identificar o melhor interesse das crianças e dos adolescentes, com maior objetividade em relação aos três aspectos: um direito, um princípio interpretativo e uma regra processual.","708725":"N/A.","705523":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Consentimento granular ou habilitador de categoria de atividades de tratamentos de dados com finalidades correlatas; Garantia de autogestão pelos pais ou responsáveis legais da régua de consentimento da criança ou adolescente; Ponto de Atenção: Legitimidade em casos de perda da autoridade parental. ","708742":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Implementar processo automatizado para confirmação de filiação, por ex., via receita e/ou outros órgãos reconhecidos; Comprovação documental no cadastro da criança; Coleta via SMS ou e-mail dos pais ou responsáveis legais, quando já houver vinculo validado no cadastro da criaça.","708745":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Seguir as disposições do direito civil implicaria em garantir a coleta do consentimento do adolescente maior de 16 anos (relativamente incapaz) desde que assistido. Neste aspecto, além do consentimeto do adolescente, precisaria ser compovada a anuência dos pais ou responsável legal; Considerar a autônomia progressiva pode implicar em riscos pela falta de obetividade (recorte por idade); Se o tratamento de dados de um titular entre 12 e 16 anos ocorrer com base no consentimento dado diretamente por ele, é passível de questionamentos sobre a sua validade; Em específico, no âmbito da saúde, além das questões relacionadas a capacidade civil, necessário levar em conta, também, a capacidade de discernimento, conforme CFM; Assim, independentemente do modelo adotado, necessário direcionamento específico da ANPD sobre o tema.","705539":"N/A","708762":"N/A","708764":"N/A","708768":"N/A","708772":"N/A","708775":"N/A

Contribuinte: Teresa de Souza Dias Gutierrez

Número: OP-753125

Data: 16/08/2024 - 15:32

Resumo: :"O melhor interesse do titular menor deve ser avaliado e registrado para todo e qualquer tratamento e não apenas os tratamentos com a base legal de legítimo interesse. Na

prática atual, controlador só é obrigado a realizar o balanceamento do melhor interesse do titular melhor quando está realizando ponderando sobre a viabilidade do seu interesse próprio no teste de balanceamento. Por consequência, tratamentos com bases distintas do legítimo interesse não incentivam o controlador a efetivamente ponderar sobre a necessidade e viabilidade daquele tratamento, fato que pode acabar reprimindo o melhor interesse do menor em face da ação do controlador. Para contornar esse cenário, o controlador deveria realizar testes de balanceamento para qualquer tratamento que lide com titulares menores de idade, sempre buscando avaliar se o melhor interesse, previsto no art. 14 da LGPD, está sendo observado. Essa noção já é adotada na Europa, com destaque para o Reino Unido, que já disponibilizou o Best Interests Of The Child Self-Assessment, documento que visa justamente avaliar se o melhor interesse do titular menor é efetivamente observado pelo Controlador. ","708725":"Sim, as relações de consumo digital. Quando tratamos do ambiente on-line, é necessário ter em mente que a sociedade de consumo é voltada para atrair a atenção de crianças, dada a gigantesca influência que estas têm pelos seus pais e responsáveis. Em virtude da falta de idade, maturidade e experiência, o contato prolongado com o ambiente digital, criado para efetivar e explorar consumos, resulta em: (i) dificuldade para desenvolver a capacidade de lidar com frustrações; (ii) agravamento da autoestima; e (iii) impulsionamento da adultização e erotização precoce. Ademais, por estarem em fase de socialização, crianças raramente são aptas para distinguir o público do privado. Assim, se preocupam mais em fortalecer status de popularidade do que com a segurança de dados. Ao expor seus dados corriqueiramente na internet, crianças acabam por se tornar alvos mais fácies para golpes, além de que os dados podem ser utilizados sem solicitação de consentimento para uso publicitário. Somado a isso, é preciso ressaltar que crianças no ambiente digital sofrem a chamada tripla vulnerabilidade, pois são consideradas pessoas em desenvolvimento (art. 6º do ECA) que realizam relações de consumo em um ambiente de difícil monitoramento pelos seus responsáveis. Essa realidade acaba por criar um cenário em que o princípio do melhor interesse pode, muito facilmente, ser ignorado em face de questões comerciais ou de interesse privado. Por conclusão, é fundamental que os ambientes online mais visitados (redes sociais, servidores de jogos, sites de pesquisa etc...) por menores sejam constantemente monitorados para verificar se os tratamentos de dados respeitam o melhor interesse do menor. Por fim, a ANPD poderia incentivar a adoção de boas práticas para controladores que ofertamos serviços mencionados acima. Algumas recomendações de segurança que podem ser tomadas são: (i) metodologias para verificar idade constantemente, tendo em vista que crianças e adolescentes costumam mentir a idade para acessar serviços; (ii) desabilitar algoritmos, evitando recomendações perigosas; (iii) monitorar atividades de risco, como publicações que incentivem suicídio ou violência; (iv) bloqueio de tempo de uso e fim da rolagem infinita; e (v) políticas informativas pensadas para o público menor de idade. ","705523":"É necessário que para os casos de obtenção de consentimento de pais ou responsáveis legais, deve ser garantido (i) a relação entre a criança/adolescente e o pai/responsável, como forma de garantir que o verdadeiro responsável legal está fornecendo o consentimento, e não terceiros que não possuem relação com o menor titular de dados; (ii) que a coleta de consentimento seja feita para cada atividade de tratamento de dados informando os respectivos dados a serem tratados, e não de maneira

genérica para diversas atividades; possibilitando que os pais e responsáveis possam dar o consentimento específico para cada uma das finalidades; (iii) que o responsável seja informado sobre macroprocessos, que levam a processos menores e (iv) incluir aviso para conscientização sobre a sensibilidade do tratamento de dados de crianças, em virtude da sua posição de vulnerabilidade. ","708742":"Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de “todos os esforços razoáveis”, quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança? É importante que as medidas tomadas se assegurem de coletar o consentimento específico e em destaque. Para casos em que o consentimento terá que ser coletado no ambiente digital, há alguns mecanismos que podem ser adotados para obtenção desse consentimento, tais como: 1. Assinatura de formulário de consentimento e enviá-lo ao controlador; 2. Usar um cartão de crédito, cartão de débito ou outros sistemas de pagamento online que forneça a notificação de transação para o titular da conta; 3. Ligação para um número de telefone gratuito com pessoal treinado para obter o consentimento do responsável; 4. Ligação com pessoal treinado através de videoconferência; 5. Enviar cópia de documento de identificação; 6. Responder perguntas baseadas em conhecimentos difíceis para menores de idade; Tais mecanismos são opções variadas que podem se adequar de acordo com o contexto do tratamento de dados. ","708745":"No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais? Em consonância com os dispositivos do Código Civil, Estatuto da Criança e do Adolescente e a Lei Geral de Proteção de Dados, a legislação brasileira já prevê uma autonomia progressiva de crianças e adolescentes, vez que considera os menores de 12 anos absolutamente incapazes, aqueles entre 12 e 16 anos absolutamente incapazes, devendo ser representados por pais ou responsáveis legais, e aqueles entre 16 e 18 relativamente incapazes, devendo ser assistidos pelos pais ou responsáveis. Ressalta-se que a Lei Geral de Proteção de Dados já prevê autonomia ao titular ao falar no art. 14 que para o tratamento de dados pessoais de crianças deve ser coletado o consentimento, não fazendo menção à essa necessidade para dados pessoais de adolescentes. Tendo em vista já existir de maneira consolidada na legislação brasileira uma evolução etária para a tomada de decisões, não há razoabilidade que o consentimento seja expresso de maneira adversa, isso especialmente levando em conta o ambiente digital, que proporciona uma gama de informações e interações demasiadamente vasta, sendo prudente seguir com as disposições já existentes no ordenamento brasileiro, a fim de proteger crianças e adolescentes e, ainda sim, na medida do possível respeitar seus desejos e vontades. ","705539":"-","708762":"-","708764":"-","708768":"-","708772":"-","708775":"-

Contribuinte: GABRIELA CAROLINA DE ARAUJO

Número: OP-753128

Data: 16/08/2024 - 15:53

Resumo: :"Questões adicionais demandam orientação ou regulamentação específicas pela ANPD: 1. Definição e Aplicação Prática do Melhor Interesse: A ANPD poderia fornecer exemplos práticos detalhados que ajudem a interpretar o conceito de "melhor interesse" no contexto do tratamento de dados pessoais de crianças e adolescentes. Por exemplo, no caso de adolescentes que adquirem produtos e serviços de tecnologia, como os oferecidos pela Samsung, é importante que as empresas avaliem como o princípio do melhor interesse se aplica ao permitir que esses menores façam escolhas informadas e protegidas. A inclusão de casos práticos pode auxiliar tanto os controladores de dados quanto os pais a entenderem melhor como aplicar esse princípio em situações concretas. 2. Diferenciação entre Crianças e Adolescentes: É necessário distinguir entre o melhor interesse de crianças e de adolescentes, considerando suas especificidades e níveis de maturidade. Adolescentes, especialmente a partir dos 16 anos, possuem relativa capacidade para exercer certos atos da vida civil (conforme o art. 4º do Código Civil). 3. Avaliação de Impacto e Justificação de Decisões: A ANPD poderia estabelecer diretrizes mais claras sobre como conduzir avaliações de impacto no tratamento de dados que envolvam crianças e adolescentes, garantindo que seus melhores interesses sejam considerados de forma primária. Além disso, deve ser exigida uma justificativa detalhada das decisões tomadas, demonstrando explicitamente como o melhor interesse foi considerado e quais critérios foram utilizados nessa análise. 4. Proteção contra Superexposição e Exploração Comercial: Embora a proteção contra a superexposição e exploração comercial seja relevante, é importante que a regulamentação busque um equilíbrio entre a proteção dos menores e a viabilidade das práticas de publicidade e marketing voltadas para adolescentes. A ANPD poderia considerar diretrizes que protejam os menores, sem inviabilizar a comunicação de produtos e serviços que possam ser de interesse e benefício para esse público. 5. Orientações sobre Consentimento e Autonomia Digital: A ANPD deve fornecer orientações claras sobre o consentimento informado no contexto digital, considerando a maturidade e a capacidade de compreensão das crianças e adolescentes. Além disso, é importante equilibrar o melhor interesse do menor de idade com o envolvimento do responsável e o modelo de negócio das empresas, de forma que as práticas comerciais sejam adaptadas à necessidade de proteção do público jovem. 6. Educação Digital e Envolvimento dos Pais: É essencial que a ANPD promova a educação digital tanto para crianças quanto para os pais, fornecendo recursos e ferramentas que auxiliem na navegação segura e responsável no ambiente digital. Os pais devem ser capacitados para apoiar e orientar seus filhos de forma eficaz. 7. Design Ético de Interfaces Digitais: Embora seja importante que as interfaces digitais sejam intuitivas e adequadas para crianças e adolescentes, é necessário considerar as limitações das empresas em garantir a plena compreensão dos menores. A ANPD poderia recomendar boas práticas de design, sem impor a responsabilidade exclusiva sobre as empresas, reconhecendo que a compreensão do conteúdo é um desafio que depende de vários fatores, incluindo o contexto educacional e familiar do menor. 8. Controles Parentais que Respeitem a Privacidade e o Melhor Interesse da Criança: É fundamental que

os controles parentais sejam projetados para apoiar e guiar as crianças, sem serem excessivamente invasivos. No entanto, o mérito de determinar o nível adequado de vigilância deve ser responsabilidade dos pais, que melhor conhecem as necessidades e o contexto de seus filhos. A ANPD pode fornecer orientações gerais sobre boas práticas, mas sem entrar no mérito específico de como cada família deve gerenciar a privacidade e a supervisão dos menores. 9. Equilíbrio entre o tratamento de dados de adolescentes e fabricantes: A ANPD deve fornecer exemplos e diretrizes sobre o tratamento de dados de adolescentes pelos fabricantes de software e hardware, considerando que, em muitos casos, adolescentes já possuem recursos próprios para adquirirem produtos ","708725":"Existem contextos específicos no tratamento de dados pessoais de crianças e adolescentes que requerem maior atenção em relação ao princípio do melhor interesse: 1. Marketing Personalizado e Venda de Produtos e Serviços: • Principais Questões: Coleta de dados para a personalização de ofertas e produtos voltados para crianças e adolescentes, riscos de influenciar comportamentos de consumo sem consentimento informado adequado, e a necessidade de proteger os menores de publicidade excessiva ou inapropriada. • Medidas Necessárias: Regulamentações que assegurem que a coleta de dados para fins de marketing seja realizada de forma ética, com transparência e consentimento adequado. As empresas devem ser incentivadas a desenvolver políticas que equilibrem o interesse comercial com a proteção dos menores, garantindo que a personalização de marketing respeite o princípio do melhor interesse. 2. Ações e Campanhas Voltadas para a Geração Z: • Principais Questões: Coleta de dados em eventos e feiras de tecnologia, como aquelas voltadas para gamers, onde a participação de menores é significativa. É necessário garantir que os dados coletados sejam protegidos e que os menores estejam cientes dos riscos envolvidos na exposição de suas informações pessoais. • Medidas Necessárias: Desenvolvimento de políticas de coleta de dados específicas para eventos direcionados ao público jovem, com foco na transparência e no consentimento informado. É crucial que as empresas adotem práticas que minimizem a coleta de dados sensíveis e garantam a proteção dos menores participantes. 3. Programas Educacionais e Incentivos: • Principais Questões: Participação de menores em programas como o Solve for Tomorrow, Samsung Innovation Campus e o Programa Ocean, que acontecem nas fábricas para fins educacionais. Além disso, programas de incentivos aos vendedores de parceiros comerciais, que podem incluir jovens aprendizes. • Medidas Necessárias: Criação de diretrizes claras que orientem o tratamento de dados em contextos educacionais e profissionais, assegurando que os dados dos menores sejam utilizados exclusivamente para fins legítimos e que estejam protegidos contra o uso indevido. 4. Controles Parentais em Produtos Tecnológicos: • Principais Questões: Implementação de controles parentais em dispositivos tecnológicos, garantindo que as ferramentas oferecidas sejam eficazes e respeitem a privacidade dos menores. • Medidas Necessárias: A ANPD poderia destacar a importância de ferramentas de controle parental como as implementadas em produtos da Samsung, que permitem que os pais monitorem e gerenciem o uso de dispositivos por seus filhos de maneira equilibrada, promovendo um ambiente digital seguro e respeitoso. Conclusão Para garantir a proteção dos dados pessoais de crianças e adolescentes de maneira que respeite o princípio do melhor interesse, é crucial desenvolver regulamentações e políticas públicas que abordem de forma específica os

desafios apresentados pelo ambiente digital. Isso inclui promover a transparência na coleta e uso de dados em ações de marketing e programas educacionais, assegurar que as ferramentas de controle parental sejam eficazes e equilibradas, e garantir que os dados sejam tratados de maneira ética e segura. ","705523":"Para garantir que esse consentimento seja válido e adequado, é necessário observar certos critérios e parâmetros, conforme detalhado abaixo: 1. Clareza e Transparência das Informações: o Linguagem Acessível: As informações sobre como os dados serão tratados devem ser apresentadas em uma linguagem clara e compreensível para a criança e responsáveis. Se o consentimento deve ser dado pelos pais, as informações devem ser suficientemente detalhadas para que os adultos possam tomar uma decisão informada. o Destaque das Informações Relevantes: O consentimento deve ser "específico e em destaque", o que implica que as informações sobre a coleta e uso de dados pessoais devem ser apresentadas de forma proeminente e não escondidas em termos de serviço e/ou textos legais longos e complexos. 2. Verificação de Identidade dos Pais ou Responsáveis: o Esforços Razoáveis: Os controladores devem fazer "todos os esforços razoáveis" para verificar que o consentimento foi realmente fornecido pelos pais ou responsáveis legais, considerando as tecnologias disponíveis. Isso pode incluir o envio de e-mails de verificação em casos de baixo risco ou a solicitação de provas adicionais em situações de alto risco. A ANPD pode fornecer exemplos práticos de tecnologias que cumprem esse propósito. 3. Equilíbrio de Poder e Liberdade de Consentimento: o Interesses da Criança: O consentimento não deve ser aceito se for evidente que ele é contrário ao melhor interesse da criança. Isso inclui situações em que a obtenção do consentimento dos pais seria prejudicial à criança. A ANPD pode fornecer exemplos práticos de tratamentos que não atendam este princípio, conforme apresentados nos itens anteriores. Implementação Prática e Recomendações Para a implementação prática desses critérios, a CNIL sugere algumas medidas: • Comunicação Eficaz: Desenvolver materiais educativos e informativos que expliquem claramente o processo de consentimento tanto para crianças quanto para pais. Isso pode incluir vídeos, infográficos e FAQs em plataformas digitais. Embora essa responsabilidade seja principalmente da ANPD, as empresas também podem colaborar com informações claras e acessíveis em suas plataformas. • Tecnologia Adequada: Utilizar tecnologias que facilitem a verificação de identidade e a coleta de consentimento, cujos parâmetros e requisitos dessas tecnologias deverão ser fornecidos pela ANPD, garantindo que esses processos sejam seguros e eficientes. • Educação e Sensibilização: Embora a promoção de programas de educação digital seja uma responsabilidade principal da ANPD, as empresas podem contribuir oferecendo recursos que auxiliem os pais e responsáveis a entenderem a importância do consentimento informado e como ele é aplicado no contexto dos produtos e serviços oferecidos.. Ao seguir esses critérios e recomendações, o CNIL indica que os controladores podem assegurar que o consentimento "específico e em destaque" seja obtido de maneira eficaz e em conformidade com a LGPD, protegendo os dados pessoais de crianças e adolescentes e respeitando seu melhor interesse. ","708742":"Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, especialmente os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", os controladores de dados devem adotar uma série de medidas e mecanismos para assegurar que o consentimento foi

devidamente fornecido pelos pais ou responsáveis legais de crianças no ambiente digital. As seguintes estratégias, baseadas nas recomendações da CNIL e do EDPB, são particularmente eficazes: 1. Verificação da Identidade e Autenticidade do Consentimento • Tecnologias de Verificação de Idade: Implementar sistemas de verificação de idade para garantir que o usuário seja uma criança e, portanto, necessite do consentimento dos pais. Esses sistemas podem incluir a verificação por data de nascimento e mecanismos de detecção de fraudes. No entanto, é importante ressaltar que, em casos de falha na detecção de fraude, o controlador não deve ser responsabilizado, considerando a boa-fé na implementação dessas tecnologias. A ANPD poderia fornecer diretrizes sobre como essa responsabilidade deve ser tratada. •

Métodos de Verificação: Dependendo do nível de risco associado ao processamento de dados, diferentes métodos de verificação podem ser utilizados: o E-mail de Verificação: Para situações de baixo risco, um e-mail de verificação enviado aos pais pode ser considerado, embora haja limitações na verificação da autenticidade do e-mail. Neste caso, a teoria da aparência e a presunção de boa-fé podem ser aplicadas. o

Documentação de Suporte: Em casos de maior risco, solicitar documentos adicionais, como cópias de documentos de identidade dos pais, pode ser necessário. No entanto, é essencial que a ANPD estabeleça parâmetros claros para a utilização de tais métodos. o

Serviços de Verificação de Terceiros: Utilizar serviços de verificação de terceiros que possam autenticar a identidade dos pais ou responsáveis de forma segura e eficiente. A ANPD poderia definir quais tipos de ferramentas e serviços são considerados adequados para essa finalidade. 2. Procedimentos de Consentimento Duplo (Double Opt-In) •

Consentimento Duplo: Implementar um processo de consentimento duplo, onde os pais primeiro fornecem consentimento inicial e, em seguida, confirmam sua decisão através de um segundo passo de verificação, como a inserção de um código enviado por e-mail ou SMS. 3. Engajamento com as Crianças e os Pais Inclusão das Crianças nas Decisões: Embora seja importante respeitar a capacidade de compreensão e maturidade das crianças, a decisão final sobre o tratamento de dados deve ser considerada uma responsabilidade primária dos pais ou responsáveis. A participação das crianças deve ser incentivada dentro do contexto familiar, promovendo um diálogo aberto sobre privacidade e segurança digital. É importante ressaltar que nenhuma técnica será 100% eficaz, e os controladores devem atuar de boa-fé ao implementar essas técnicas para viabilizar e verificar o consentimento. A ANPD deve considerar a boa-fé do agente de tratamento em casos de falha e fornecer orientações claras sobre como os controladores podem se proteger contra possíveis responsabilidades, desde que tenham adotado “todos os esforços razoáveis. ","708745":"Princípio da Autonomia Progressiva O princípio da autonomia progressiva, qual foi introduzida ao ordenamento jurídico brasileiro pelo Decreto Nº 99.710/90, qual promulgou a Convenção Sobre os Direitos da Criança, possui ampla discussão conceitual e já reverbere em instrumentos normativos voltadas ao ambiente digital, como na Resolução Nº 245 do CONANDA. Sendo assim, mostra-se plenamente viável sua aplicação prática no contexto da LGPD. Este princípio, neste contexto, pode ser entendido como a previsão das capacidades e a autonomia dos adolescentes serem respeitadas e desenvolvidas gradativamente. Sob este, sugere-se que os adolescentes possam, em determinados contextos, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis,

desde que considerado o melhor interesse do adolescente, cuja definição deverá ser esclarecida pela ANPD. Diretrizes da CNIL e EDPB As diretrizes da CNIL e do EDPB oferecem uma estrutura prática para implementar o princípio da autonomia progressiva no contexto digital: 1. Verificação da Idade e Maturidade o Avaliação de Maturidade: O nível de maturidade do adolescente deve ser considerado. Por exemplo, um adolescente de 16 anos pode ter a capacidade de entender e consentir com o tratamento de seus dados de forma mais autônoma em comparação com um adolescente mais jovem. o Verificação de Idade: Utilizar tecnologias para verificar a idade do usuário, cujos parâmetros de utilização e desenvolvimento deverão ser exemplificados pela ANPD, garantindo que o consentimento seja apropriado para a faixa etária. 2. Consentimento Conjunto o Consentimento Conjunto: Em situações que demandem maior segurança, como para casos de crianças menores de dezesseis anos, pode ser implementado um sistema de consentimento conjunto, onde tanto o adolescente quanto os pais ou responsáveis legais fornecem consentimento. Isso garante que ambos estejam cientes e de acordo com o tratamento de dados. 3. Informação Clara e Acessível o Comunicação Transparente: Informações sobre o tratamento de dados devem ser apresentadas de forma clara e acessível. Isso inclui o uso de linguagem simples e direta. 4. Processos de Consentimento Dinâmico o Revisão Periódica de Consentimento: Estabelecer mecanismos para que o consentimento possa ser revisado e atualizado periodicamente, permitindo que adolescentes com idade entre dezesseis e dezoito anos possam assumir maior autonomia na gestão de seus dados. 5. Engajamento Ativo dos Adolescentes o Participação Ativa: Incentivar a participação ativa dos adolescentes no desenvolvimento de políticas e práticas relacionadas ao tratamento de dados. Esta previsão encontra respaldo no ordenamento jurídico pátrio no art. 7º da Resolução Nº 245 do CONANDA. Conclusão Considerando o princípio da autonomia progressiva e a responsabilidade civil dos pais, é viável que adolescentes forneçam consentimento para o tratamento de seus dados pessoais em determinados contextos, especialmente quando há uma avaliação adequada de sua maturidade e capacidade de compreensão a partir de critérios concretos, como ter idade entre dezesseis e dezoito anos. As práticas recomendadas pelas autoridades de proteção de dados, combinadas com uma abordagem educacional e participativa, podem garantir que esse processo seja realizado de maneira segura e conforme os melhores interesses dos adolescentes. ","705539":"Para garantir o respeito ao melhor interesse de crianças e adolescentes, promover altos níveis de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso de plataformas digitais, podem ser utilizados como baliza os parâmetros estabelecidos na Resolução Nº 245 do CONANDA. Este serve como um guia abrangente, destacando a importância de uma abordagem integrada e multissetorial para proteger os direitos das crianças e adolescentes no ambiente digital, assegurando a criação de um ecossistema seguro, inclusivo e informativo. Ao analisar estes dispositivos no contexto do tratamento de dados pessoais, podem ser implementadas as seguintes medidas: 1. Princípios de Proteção: o Não Discriminação: Garantia de igualdade e não discriminação. o Primazia do Interesse Superior da Criança e do Adolescente: Todas as operações de tratamento devem priorizar o bem-estar e os direitos desses indivíduos. o Direito ao Desenvolvimento Integral: Proteção ao desenvolvimento físico, mental, moral, espiritual e social. o Respeito à Liberdade de Expressão e Autonomia:

Garantia de acesso à informação e conhecimento sobre as operações de tratamento de dados. o Proteção de Dados e Privacidade: Garantia da proteção de dados pessoais e da autodeterminação informativa. 2. Parâmetros de Design e Implementação: o Design de Produtos e Serviços: Desde a concepção, os produtos e serviços, conforme aplicável, devem considerar o melhor interesse das crianças e adolescentes, cuja definição deverá ser exemplificada pela ANPD, incluindo mecanismos de proteção e segurança. o Informação e Transparência: Informações sobre o uso de dados devem ser fornecidas de forma clara, acessível e adequada à compreensão das crianças e adolescentes a partir de critérios pré-definidos de públicos alvo definidos por parte da ANPD. o Consentimento Específico e Destacado: O tratamento de dados deve ser baseado em consentimento livre, específico e informado dos responsáveis e, quando possível, dos próprios menores, considerando seu grau de maturidade a partir de critérios objetivos estabelecidos pela ANPD. o Minimização de Dados: Apenas os dados estritamente necessários devem ser coletados e armazenados pelo tempo necessário para a finalidade específica. o Proteção contra Fins Comerciais: Dados pessoais não devem ser utilizados para fins comerciais, como a criação de perfis de comportamento ou direcionamento de publicidade, ressalvada a hipótese do Controlador fornecer essa informação de forma clara e transparente ao titular, com possibilidade de opt-out de forma simplificada. 3. Salvaguardas Específicas: o Proteção Contra Conteúdos Nocivos: Implementação de mecanismos de verificação etária e controle parental para impedir o acesso a conteúdos inadequados. o Educação e Conscientização: Promoção de campanhas de sensibilização sobre os riscos e direitos no ambiente digital, incluindo formação para profissionais que lidam com crianças. o Participação Ativa: Envolvimento de crianças e adolescentes no desenvolvimento de políticas, programas e serviços que afetem seu uso do ambiente digital. o Mecanismos de Denúncia e Mediação Parental: Disponibilização de canais acessíveis para denúncias de conteúdos nocivos e recomendação ativa de participação de responsáveis legais. 4. Responsabilidades das Empresas: o Desenvolvimento e Implementação de Medidas de Segurança: Adoção de práticas de segurança, cujos parâmetros devem ser exemplificados pela ANPD, que protejam a privacidade e os dados pessoais das crianças e adolescentes. o Prevenção de Abusos e Explorações: Criação de ferramentas para prevenir e mitigar abusos, violência, discriminação e exploração no ambiente digital para empresas que tenham crianças e adolescentes como seu público alvo. o Avaliação de Riscos: Realização de avaliações contínuas de riscos relacionados ao uso de seus serviços por crianças e adolescentes. ","708762":"1. Introdução A verificação de idade em plataformas digitais é um aspecto crucial para a proteção dos dados pessoais de crianças e adolescentes, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD). A ANPD, ao desenvolver um projeto regulatório sobre o tratamento de dados de crianças e adolescentes, deve considerar técnicas e boas práticas que garantam a conformidade com os princípios da LGPD e promovam a proteção adequada dos menores no ambiente digital. 2. Boas Práticas para Verificação de Idade A CNIL (Comissão Nacional de Informática e Liberdades da França), a PDPC (Comissão de Proteção de Dados Pessoais de Singapura) e o CONANDA (Conselho Nacional Dos Direitos Da Crianças E Do Adolescentes) oferecem diretrizes que podem servir de base para a implementação de práticas eficazes e respeitosas à privacidade para a verificação de idade. A seguir, apresentamos uma

visão geral das boas práticas e técnicas recomendadas: 2.1 Verificação de Idade Baseada em Declaração e Certificação • Declaração por Parte do Usuário: o Autoridade dos Pais ou Responsáveis: A verificação pode incluir a declaração da idade pelo usuário ou responsável, embora essa prática seja menos segura e sujeita a manipulação. o Certificação por Documentos Oficiais: Documentos como passaportes ou carteiras de identidade podem ser utilizados para confirmar a idade, mas envolvem coleta de dados sensíveis e devem ser usados com cautela. • Certificação por Terceiros de Confiança: o Instituições ou Plataformas de Verificação: A utilização de serviços de verificação por terceiros confiáveis pode ser uma alternativa, desde que respeite a minimização dos dados pessoais coletados. 2.2 Verificação por Métodos Tecnológicos • Reconhecimento Facial: o Uso Controverso: Técnicas como reconhecimento facial levantam preocupações de privacidade e podem ser vistas como desproporcionais para a finalidade de verificação de idade. • Limitação do uso de dados o Finalidade: Os dados pessoais coletados para a finalidade de verificação de idade não devem ser tratados para qualquer outra finalidade, bem como devem ser excluídos imediatamente após a conclusão da verificação. 3. Recomendação para a ANPD 3.1 Pesquisa e Desenvolvimento de Tecnologias de Verificação de Idade A ANPD pode promover a pesquisa e o desenvolvimento de ferramentas de verificação de idade por meio de um sandbox regulatório. A CNIL e a PDPC indicam que há espaço para a inovação tecnológica na verificação de idade, sempre respeitando o princípio da minimização de dados e a proporcionalidade com os riscos envolvidos. • Sandbox Regulatório: A ANPD deve considerar a criação de um ambiente de testes para novas tecnologias de verificação de idade, avaliando soluções que equilibrem segurança e privacidade. 3.2 Aplicação de Princípios de Minimização e Proporcionalidade • Adequação ao Risco: A ANPD deve garantir que a verificação de idade respeite a proporcionalidade e a minimização dos dados pessoais, com base na avaliação dos riscos associados ao tratamento de dados, assim como que estes atendam somente à finalidade de confirmação de idade. • Métodos de Verificação: Para serviços que apresentam mais riscos a depender do público alvo a que se destinem com base na idade média deste grupo, como redes sociais e plataformas de jogos, métodos mais rigorosos de verificação devem ser adotados, enquanto serviços de baixo risco podem utilizar abordagens menos intrusivas, como auto-declaração. 4. Conclusão A verificação de idade é uma questão complexa que exige um equilíbrio entre a proteção da privacidade e a eficácia das medidas de segurança. A ANPD deve adotar uma abordagem baseada em riscos, promovendo práticas que respeitem a privacidade dos usuários e cumpram os requisitos legais estabelecidos pela LGPD. Agradecemos a oportunidade de participar desta consulta pública e esperamos que as recomendações aqui apresentadas contribuam para a elaboração de um regulamento eficaz e justo para a verificação de idade em plataformas digitais. ","708764":"A coleta de dados pessoais de crianças e adolescentes por plataformas digitais deve ser realizada com extrema cautela, respeitando os princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e as diretrizes da Resolução Nº 245 do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA). A seguir, destacamos as limitações que devem ser observadas para garantir a proteção adequada desses dados, em conformidade com o artigo 14 da LGPD. 1. Verificação de Idade 1.1 Mecanismos de Verificação A verificação da idade é um aspecto crítico para proteger crianças e adolescentes

de conteúdos e serviços inadequados. No entanto, os dados coletados para este fim devem ser limitados apenas à verificação de idade e não devem ser usados para outras finalidades. •

Limitação de Uso: Os dados obtidos para verificação etária devem ser estritamente utilizados apenas para confirmar a idade do usuário, como estipulado pela Resolução da CONANDA. •Tecnologias de Verificação: Devem ser implementadas tecnologias que minimizem a coleta de dados pessoais, como a utilização de estimativas de idade baseadas em comportamentos gerais, sempre considerado o nível de eficácia comprovado para estas técnicas e a boa-fé do agente de tratamento, e desde que não resultem na formação de perfis comportamentais, devendo a ANPD trazer premissas concretas de tecnologias aptas a esta finalidade. • Mediação parental: O CONANDA igualmente apregoa em sua resolução a necessidade das empresas de implementar mecanismos de mediação parental e participação dos responsáveis legais nestes ambientes. Esta prática deve igualmente estar atrelada aos princípios norteadores da LGPD. 2. Conclusão A proteção dos dados pessoais de crianças e adolescentes é essencial para garantir seu bem-estar e segurança no ambiente digital. As plataformas digitais devem observar rigorosamente as limitações estabelecidas pela LGPD e pela Resolução da CONANDA, coletando apenas os dados estritamente necessários e respeitando a finalidade específica do tratamento. A ANPD desempenha um papel fundamental na orientação e fiscalização dessas práticas, promovendo um ambiente digital seguro e protegido para os menores. ","708768":"1. Introdução Este material apresenta mecanismos e boas práticas recomendadas, baseadas na Resolução Nº 245 do CONANDA e nas diretrizes da CNIL, para ampliar o controle parental de forma eficaz e respeitosa à privacidade dos menores. 2. Mecanismos e Boas Práticas para Controle Parental 2.1 Mecanismos de Mediação Parental Conforme o Art. 20 da Resolução Nº 245 do CONANDA, as empresas provedoras de ambientes e serviços digitais devem disponibilizar mecanismos de mediação parental e promover ativamente a participação dos responsáveis legais. As seguintes práticas são recomendadas: • Filtros de Conteúdo Inapropriado: Implementação de filtros diretamente no dispositivo ou pelo aplicativo/serviço para bloquear conteúdos inadequados para a idade. • Regulação de Uso: Ferramentas para limitar o tempo de tela, regular interações online e gerenciar permissões para gastos online. •

Monitoramento de Atividades: Acesso ao histórico de navegação, conversas e conteúdo, além de relatórios sobre geolocalização e dados de transações. 2.2 Princípios de Proporcionalidade e Transparência Baseando-se nas diretrizes da CNIL, os controles parentais devem seguir os princípios de proporcionalidade, transparência e segurança: •

Proporcionalidade: Os controles devem ser adequados ao interesse, idade e maturidade da criança, evitando recursos intrusivos como rastreamento constante. •

Transparência: Explicação clara para a criança sobre quais controles parentais estão sendo usados e como funcionam. • Segurança dos Dados: Garantir que terceiros não tenham acesso aos dados das crianças, como informações de geolocalização. 3. Boas Práticas na Implementação de Controle Parental 3.1 Incentivo à Implementação As empresas devem ser incentivadas a implementar mecanismos de controle parental que respeitem a privacidade e o melhor interesse das crianças e adolescentes. É importante que as práticas adotadas estejam alinhadas com os princípios da LGPD, como minimização de dados e finalidade específica. 3.2 Avaliação e Melhoria Contínua •Melhoria Baseada em Evidências: Os mecanismos de

mediação parental e segurança devem ser continuamente aprimorados com base em evidências, garantindo que sejam eficazes e respeitem a privacidade. 4. Recomendações para a ANPD 4.1 Orientação e Fiscalização A ANPD deve fornecer diretrizes claras para a implementação de mecanismos de controle parental e fiscalizar seu cumprimento, garantindo que as práticas adotadas pelas empresas sejam efetivas e respeitem os direitos das crianças e adolescentes. 4.2 Educação e Conscientização • Campanhas de Conscientização: Promover campanhas educativas para informar pais e responsáveis sobre a importância do controle parental e as ferramentas disponíveis. • Formação e Apoio: Oferecer programas de formação e apoio técnico para ajudar os responsáveis a utilizarem os controles parentais de forma eficaz. 5. Conclusão A ampliação do controle parental no tratamento de dados pessoais de crianças e adolescentes é essencial para garantir um ambiente digital seguro e saudável. A implementação de mecanismos de mediação parental, respeitando os princípios de proporcionalidade, transparência e segurança, é fundamental para proteger a privacidade e o bem-estar dos menores. A ANPD deve liderar esses esforços, fornecendo orientações claras e promovendo a conscientização sobre a importância dessas práticas. ","708772":"1. Introdução Este documento apresenta boas práticas recomendadas para atingir esses objetivos, com base na Resolução Nº 245 do CONANDA e nas diretrizes da CNIL. 2. Princípios Fundamentais de Transparência 2.1 Privacidade por Padrão Conforme o Art. 12 da Resolução Nº 245 do CONANDA, a privacidade de crianças e adolescentes deve ser respeitada e protegida por padrão. Isso inclui: • Coleta Mínima de Dados: Apenas a quantidade mínima de dados pessoais deve ser coletada para a finalidade específica do serviço, e o armazenamento deve durar apenas o tempo necessário para essa finalidade. • Altos Padrões de Proteção: Os dados devem ser tratados com os mais altos padrões de proteção, segurança e procedimentos éticos 3. Boas Práticas para Transparência e Informação 3.1 Linguagem Simples e Acessível De acordo com o Art. 13 da Resolução Nº 245 do CONANDA, as empresas devem informar adolescentes sobre o uso de seus dados em linguagem simples, acessível e adequada. Algumas boas práticas incluem: • Sentenças Curtas e Claras: Utilizar frases curtas e diretas para explicar como os dados são coletados, usados e protegidos. •Elementos Interativos: Incluir ícones, vídeos ou imagens para tornar as informações mais compreensíveis e atraentes. • Informações Contextuais: Fornecer informações quando são necessárias para tomar uma decisão, como ao criar uma conta ou ajustar configurações de privacidade. 3.2 Design Ético de Interfaces A CNIL destaca a importância do design das interfaces para assegurar que adolescentes compreendam e possam exercer seus direitos. As seguintes práticas são recomendadas: • Evitar Dark Patterns: Design de interfaces deve evitar técnicas enganosas que manipulam a atenção e o comportamento do usuário. • Configurações de Privacidade Simples: Configurações de privacidade devem ser fáceis de mudar, com opções como geolocalização desativadas por padrão. 4. Implementação de Canais de Comunicação 4.1 Publicação de Compromissos Empresas devem publicar uma lista de seus compromissos com a proteção de dados de crianças, incluindo como cumprem as recomendações de transparência e proteção de dados. Isso ajuda a reforçar a confiança e garantir a clareza sobre as práticas adotadas. 5. Recomendações para a ANPD 5.1 Orientação e Fiscalização A ANPD deve fornecer diretrizes claras e específicas sobre como as plataformas digitais podem implementar práticas

de transparência adequadas para crianças e adolescentes. Além disso, deve fiscalizar o cumprimento dessas diretrizes. 5.2 Educação e Conscientização • Campanhas Educativas: Promover campanhas para educar crianças, adolescentes e seus responsáveis sobre a importância da privacidade e os direitos sobre seus dados pessoais. • Materiais Didáticos: Desenvolver e disponibilizar materiais educativos que expliquem, de forma simples e clara, como os dados pessoais são tratados e protegidos. ","708775":"N/A

Contribuinte: Paulo Henrique Atta Sarmento

Número: OP-753129

Data: 16/08/2024 - 15:54

Resumo: :"A ANPD (Autoridade Nacional de Proteção de Dados) enfrenta uma contradição em suas diretrizes sobre o tratamento de dados de crianças. A exigência de que o uso de dados seja sempre justificado pelo melhor interesse da criança, de certa forma, contradiz a permissão de utilizar a base legal do legítimo interesse do controlador (que, presume-se, prescreve a utilização dos dados no interesse exclusivo do controlador, sem referência aos interesses do titular). A base legal do legítimo interesse foi criada para permitir que o controlador utilize dados para seus próprios interesses independentemente dos interesses do titular. Isso inclui situações onde o titular dos dados já avaliou e consentiu com o tratamento, como ocorre em relação às bases legais de execução de contrato, onde há solicitação direta autorizando o tratamento. Em alguns casos, a relação entre o melhor interesse da criança e o interesse do controlador de dados é muito fraca. Por exemplo, em um caso de tratamento de dados para aperfeiçoamento do produto oferecido às crianças, o fornecimento de um produto superior funcionará, teoricamente, em benefício de todos. Porém, a noção genérica de aperfeiçoamento do produto como satisfazendo o requisito de melhor interesse da criança pode colocar em risco a intenção original do instituto, excessivamente flexibilizando a intenção da lei em cominar que o melhor interesse seja um requisito especial. A ANPD precisa se pronunciar para esclarecer isso melhor. Essencialmente, embora a utilização dos dados para melhorar produtos destinados às crianças possa ser vista como uma forma de beneficiar esse público, é crucial que tal justificativa não seja usada de forma ampla e genérica. Isso poderia comprometer a finalidade original da legislação, que é garantir que o melhor interesse da criança seja sempre uma consideração especial e prioritária. A ANPD tem um papel importante em esclarecer esses pontos para evitar interpretações que possam enfraquecer a proteção dos dados das crianças. ","708725":"Sim, existem situações que demandam maior atenção e detalhamento. Um dos desafios em determinar o melhor interesse de menores de 12 anos está relacionado à dependência necessária da criança em relação ao responsável legal. A questão sobre a interpretação do melhor interesse, dada essa dependência, pode se tornar mais controversa. No contexto bancário, por exemplo, a abertura de contas em nome de crianças pode ser interpretada como uma realização de seu melhor interesse. Em cenários ideais, essa abertura de conta contribuiria para a criação de uma reserva financeira particular para a criança, permitindo sua participação direta como titular de conta e promovendo sua autonomia e educação financeira. Um produto que ofereça um

ambiente adequado para que as crianças possam aprender sobre gestão financeira e adquirir independência, nesse sentido, serve aos seus melhores interesses. Contudo, se um responsável legal não agir de boa-fé, ele pode utilizar uma conta desenhada para crianças em nome próprio, inclusive para finalidades ilícitas. A necessária dependência das crianças em relação aos seus responsáveis legais as torna mais vulneráveis para esse tipo de abuso. Em outras palavras, a concretização do melhor interesse pode ser garantida pelo controlador dos dados até certo ponto, levando em consideração o papel prioritário do responsável legal sempre que uma criança for envolvida. Nesse sentido, a regulação da LGPD deve considerar que a avaliação do melhor interesse da criança deve ser baseada na boa-fé do controlador em fornecer serviços que potencialmente beneficiem a criança, mas que não poderão protegê-la completamente de eventuais abusos por parte de um responsável legal. Portanto, é crucial que a regulação pela ANPD aborde a questão sobre a correta atribuição de responsabilidades entre controladores de dados e responsáveis legais quando se trata da realização do melhor interesse de crianças. No contexto bancário, sugerimos que a realização do melhor interesse das crianças é atingida a partir de requisitos como (i) a promoção da educação financeira; (ii) a inclusão da criança em ambientes de gestão financeira, considerada sua progressão de autonomia e capacidades específicas em cada faixa etária; (iii) o fornecimento de produtos com adequado nível de clareza e facilidade de acesso para cada faixa etária; (iv) o uso minimizado de dados para atingir tais objetivos. Para a minimização, alguns elementos concretos podem ser considerados para aferir o compromisso do controlador, como a adoção de cláusulas contratuais limitando a ação de operadores de dados sobre os dados de crianças e tecnologias de monitoramento de tais dados, para a prevenção de eventuais abusos. ","705523":"O §1º do art. 14 diz: “§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.” A ideia central do dispositivo era assegurar que, para qualquer ação envolvendo o uso de dados de crianças, haja autorização específica do responsável legal. No entanto, o estudo preliminar sobre hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes, bem como o Enunciado CD/ANPD nº 01, de 22 de maio de 2023, tentaram flexibilizar essa norma. Esses documentos sugerem que qualquer base legal de tratamento dos artigos 7 e 11 da LGPD poderia ser utilizada como alternativa para o tratamento de dados de crianças. Contudo, essa tentativa de flexibilização foi mal formulada e vaga, resultando em potenciais complicações jurídicas. Por exemplo: há uma série de direitos garantidos na LGPD especificamente para os casos de tratamento de dados com base legal no consentimento. São eles: (i) art.7º, § 5º: obtenção de consentimento específico para compartilhamento de dados; (ii) art. 8º, §5º: revogação de consentimento; art. 18, inciso VI: eliminação de dados com base no consentimento; (iii) art. 8º, §6º: informações sobre qualquer alteração na finalidade; forma e duração do tratamento identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento, conforme o art. 9º; (iv) art. 18, VIII: informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; etc. Não está claro, dado o Enunciado CD/ANPD nº 01, 22/2023, se o controlador deverá levar em consideração o fornecimento completo de todos os direitos baseados em consentimento em relação a qualquer novo uso de

dados de crianças, ou se poderá, por sua iniciativa, iniciar formas de tratamento com base legal em outros incisos do art. 7º que não prescrevem a observação estrita de tais direitos baseados no consentimento. Além disso, a imposição da observação destes direitos adicionais, particulares aos casos de base legal no consentimento, poderá criar uma barreira desnecessária ao desenvolvimento de mercados competitivos voltados a produtos e serviços para crianças. Futuras regulações pela ANPD deverão detalhar quais formas específicas de tratamento de dados requerem o consentimento parental e quais delas poderão ser realizadas por iniciativa do controlador, fundadas em outras bases legais. Uma sugestão é que o consentimento seja imprescindível na coleta inicial dos dados, bem como para a finalidade principal declarada no primeiro momento da relação com o responsável legal. Posteriormente, no entanto, o controlador poderia utilizar os dados para finalidades acessórias, não sendo necessário obter consentimento parental para cada nova finalidade específica, desde que essas finalidades sejam claramente incluídas em materiais de transparência, como políticas de privacidade ou notificações aos responsáveis legais (que prescindem do aceite explícito e registrado do responsável). ","708742":"Documentação Digital: Solicitar o envio de documentos comprobatórios, como RG ou CPF, para verificar a identidade. Tecnologias de Reconhecimento: Utilizar tecnologias de reconhecimento facial ou biometria para validar a identidade do responsável. Formulários Digitais Seguros: Implementar formulários digitais com campos obrigatórios para o consentimento explícito, incluindo a assinatura digital dos responsáveis. Avisos e Confirmações: Enviar e-mails ou mensagens de confirmação para os responsáveis, solicitando a confirmação do consentimento. Registro de Consentimento: Manter um registro detalhado de todos os consentimentos obtidos, incluindo data, hora e método de verificação. ","708745":"É essencial considerar o princípio do melhor interesse e a autonomia progressiva dos adolescentes para decisões a respeito dos seus próprios dados. Em determinados contextos e situações, onde o impacto do tratamento de dados é claramente compreendido pelo adolescente e é de seu interesse, pode ser permitido que forneçam consentimento de forma autônoma. ","705539":"Para assegurar o respeito ao melhor interesse de crianças e adolescentes no tratamento de seus dados pessoais por plataformas digitais, é essencial observar um conjunto de princípios, em especial, a transparência, e a minimização de dados. Medidas de design centradas na privacidade desde a concepção (Privacy by Design) e configurações padrão que ofereçam o maior nível de proteção possível (Privacy by Default) são fundamentais. As interfaces e a linguagem das plataformas devem ser intuitivas e adequadas à faixa etária, facilitando a compreensão e a tomada de decisões informadas. Além disso, é importante fornecer alertas contextuais sobre práticas seguras e permitir a reportabilidade de preocupações ou incidentes de privacidade. Revisões periódicas das políticas e práticas de tratamento de dados são necessárias para manter a conformidade com as normas legais e garantir a proteção contínua dos dados pessoais de crianças e adolescentes. ","708762":"Uma prática comum é a utilização de mecanismos de auto-declaração, onde os usuários informam sua data de nascimento durante o processo de registro. Porém, a abordagem deve ser complementada com medidas adicionais para evitar falsificações, como a inclusão de controles de consentimento parental e, quando possível, verificação biométrica associada à determinação da idade. Por exemplo, algumas plataformas utilizam sistemas de

verificação por meio de documentos de identidade, onde os usuários enviam uma foto de um documento oficial e fotos ou vídeos pessoais, ou seja, a utilização de inteligência artificial para analisar características faciais e estimar a idade dos usuários. ","708764":"A natureza dos dados coletados deve ser mais estritamente limitada ao necessário para a finalidade específica do tratamento. É importante que haja uma regulação mais rigorosa do perfilamento de crianças e adolescentes, buscando evitar ao máximo o direcionamento de conteúdo baseado em perfis inferidos. Isso porque o fenômeno de criação de "echo-chambers" (ou seja, "um ambiente onde uma pessoa só encontra informações ou opiniões que refletem e reforçam as suas próprias") pode ser particularmente danoso aos menores de idade. É importante que a regulação reconheça que parte do direito de auto-determinação informativa, especialmente no caso de crianças e adolescentes, se relaciona com o acesso amplo a informações, o que poderá alterar a tomada de decisões, a formação de opiniões e a construção da identidade própria. Como reconhecido no Artigo 29º das Diretrizes do Grupo de Trabalho para a Proteção de Dados sobre a tomada de decisão individual automatizada e a definição de perfis para efeitos do Regulamento 2016/679 que "Como as crianças representam um grupo mais vulnerável da sociedade, as organizações devem, em geral, abster-se de traçar perfis para fins de marketing. As crianças podem ser particularmente suscetíveis no ambiente online e mais facilmente influenciadas pela publicidade comportamental. Por exemplo, em jogos online, a criação de perfis pode ser usada para atingir jogadores que o algoritmo considera mais propensos a gastar dinheiro no jogo, bem como para fornecer anúncios mais personalizados. A idade e a maturidade da criança podem afetar a sua capacidade de compreender a motivação por detrás deste tipo de marketing ou as consequências. Tendo em conta estes comentários, espera-se que justifique o seu tratamento, evidenciando as salvaguardas que implementou e demonstrando que é apropriado utilizar os dados pessoais das crianças desta forma". ","708768":"Para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital, empresas podem oferecer ferramentas de controle parental robustas, incluindo configurações de privacidade personalizáveis, monitoramento de atividades e filtros de conteúdo. O ideal é que os responsáveis possam ajustar o nível de proteção e supervisão conforme necessário, sendo que o nível de interferência dos responsáveis será decrescente, conforme a progressão de autonomia da criança ou adolescente. O consentimento parental inicial deve ser granular, permitindo que os responsáveis escolham quais dados podem ser coletados e para quais finalidades. Porém, conforme o desenvolvimento da criança/adolescente, mais finalidades deverão ser consentidas pelo próprio titular de dados, com reconhecimento da sua progressão cognitiva para decidir sobre o tratamento dos próprios dados. Por fim, especificamente para crianças e adolescentes, é importante promover a educação e a conscientização sobre privacidade e segurança digital. Programas educativos e guias práticos e canais de comunicação eficazes para responder a dúvidas e preocupações dos responsáveis também são cruciais. ","708772":"É fundamental que as políticas de privacidade e termos de uso sejam redigidos em uma linguagem simples e compreensível, especialmente adaptada ao público jovem e seus responsáveis. Além disso, é útil utilizar formatos visuais e interativos, como infográficos, vídeos explicativos e tutoriais para comunicar informações complexas. As plataformas devem oferecer notificações e lembretes contextuais que

informem os usuários sobre suas práticas de privacidade e segurança, inclusive opções de consentimento granular, permitindo que os usuários escolham quais tipos de dados desejam compartilhar em cenários específicos. ","708775":"Não há.

Contribuinte: LAURA ALIENDE DA MATTA

Número: OP-753131

Data: 16/08/2024 - 15:58

Resumo: :"A Entertainment Software Association (ESA) é a associação comercial dos EUA que representa quase todas as principais editoras de videogames e fabricantes de consoles de videogame e dispositivos portáteis. Seus membros oferecem experiências interativas de alta qualidade que promovem a contação de histórias, competição e comunicação, mantendo a segurança de todos os jogadores de videogame como prioridade máxima. Por pelo menos 30 anos, o setor tem se empenhado em esforços contínuos para desenvolver e oferecer ferramentas que ajudem pais, responsáveis e jogadores a criar uma experiência de jogo on-line segura, conforme detalhado no documento Confiança e Segurança (vide anexo). No Brasil, o sistema Classind atribui classificações de idade e conteúdo aos videogames. Sob a atribuição do Ministério da Justiça, Classind tem 6 categorias de classificação etária, descritores de conteúdo para explicar as razões por trás da indicação e elementos interativos para destacar recursos como compras no jogo ou comunicação com o usuário. Classind faz parte da International Age Rating Coalition, uma coalizão formada por autoridades de diversos países. O Classind fornece às famílias informações necessárias para escolher a experiência de videogame adequada, incluindo informações essenciais para proteger crianças e adolescentes de conteúdo inadequado. Ele define critérios para a análise de obras audiovisuais e observa os princípios do ECA. ESA compartilha os objetivos da ANPD de proteger crianças e adolescentes e recomenda que a ANPD considere as questões de transparência e minimização de dados como indicadores-chave do respeito aos seus melhores interesses. Seus membros têm sido líderes em garantir a transparência na forma como informações pessoais são tratadas para experiências de jogos on-line e em oferecer ferramentas para a tomada de decisões informadas sobre configurações de privacidade, inclusive para pais e responsáveis para gerenciar as escolhas de entretenimento de seus filhos e garantir experiências adequadas à idade em videogames. Veja informações sobre transparência no item III.1. Em apoio à minimização, membros da ESA usam configurações padrão de proteção à privacidade para jogadores menores de idade, incluindo, por exemplo, limitação da coleta de dados, desativação do bate-papo e de outras comunicações no jogo, exigência de permissão dos pais para adicionar amigos ou jogar jogos com vários jogadores e desativação da coleta de dados de localização por padrão. A ESA incentiva a ANPD a apoiar a flexibilidade contínua na proteção de crianças e adolescentes ao invés de adotar uma abordagem única para todos. Especificamente, a ESA recomenda que a ANPD publique uma orientação de conformidade voluntária sobre os princípios de melhor interesse (incluindo transparência e minimização de dados) ao invés de adotar uma regulamentação prescritiva que poderia desincentivar inovações contínuas para proteger as crianças em todas as

tecnologias, plataformas e contextos. A ESA recomenda, de forma enfática, que a ANPD permita que as partes interessadas analisem e forneçam comentários sobre qualquer minuta de regulamentação formal antes de sua finalização, isso porque regulamentações tem o potencial de interromper uso de uma variedade de tecnologias popular voltadas para o consumidor, caso as diferenças no uso de tecnologia entre plataformas e setores não sejam completamente levadas em consideração. Por fim, ESA incentiva a ANPD a garantir que tais orientações estejam alinhadas com outras iniciativas em curso no momento. Por exemplo, em nível nacional, ANPD deve coordenar com outros órgãos brasileiros envolvidos em questões de segurança e bem-estar das crianças, a nível nacional, como aquelas vinculadas à Secretaria de Comunicação Social da Presidência. ANPD também deve dialogar com legisladores para evitar criação políticas conflitantes. A nível global, ANPD deve considerar alinhamento com novas medidas de proteção de dados com frameworks globais, como o Regulamento Geral de Proteção de Dados da UE e, nos EUA, a Lei de Proteção à Privacidade Online das Crianças. ESA entende que tal alinhamento promoveria ainda mais sua conformidade. ","708725":"A indústria de videogames prioriza a segurança das crianças e procura minimizar a coleta de dados de menores, ao mesmo tempo em que garante a coleta apropriada de informações pessoais para administrar os esforços de confiança e segurança on-line, e garantir que o ambiente para os jogadores seja adequado à faixa etária. Algumas dessas práticas estão detalhadas abaixo e no documento anexo sobre Confiança e Segurança (Trust and Safety, em inglês) (Anexo: O Setor de Videogames Prioriza a Confiança e a Segurança (The Video Games Sector Prioritizes Trust and Safety, em inglês)). A ESA incentiva a ANPD a apoiar esses esforços como parte do princípio do melhor interesse, incluindo onde tais práticas possam exigir a coleta de certos dados. As empresas membros da ESA desenvolveram e implantaram tecnologias e medidas para ajudar a manter os jogadores seguros, evitar o ódio, o assédio e outros comportamentos inadequados, além de capacitar os jogadores e seus responsáveis. Algumas empresas, por exemplo, implementaram monitoramento automatizado de bate-papo, silenciamento automático e/ou moderação humana para limitar ou filtrar conteúdo ou comportamento indesejado e, quando apropriado, tomar medidas contra malfeitores para fazer cumprir os padrões da comunidade de jogos ou seus termos de serviço para proteger outros jogadores. Algumas empresas de videogame também usam aprendizado de máquina para identificar comportamentos de trapaça e garantir que os jogadores possam participar de uma competição de forma justa e positiva. Os membros da ESA também tomam várias medidas para combater a exploração infantil. Algumas empresas utilizam tecnologias de aprendizado de máquina para detectar, abordar e denunciar predadores on-line que tentam aliciar menores. A indústria de videogames atua em conjunto com terceiros reconhecidos nessa frente, como o National Center for Missing and Exploited Children (NCMEC), uma organização não governamental dos Estados Unidos, e com as autoridades policiais para combater imagens e conteúdos inadequados. Por exemplo, algumas empresas membro que permitem o envio de imagens pelos usuários utilizam tecnologias de "hashing" de imagens para combater a exploração infantil. Assinaturas digitais, ou "impressões digitais" de imagens conhecidas de exploração infantil são obtidas junto ao NCMEC com o objetivo de identificar e detectar tais imagens antes que possam ser publicadas. A indústria de videogames leva a sério sua responsabilidade de compartilhar

informações relevantes sobre exploração infantil com o NCMEC e com as autoridades policiais para apoiar a investigação de quaisquer imagens recentemente identificadas por eles. Os jogos educativos também são outro exemplo de esforços para apoiar um ambiente seguro e adequado à faixa etária para o aprendizado. Por exemplo, um jogo educativo pode processar dados de jogabilidade para reconhecer que o jogador está com dificuldades em matemática, mas se sai bem em leitura, e recomendar mais conteúdos relacionados à matemática. . É fundamental que as empresas de videogame continuem a ter flexibilidade para apoiar e inovar nesses e outros esforços no futuro. ","705523":"Incentivamos a ANPD a fornecer orientações adicionais voluntárias (e não regulamentação formal) sobre possíveis abordagens para obter o consentimento “específico e destacado” de pais ou responsáveis. Essas orientações devem ser práticas e adaptáveis a uma variedade de tecnologias e experiências, e estar alinhadas com outros frameworks globais, como o GDPR e a COPPA. Entendemos que qualquer nova orientação deve também evitar determinar mecanismos de consentimento específicos, linguagem, timing, localização ou frequência. Qualquer determinação de tipos específicos e limitados de tecnologias pode impor um grande ônus às empresas que teriam que alocar recursos para criar padrões potencialmente inadequados, ao mesmo tempo em que restringiria a liberdade das empresas de criar ou adotar tecnologias mais eficientes para obter consentimentos. Como mencionado também nos itens II.2 abaixo, a relação entre operadores de plataformas de videogame (por exemplo, celulares, PCs, consoles e portáteis) e editores de videogames, editores esses que podem oferecer múltiplos jogos em diferentes plataformas, é única para a indústria de videogames. A ESA incentiva a ANPD a permitir que operadores de plataformas e editores de jogos considerem voluntariamente soluções apropriadas à luz da funcionalidade técnica da plataforma e dos jogos disponíveis, seja (a) implementando mecanismos de consentimento baseados na plataforma, (b) confiando nos mecanismos de consentimento implementados pelos editores dos jogos em suas plataformas, ou (c) uma combinação de ambos. A ESA incentiva a ANPD a apoiar a flexibilidade para desenvolver quaisquer abordagens desse tipo. Ao oferecer orientações que permitam aos provedores de videogames ajustar a combinação desses mecanismos de acordo com seus serviços específicos, a ANPD garantirá aos pais e responsáveis que o princípio geral do consentimento esteja em vigor e, ao mesmo tempo, que eles mantém a capacidade de decidir o tipo de sistema mais adequado para as crianças e adolescentes sob seus cuidados. Esse tipo de flexibilidade tem se mostrado bem-sucedida nos Estados Unidos, onde a COPPA prevê múltiplos métodos aprovados para a obtenção do consentimento parental.","708742":"A ESA sugere que a ANPD considere a possibilidade de publicar orientações voluntárias sobre as principais características que devem ser reconhecidas na obtenção do consentimento, ao invés de exigir medidas e mecanismos tecnológicos específicos que possam ser aplicados de forma especifica a determinados setores ou tipos de plataformas, ou que estejam sujeitos a mudanças em função de futuras inovações tecnológicas. Além disso, as recomendações de orientação e política da ANPD devem permanecer flexíveis para se adaptarem às boas práticas, tecnologias e mecanismos disponíveis, bem como à exigência legal de adotar "todos os esforços razoáveis" para garantir o consentimento válido dos pais ou responsáveis pela criança. Isso é fundamental para garantir que a indústria de videogames continue a ter a capacidade de inovar e melhorar a segurança on-line e proteger a privacidade dos jogadores

menores de idade ao longo do tempo e em diferentes plataformas e tipos de jogos. Como detalhado no item II.1 acima, a relação entre operadores de plataformas de videogame (por exemplo, celulares, PCs, consoles e aparelhos portáteis) e editores de videogames, editores esses que podem oferecer múltiplos jogos em diferentes plataformas, é única para a indústria de videogames. A ESA incentiva a ANPD a permitir que operadores de plataformas e editores de jogos considerem voluntariamente soluções que sejam apropriadas em função da funcionalidade técnica da plataforma e dos jogos disponíveis, seja (a) implementando mecanismos de consentimento baseados na plataforma, (b) respeitando os mecanismos de consentimento implementados pelos editores dos jogos em suas plataformas, ou (c) uma combinação de ambos. A ESA defende uma abordagem flexível ao consentimento, pois a viabilidade de qualquer mecanismo de consentimento dependerá fortemente dos requisitos técnicos específicos da plataforma e dos jogos associados.","708745":"A ESA incentiva a ANPD a apoiar autonomia um pouco maior para os adolescentes mais velhos em sua ao interação com videogames. Entendemos que legisladores reconheceram a importância de respeitar as escolhas dos pais com relação às informações pessoais de seus filhos pequenos e os direitos dos adolescentes de exercerem esses direitos de forma mais direta.","705539":"Os membros da ESA são comprometidos com a promoção da transparência sobre as práticas de tratamento de dados na indústria e a minimização da coleta de dados de menores. Esses dois princípios devem ser o foco de qualquer orientação da ANPD e essa orientação deve ser voluntária para incentivar os pais e responsáveis a tomarem decisões informadas e promover o desenvolvimento de ferramentas inovadoras. ESA fornece ferramentas para informar os pais e ajudá-los a entender e gerenciar as interações de suas crianças e adolescentes com seus videogames, consoles e dispositivos portáteis. A ESA têm sido líder em garantir transparência na forma como informações pessoais são tratadas para experiências de jogos on-line e em oferecer ferramentas para tomada de decisões informadas sobre configurações de privacidade, inclusive para que pais e responsáveis possam gerenciar as escolhas de entretenimento de seus filhos e garantir experiências adequadas à idade em videogames. Informar pais e responsáveis, incluindo por meio de avisos de privacidade e fornecimento de informações facilmente acessíveis sobre as classificações e descritores da ClassInd para explicar as razões por trás das indicações atribuídas permite que eles tomem decisões informadas antes de fazer configurações de privacidade e seleções de jogos. A ESA apoia os princípios de minimização e procura coletar e tratar somente os dados sobre menores que sejam estritamente necessários para garantir a segurança do jogador e um ambiente adequado à idade. Como parte desses esforços, seus membros usam configurações padrão de proteção à privacidade para jogadores menores, desativando bate-papo e outras comunicações dentro do jogo, exigindo permissão dos pais para adicionar amigos ou jogar em modo multijogador, e desativando coleta de dados de localização por padrão. A ESA implantou tecnologias e medidas para ajudar a manter os jogadores seguros, prevenir o ódio, assédio e outros comportamentos inadequados e empoderar jogadores e seus responsáveis. Algumas empresas implementaram monitoramento automatizado de bate-papo, silenciamento automático e/ou moderação humana para limitar ou filtrar conteúdo ou comportamento indesejado e, quando apropriado, tomar medidas contra malfeitores para fazer cumprir os padrões da comunidade de jogos ou seus termos de serviço para proteger outros jogadores. Essas medidas importantes

de confiança e segurança podem incluir o tratamento de dados pessoais de menores sendo que seus membros procuram limitar esse tratamento ao estritamente necessário. Medidas de design de videogames variam de acordo com o tipo de recursos e funcionalidades oferecidos no jogo ou na plataforma. Ressaltamos que qualquer orientação voluntária da ANPD deve ser flexível o suficiente para ser prática em todos os contextos. Ex. muitos jogos e consoles oferecem configurações padrão de proteção de privacidade para jogadores menores e controles parentais que limitam o acesso à comunicação no jogo e outros recursos interativos. Esse tipo de autorregulação e inovação deve ser incentivado. As plataformas de videogames já implementaram ferramentas robustas de privacidade, controles parentais e outras proteções, limitando o tempo que as crianças podem passar jogando videogames, restringindo comunicações on-line com outros usuários, gerenciando a quantidade de dinheiro que as crianças podem gastar, instituindo controles parentais por senha ou PIN para que as crianças não possam contornar as configurações de segurança. Como essas ferramentas estão disponíveis no nível do dispositivo, ANPD deve permitir que os editores de jogos confiem nas seleções de privacidade e controle parental feitos em consoles, PCs e celulares. Esse sistema incentiva e apoia pais e responsáveis a tomarem decisões consistentes e informadas de maneira simplificada. Ao mesmo tempo, os editores podem ter a liberdade de adotar medidas adicionais para proteger a privacidade e a segurança dos menores. Conclusão no item III.6 abaixo.","708762":"A ESA solicita à ANPD que adote uma abordagem flexível para a verificação de idade em plataformas digitais, permitindo uma variedade de técnicas adequadas que protejam efetivamente crianças e adolescentes (por exemplo, (a) uma empresa deve realizar uma avaliação de risco obrigatória do processo pretendido e (b) a implementação de medidas eficazes para garantir a minimização de dados). Além disso, mecanismos neutro de verificação de idade é um método menos oneroso para as famílias do que outras técnicas de estimativa de idade que exigem identificadores físicos. Recomendamos que a ANPD forneça orientações claras e voluntárias sobre métodos aceitáveis que possam atender às preferências de privacidade, segurança e conveniência do usuário. É importante ressaltar que a ANPD deve encarar com ceticismo as recomendações de abordagens excessivamente prescritivas, como a exigência de que os usuários forneçam documento de identidade emitidas pelo governo (como RG) para jogar videogames. Essa abordagem é desnecessária, pode ser excessivamente intrusiva e onerosa para os usuários e gerar preocupações adicionais com a privacidade (incluindo a privacidade das crianças e adolescentes, bem como dos pais e responsáveis). Em suma, uma exigência para que as empresas utilizem credenciais de identificação violaria o princípio da minimização de dados, que estabelece que os provedores devem tratar apenas os dados estritamente necessários para atingir o objetivo comercial. Ao adotar soluções flexíveis e práticas, a ANPD poderá garantir uma proteção robusta para jovens usuários sem criar barreiras desnecessárias para as famílias. Além disso, a ESA adverte contra o uso de técnicas de estimativa de idade com relação ao público-alvo. Embora aparentemente bem-intencionadas, essas técnicas são potencialmente invasivas à privacidade e, inadvertidamente, podem fazer com que os operadores coletem mais informações pessoais dos consumidores do que seria necessário para fornecer o serviço, além de serem difíceis de implementar na prática. A ESA também adverte contra o uso de avaliações de usuários e da idade dos usuários em sites e serviços similares como evidência

da composição ou do público-alvo que pretende avaliar. Nenhum desses dados serve como evidência confiável da idade dos usuários. As avaliações de usuários de um videogame, por exemplo, podem entrar em conflito umas com as outras e podem mudar ao longo do tempo, à medida que o jogo se torna popular entre diferentes públicos e se torna mais nostálgico com o passar do tempo. Além disso, dois serviços podem ser semelhantes sem que ambos sejam direcionados ao mesmo público. Por exemplo, um jogo de corrida de carros pode ser direcionado a jogadores mais velhos com base em seu design visual e de áudio, enquanto outro pode ser direcionado a crianças.","708764":"A flexibilidade contínua para lidar com contextos específicos é especialmente importante para os videogames. Durante várias décadas, os membros da ESA têm se esforçado para desenvolver processos adequados de minimização de dados, configurações de privacidade e controles parentais, incluindo configurações padrão, que são adaptados à indústria de videogames. Eles buscam acomodar os diferentes contextos nos quais as empresas de videogame podem tratar informações pessoais e as diferentes funcionalidades de jogos que os consumidores podem optar por usar. Incentivamos a ANPD a continuar apoiando esses esforços. Entendemos que a ANPD não deve impor proibições absolutas sobre a coleta de determinadas categorias de dados. Dependendo do contexto, um provedor pode ter interesse em realizar a coleta e a retenção de dados com o objetivo de identificar comportamentos inadequados. Para exemplos de iniciativas relacionadas à confiança e à segurança, veja o documento Confiança e Segurança (Trust and Safety, em inglês) anexo (Anexo: O setor de videogames prioriza a confiança e a segurança (The Video Games Sector Prioritizes Trust and Safety, em inglês)). Ao invés de limitações específicas, a ANPD deve reforçar o princípio geral de minimização de dados, que estabelece que os provedores devem tratar apenas os dados estritamente necessários para atingir o objetivo comercial.","708768":"Conforme observado na resposta ao item III.3, a indústria de videogames dos EUA desenvolveu configurações de privacidade e controles parentais personalizados que se adaptam aos diferentes contextos em que as empresas de videogames podem tratar informações pessoais e às diferentes funcionalidades dos jogos que as crianças e seus pais ou responsáveis podem optar por usar. Muitos membros da ESA usam mecanismos como configurações padrão de proteção à privacidade para jogadores menores de idade, incluindo a minimização da coleta de dados, a desativação do bate-papo e de outras comunicações dentro do jogo, a exigência de permissão dos pais para adicionar amigos ou jogar jogos multijogador (multiplayer, em inglês) e a desativação da coleta de dados de localização por padrão para aumentar o controle dos pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital. Esses controles parentais geralmente são protegidos por pin ou senhas para garantir que sejam usados apenas pelos pais e não sejam burlados pelas crianças.","708772":"Os membros da ESA estão comprometidos em proporcionar aos consumidores transparência e controle sobre suas informações pessoais. Juntamente com seus membros, a ESA tem estado na vanguarda da promoção da privacidade e da segurança dos consumidores, incluindo menores de idade, por quase três décadas. Por meio de práticas voluntárias e em conformidade com a legislação existente, os provedores de videogames fornecem aos jogadores e responsáveis divulgações sobre a coleta de dados que são facilmente acessíveis e escritos de forma clara. Quando apropriado, os avisos de privacidade são adaptados à faixa etária do público, por exemplo, para públicos mais jovens,

os avisos são adequados para crianças e escritos em linguagem fácil de entender. ","708775":"Conclusão do item III.1 acima. Com base em sua experiência, ESA solicita à ANPD que assegure que qualquer orientação voltada para a proteção de dados pessoais e mitigação de riscos provenientes do uso de plataformas digitais permaneça flexível para acomodar diferenças importantes entre (a) indústrias e contextos, (b) preferências e expectativas razoáveis dos consumidores, (c) ferramentas de privacidade e as configurações de controle parental que já existem nas plataformas (ou seja, se uma empresa desenvolve um jogo que só pode ser jogado em uma determinada plataforma e essa já implementou esses controles de proteção de privacidade, o desenvolvedor do jogo não deveria ter que incorporar esses controles como nativos, pois os jogadores/pais/responsáveis podem acessar esses controles na plataforma) e (d) em tecnologias em evolução. Essa orientação deve ser consistente com os frameworks globais - GDPR e COPPA. A ESA agradece os esforços contínuos da ANPD para criar um ambiente seguro e de apoio para as crianças no espaço digital. Como uma das principais partes interessadas nesse espaço, a ESA testemunhou o desenvolvimento de práticas confiáveis no setor que fornecem ferramentas inovadoras para os pais. As práticas estabelecidas pelos membros da ESA, que provaram ser seguras e adaptáveis, mostraram que a flexibilidade concedida à indústria foi fundamental para promover esses avanços. Essa flexibilidade permite que as empresas continuem evoluindo e criando novas soluções que atendam às necessidades tanto de pais quanto de crianças, ao mesmo tempo em que permanecem alinhadas com os objetivos do marco legislativo de proteção de dados. Acreditamos firmemente que a inovação contínua nessa área é essencial. Para isso, é fundamental evitar regulamentações excessivamente prescritivas que possam complicar a conformidade à medida que o tempo e a indústria evoluem. Em vez disso, defendemos uma abordagem que promova a inovação e, ao mesmo tempo, garanta a adesão às metas regulatórias. Apoiamos a abordagem da ANPD de consultar a sociedade sobre esse importante tópico. Pedimos que a ANPD considere a importância de manter uma abordagem flexível ao estabelecer uma orientação voluntária sobre esse importante assunto. A proteção adequada dos dados pessoais de crianças e adolescentes e seu acesso a conteúdo apropriado em plataformas digitais tem sido discutida em várias jurisdições (por exemplo, EUA, Reino Unido, França, Irlanda), especificamente sobre a questão da garantia de idade. Dada a variedade de métodos e tecnologias atualmente disponíveis, a ESA recomenda que a ANPD adote uma abordagem educacional em vez de uma abordagem regulatória para essas questões e evite emitir uma regulamentação formal que poderia exigir uma revisão a cada poucos meses devido às mudanças na tecnologia e nas considerações empresariais sobre os meios mais eficazes e eficientes de promover o processamento de dados com proteção de privacidade. A ESA solicita que a ANPD (1) publique orientações voluntárias sobre os padrões minimamente aceitos de verificação de idade (por exemplo, (a) uma empresa deve realizar uma avaliação de risco obrigatória do processo pretendido, (b) implementação de medidas eficazes para garantir a minimização de dados) e (2) conduza estudos adicionais e envolva mais partes interessadas em relação à verificação e garantia de idade, promovendo melhores práticas na proteção de dados em plataformas digitais. A ANPD poderá também promover uma cultura de proteção de dados, tomando medidas para envolver pais e responsáveis e incentivá-los a se manterem informados à medida que as práticas evoluem. A

ESA e seus membros estão profundamente comprometidos com os objetivos de proteger os dados de crianças e adolescentes e garantir a transparência, a verificação efetiva da idade, o controle parental e as melhores práticas. Estamos ansiosos para colaborar com a ANPD em sua avaliação de possíveis orientações voluntárias nessas áreas.

Contribuinte: JULIO CESAR DE OLIVEIRA ALVES

Número: OP-753137

Data: 16/08/2024 - 16:09

Resumo: :"Sem considerações.","708725":"O Código Civil estabelece quem são os responsáveis legais de um menor. De acordo com o artigo 1.634, são considerados responsáveis legais os pais, o tutor e o guardião. Há situações no qual o tratamento de dados poderá ser realizado por outra base legal, a exemplo da execução de contrato, no qual o envio dos dados pessoais dos menores de idade será encaminhado por terceiros. A exemplo: Funcionário possuiu o benefício do plano de saúde na empresa contratante, podendo ser incluído no plano, além do cônjuge ou companheiro, os filhos e enteados. A empresa possuiu contrato estabelecido com a Operadora de Plano de Saúde, no qual requerer dados pessoais e/ou sensíveis para ingresso no plano de saúde dos dependentes do funcionário, inclusive do menor. Vamos considerar aqui o ingresso de um enteado. Estas informações podem ser encaminhadas diretamente pelo funcionário (padrasto ou madrasta) ou empresa. Porém, no exemplo, o funcionário (padrasto ou madrasta) não é responsável legal pelo menor, a dependência do menor deriva com a comprovação de vínculo com o(a) companheiro (a), tal como ocorre na possibilidade de declarar enteados no Imposto de Renda. Como realizar o tratamento dos dados do menor, sem inviabilizar o acesso deste, no qual o ingresso no plano de saúde foi requerido por terceiro, porém, visando o melhor interesse da criança. ","705523":"Em meio físico ou digital, sugere-se estabelecer o tamanho de fonte do texto, que não seja inferior ao corpo 12, assemelhando-se ao disposto na Lei 11.785/2008, e que o tipo de fonte seja legível, facilitando a leitura do titular dos dados. O consentimento específico e em destaque deverá ser apartado e destacado, utilizando formatação diferenciada no texto, a exemplo do negrito ou informações em quadro com sombreamento, ainda, com opção de identificar plenamente o consentimento para cada uma das atividades de tratamento de dados pessoais no qual a base legal é a do consentimento, em meio físico contendo campo para assinatura ou rubrica, em digital caixa de seleção, a exemplo: li e concordo. ","708742":"Sugere-se, a exemplo de aplicativos de controle de acessos, cito Google Family, uma boa prática seria vincular no cadastro inicial, o e-mail de pelo menos um dos pais ou responsável pela criança, esse recebia uma solicitação de confirmação do consentimento, ou ainda opção para revogação.","708745":"Sem considerações.","705539":"Sem considerações.","708762":"Sem considerações.","708764":"Sem considerações.","708768":"Sem considerações.","708772":"Sem considerações.","708775":"Sem considerações.

Contribuinte: Tatiane Vieira

Número: OP-753141

Data: 16/08/2024 - 16:52

Resumo: :"O Enunciado CD/ANPD n° 01/2022 e o Guia Orientativo sobre Hipóteses Legais de Tratamento de Dados Pessoais sobre o Legítimo Interesse orientam de forma satisfatória a devida utilização da base legal do legítimo interesse no contexto de tratamento de dados de crianças e adolescentes, especialmente quando disciplina ser necessário um teste de balanceamento, tendo a necessidade de gradação dos riscos, e ser a base legal adequada quando há uma relação prévia e direta do controlador com os titulares. Sugerimos que seja feita a regulamentação no sentido do Guia, estipulando a necessidade de teste de ponderação prévio ao tratamento nas hipóteses de tratamento de dados de crianças e adolescentes, por meio de relatórios de impactos, prevendo não somente os possíveis riscos envolvidos, mas também as medidas de mitigação propostas para evitar a ocorrência desses riscos. Busca-se, assim, permitir que o controlador realize a gradação dos riscos envolvidos no tratamento de maneira prévia, a ponderação acerca do interesse da criança no caso concreto e eventuais interesses contrapostos, a fim evitar a legitimação de riscos inaceitáveis e tratamento de dados em desacordo com o melhor interesse. ","708725":"Situação do melhor interesse da criança em escolas públicas, escolas e creches em geral e clínicas de saúde.","705523":"Para plataformas e aplicativos, utilizadas diretamente pelas crianças e adolescentes, é recomendável utilizar design amigável e compatível com a compreensão de crianças e adolescentes incluindo o uso de ícones, símbolos visuais e elementos gráficos como cartoons e gamificação e vídeos para explicar a necessidade de coleta do consentimento de pais ou responsáveis e o que a criança deve fazer. Pode-se utilizar como critério o envio da carteira de identidade do responsável legal da criança ou adolescente e a certidão de nascimento ou carteira de identidade da criança ou adolescente, acompanhado de um aceite, através de assinatura válida, em relação ao tratamento de dados pessoais na hipótese em questão. Além dessas medidas é importante que seja viabilizada a revogação do consentimento a qualquer momento por meio de informação clara e acessível e pergunta periódica realizada aos pais.","708742":"Considerando o ambiente digital, verifica-se como uma alternativa para viabilizar a verificação do consentimento a autenticação via biometria ou GOV.BR nas lojas de aplicativos como forma de garantir a verificação da identidade dos responsáveis e centralizar a implementação. Caso esta iniciativa não seja possível, pode ser considerada uma boa prática a implementação de mecanismos de autenticação (como sistema de gerenciamento de identidade e acesso - IAM) por outros sistemas pelas próprias plataformas.","708745":"Pode-se considerar a autonomia progressiva, em consonância com o melhor interesse, desde que não envolva compras online e objetos que possam gerar algum prejuízo ao adolescente, bem como designs capazes de induzir ou manipular de forma significativa o comportamento do jovem. É importante que neste caso seja exigido relatório de impacto prevendo os riscos nesta hipótese e medidas técnicas e administrativas de prevenção adotadas.","705539":"Algumas medidas para mitigar os riscos decorrentes dessas plataformas digitais são as seguintes: vedação à publicidade online voltada para crianças, vedação à possibilidade de compra facilitada (ex.: compra com 1 clique), configuração de

privacidade por padrão com opt-out para cookies (e outras tecnologias de coleta automática de dados) não necessários, necessidade de garantir controle parental antes de liberar o uso da plataforma (com autenticação da identidade do responsável), bem como uso de ban temporário como ferramenta repressiva. Além disso, é recomendável utilizar design amigável e compatível com a compreensão de crianças e adolescentes incluindo o uso de ícones, símbolos visuais e elementos gráficos como cartoons e gamificação e vídeos para explicar como ocorre o tratamento de dados pessoais, promovendo a informação e garantindo a transparência, fomentando nos jovens, desde cedo, a cultura e a conscientização sobre a necessidade de proteger seus dados pessoais. ","708762":"Alguns exemplos de técnicas disponíveis para a verificação de idade dos usuários de plataformas digitais são as seguintes: autenticação via biometria ou GOV.BR nas lojas de aplicativos como forma de garantir a autenticação dos responsáveis e centralizar a implementação; solicitação de foto do responsável com documento de identificação e envio da certidão de nascimento ou documento de representação legal; integração com instituições financeiras para autenticação por biometria (alerta-se que neste caso há o tratamento de dados pessoais sensíveis, o que denota uma maior cautela da plataforma e a necessidade de observância do rol de bases legais do art. 11 da LGPD - podendo ser para obrigação legal ou regulatória, se houver regulamentação da ANPD neste sentido) ou outros sistemas de verificação disponíveis no mercado. ","708764":"Deve ser vedada a formação de perfis comportamentais dos usuários, identificação de humor e padrão de emoção, indução e manipulação de pensamento (em linha com neurodireitos), social score e propagandas direcionadas com base nas suas pesquisas e interesses, sobretudo a coleta de cookies (e outras tecnologias de coletas automáticas de dados) não necessários, como analíticos e de propaganda, por padrão. Ademais, deve-se evitar ao máximo a coleta e possibilidade de compartilhamento de fotos/imagens dentro da plataforma (por meio de chat, por exemplo) ou incluir ferramenta que mascare (anonimize) dados pessoais potencialmente sensíveis e incluir a necessidade de informação clara e em linguagem simples sobre o alerta para não compartilhamento de dados como endereço e imagens para proteger crianças e adolescentes de situações de assédio. ","708768":"A necessidade de dupla autenticação para uso da Plataforma online em dispositivos pertencente aos pais e responsáveis legais (necessidade de autenticação por conta google, por exemplo) e mensagem clara e objetiva, preferencialmente utilizando design amigável com elementos visuais e vídeos explicativos curtos contendo explicações sobre os riscos envolvendo o uso da plataforma e as restrições existentes nas configurações de privacidade que podem ser ativadas. Ademais, é importante que as principais configurações de privacidade sejam ativadas por padrão e que seja encaminhada mensagem aos pais ou responsáveis acerca do uso de chat na plataforma para sua autorização e inclusão de filtros no chat com identificação de solicitação de dados pessoais ou compartilhamento de imagens para reportar aos responsáveis caso verificado alguma atividade suspeita. ","708772":"Podem ser utilizadas ferramentas de Privacy by Design e linguagem simples, por meio de cartoons contendo uma história que vá explicando o uso de dados, uma gamificação da política de privacidade com um quiz interativo para pais e filhos sobre proteção de dados na plataforma, vídeos curtos sobre alertas que os pais devem ter e configurações de privacidade e controle parental, por exemplo. Pode ser realizado um vídeo educacional contendo uma história que tenha relação

com a importância da proteção dos dados e de não fornecimento de dados pessoais no chat.","708775":"Não.

Contribuinte: CHRISTINE MATTOS ALBIANI LEMOS

Número: OP-753147

Data: 16/08/2024 - 17:15

Resumo: :"É importante harmonizar a compreensão sobre a aplicação do Legítimo Interesse atualmente veiculada pela ANPD com o princípio do melhor interesse das crianças e adolescentes previsto no artigo 227 da Constituição Federal, materializado pelo Estatuto da Criança e do Adolescente (ECA) e com a Convenção sobre os Direitos da Criança ratificada pelo Brasil. Atualmente, vemos duas possibilidades interpretativas que divergem entre si apesar da sua importância para a aplicação benéfica da LGPD às crianças e adolescentes. A primeira, indica a proteção dos dados pessoais de crianças e adolescentes sob a rubrica de dados pessoais sensíveis. Isso traria como consequência a possibilidade de utilizar somente as bases legais do artigo 11º da LGPD para tratar os dados pessoais desses titulares. É possível ver esse raciocínio, que traz dados pessoais de crianças e adolescentes ao mesmo nível de criticidade de dados pessoais sensíveis, subjacente à Resolução nº 2/2022, para microempresa e empresas de pequeno porte, quando na alínea "d", do inciso II, do §4º a ANPD adota a seguinte redação: Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados: II - critérios específicos: d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos. Isso também acontece na Resolução de Dosimetria e Aplicação de Sanções Administrativas, quando no §3º, do inciso I, do artigo 8º a autoridade diz que a infração será considerada grave quando envolver dados sensíveis ou dados de crianças e adolescentes, equiparando novamente essas duas categorias: Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em § 3º A infração será considerada grave quando: I - verificada uma ou mais hipóteses estabelecidas no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes: c) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças e adolescentes e de idosos. No entanto, a mesma ANPD emitiu posicionamento de que todas as bases legais poderiam ser utilizadas para tratar os dados pessoais desses titulares, inclusive o legítimo interesse. No Enunciado nº 1 de 2023, a ANPD indicou que: "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei." A harmonização desses dois tipos de compreensão passa pela busca do balanceamento entre o legítimo interesse do controlador e o melhor interesse das crianças e adolescentes, documentadamente, na etapa de balanceamento do teste do legítimo interesse. Para isso, uma sugestão seria o aprimoramento da recomendação de 2023 e do guia de uso da base legal do legítimo interesse, para que esses dois documentos

incorporassem dois pontos: 1. O primeiro, é que os controladores de dados devem levar em consideração o contexto específico de tratamento de dados pessoais e quais são os elementos relevantes para avaliar os melhores interesses, atribuindo pesos para o que é mais e menos importante para a preservação do melhor interesse das crianças e adolescentes; 2.O segundo, é que os controladores devem seguir um procedimento que garanta a adoção de salvaguardas adequadas para assegurar o melhor interesse desse tipo de titular de dados. Além disso, seria interessante que a ANPD evidenciasse quais são etapas adicionais podem ser acrescentadas ao "teste do legítimo interesse" proposto no Guia emitido por ela, para garantir a consideração o balanceamento entre os dois tipos de interesse que estão associados à aplicação dessa base legal. [continuação em documento enviado por email]","708725":"Sim, existem situações nas quais o ambiente e as condições nas quais as crianças possam estar mais vulneráveis à conteúdo problemático ou interações irrestritas com outras pessoas. Nesse sentido, elencamos as situações que entendemos que devem ser melhor estudadas: • Controle de acesso a conteúdo; • Situações e ambientes que demandam verificação de idade de acesso; • Monitoramento de espaços físicos e lógicos ocupados por esse público – por exemplo: monitoramento do desenvolvimento escolar; • Reconhecimento facial; • Prevenção à fraude utilizando nome e dados pessoais de crianças e adolescentes; • Processos de perfilização, sobre os quais é essencial a manifestação da ANPD, dada sua competência, notadamente a prevista nos arts. 55-J, XX e 55-K, e diante da vedação constante da Resolução CONANDA nº 245/2024 . ","705523":"Em primeiro lugar, é necessário ter em mente que obter o consentimento dos pais ou responsáveis legais não exclui o direito de crianças e adolescentes de compreender, dentro de seu contexto e desenvolvimento, o que acontece com os seus dados pessoais, para sua autodeterminação informativa, incluindo o exercício de seus direitos como titulares de dados pessoais. Por isso, o primeiro critério a ser observado é a necessidade de garantir um aviso de privacidade que possa ser compreendido por crianças e adolescentes. Esse mecanismo de transparência pode até ser o mesmo direcionado para pais ou responsáveis legais, mas é importante que ele seja lúdico, que apresente os esforços do controlador para se fazer entender pelo público infanto-juvenil, nos termos do artigo 14 da LGPD. O segundo critério a ser aplicado é o da especificidade. É preciso que fiquem evidentes as finalidades com as quais os pais ou responsáveis estão consentindo. Nesse sentido, a interpretação dada pela ANPD ao art. 14, LGPD, em seu Enunciado nº 01/2023, que autoriza a fundamentação de atividades de tratamento de dados pessoais nas diversas bases legais, desde que observado o melhor interesse de crianças e adolescentes, fomenta a utilização mais específica e responsável da base legal do consentimento. Não fosse assim, pais e responsáveis seriam mais facilmente instados a consentir com longos textos contendo diferentes finalidades de produtos e serviços. O Enunciado ANPD, ao reiterar a permissão legal para bases diversas, incentivou, na prática, o uso específico, destacado e pormenorizado, da base legal do consentimento. Como terceiro critério, o campo no qual se coleta o consentimento deve ser fisicamente e visualmente destacado dos demais, de forma que os pais ou responsáveis consigam identificar de forma clara onde podem permitir ou não o uso das informações. Como quarto critério, sugere-se a verificação dos esforços empregados para verificar a idade do responsável legal que está consentindo. Isso é dizer que existe um requisito de

verificabilidade para que o consentimento parental seja válido. Por fim, como quarto critério, sugere-se que os dados não podem ser coletados antes do consentimento parental. Ou seja, todos os esforços devem ser feitos para que a coleta só se inicie de fato após esse processo de registro do consentimento. Em primeiro lugar, é necessário ter em mente que obter o consentimento dos pais ou responsáveis legais não exclui o direito de crianças e adolescentes de compreender, dentro de seu contexto e desenvolvimento, o que acontece com os seus dados pessoais, para sua autodeterminação informativa, incluindo o exercício de seus direitos como titulares de dados pessoais. Por isso, o primeiro critério a ser observado é a necessidade de garantir um aviso de privacidade que possa ser compreendido por crianças e adolescentes. Esse mecanismo de transparência pode até ser o mesmo direcionado para pais ou responsáveis legais, mas é importante que ele seja lúdico, que apresente os esforços do controlador para se fazer entender pelo público infanto-juvenil, nos termos do artigo 14 da LGPD. O segundo critério a ser aplicado é o da especificidade. É preciso que fiquem evidentes as finalidades com as quais os pais ou responsáveis estão consentindo. Nesse sentido, a interpretação dada pela ANPD ao art. 14, LGPD, em seu Enunciado nº 01/2023, que autoriza a fundamentação de atividades de tratamento de dados pessoais nas diversas bases legais, desde que observado o melhor interesse de crianças e adolescentes, fomenta a utilização mais específica e responsável da base legal do consentimento. Não fosse assim, pais e responsáveis seriam mais facilmente instados a consentir com longos textos contendo diferentes finalidades de produtos e serviços. O Enunciado ANPD, ao reiterar a permissão legal para bases diversas, incentivou, na prática, o uso específico, destacado e pormenorizado, da base legal do consentimento. [continuação em documento enviado por email]","708742":"Como sugestões para a obtenção de um consentimento válido, a ANPD pode se inspirar na lista de métodos elencada pelo COPPA, na seção 312.5 (b) (2): “Fornecer um formulário de consentimento a ser assinado pelos pais e devolvido ao operador por correio postal ou e-mail; Exigir que um pai utilize um cartão de crédito em conexão com uma transação; Pedir que um pai ligue para um número de telefone gratuito atendido por pessoal treinado; Utilizar um documento público; usar e-mail acompanhado por um PIN ou senha obtidos através de um dos métodos de verificação listados pela autoridade”. Outras alternativas sugeridas por diferentes organizações à Federal Trade Comission, na oportunidade de uma mesa redonda, tais como: o reconhecimento por imagem, coleta de documento identificador como RG ou CPF, a criação de portais específicos para que os pais possam alterar as preferências de privacidade e coleta de dados pessoais de seus filhos, o método de envio de e-mail ou outro método de comunicação como SMS, para confirmar o consentimento inicialmente dado para o uso dos filhos. É importante que qualquer lista proposta pela autoridade seja adequadamente adaptada à realidade brasileira e que a ANPD evidencie, por meio dela, o tipo de ação que será considerada como “esforço razoável”, ou seja, que implicará o cumprimento das disposições do artigo 14º da LGPD. Nesse sentido, a ANPD deve levar em consideração o modelo de negócio dos controladores sob sua fiscalização e o seu faturamento, assim como as tecnologias que estão à sua disposição para realizar a coleta do consentimento. Por fim, o julgamento quanto à razoabilidade dos esforços empregados pelos agentes de tratamento também deve levar em consideração o risco que a atividade de tratamento para a qual se coleta o consentimento impõe às crianças e

adolescentes. Atividades de tratamento de risco baixo podem contar com métodos de obtenção e verificação do consentimento mais simples, enquanto atividades consideradas mais arriscadas devem ter camadas mais robustas de captação de evidências sobre a obtenção do consentimento. Também é importante que os controladores possam submeter as suas alternativas à apreciação da autoridade sem que sejam punidos por isso. Nesse caso, as iniciativas seriam validadas pela própria autoridade como forma de estimular o desenvolvimento de mecanismos para a obtenção do consentimento parental. É importante, no entanto determinar um prazo para a apreciação e parecer da ANPD sobre os casos apresentados, de forma a garantir a segurança jurídica desse processo. ","708745":"No Brasil, não se pode dizer que o conceito de autonomia progressiva foi totalmente incorporado pela legislação. A leitura do artigo 3º do nosso Código Civil indica que todas as pessoas com menos de 16 anos são absolutamente incapazes de exercer sozinhas os atos da vida civil. No entanto, em seu artigo 14, §1º, a LGPD determina que o consentimento será exigido para o tratamento de dados de crianças, que, nos termos do art. 2º, caput, do ECA, são as pessoas com até 12 anos incompletos. Se formos interpretar a LGPD, à luz somente do Código Civil, isso significaria impor aos agentes de tratamento a obrigação de obter o consentimento dos pais ou responsáveis legais não apenas de todas as pessoas com menos de 12 anos, mas também de todas entre 12 e 16 anos. É importante compreender também em que contexto da vida civil essa capacidade é exercida. De acordo com a pesquisa TIC Kids Online de 2023 , 95% das pessoas de 9 a 17 anos é usuária de internet, o que representa hoje 25 milhões de pessoas. No ano de 2019, a mesma pesquisa demonstrou que 29% dos usuários de 9 a 17 anos ajudaram os pais a fazerem alguma atividade online ou ainda que 28% destes jovens usuários oferecem apoio aos responsáveis pelo menos uma vez por semana. Por isso, não é possível ignorar a necessidade de viabilizar o acesso das pessoas com menos de 16 anos a aplicações na web. Nesse sentido, a teoria da autonomia progressiva é interessante pois encontra-se positivada em instrumentos legais internacionais que já são utilizados para interpretar as normas brasileiras à luz do melhor interesse das crianças e adolescentes. Nessa toada, é possível citar: • A Convenção sobre os Direitos da Criança e do Adolescente, que, no artigo 5º, dispõe que os Estados devem reconhecer o direito e o dever dos pais, famílias e tutores de orientar a criança sobre como exercer seus direitos “de acordo com a evolução de suas faculdades” • A Opinião Consultiva 17/2022, da Corte Interamericana de Direitos humanos, que evidencia existir “um grande variedade no grau de desenvolvimento físico e intelectual, na experiência e nas informações que possu[em].” as pessoas com menos de 18 anos; • O Comentário Geral nº 25 sobre os direitos das crianças e adolescentes no ambiente digital, que reconhece expressamente que a evolução da autonomia da criança e adolescente tem um significado especial no ambiente digital Assim, entendemos que o conceito de autonomia progressiva deve servir para harmonizar a aplicação do artigo 14 da LGPD e do Código Civil, viabilizando as atividades online de crianças e adolescentes e balizando a aplicação do melhor interesse nas três formas apresentadas na resposta à primeira pergunta. O conceito deve impulsionar uma limitação à necessidade de consentimento parental para toda e qualquer atividade de tratamento de dados, viabilizando o seu tratamento por meio da aplicação de outras bases legais, conforme disposto pela ANPD. Entendemos que cabe à ANPD interpretar a LGPD à luz do Código Civil, e modular as situações nas quais

a autonomia progressiva poderia ser uma alternativa para viabilizar a participação dos adolescentes em determinados contextos da vida civil, em ambiente digital. Contudo, ressaltamos a necessidade de cautela com expansão da autonomia progressiva ao âmbito da responsabilização criminal. O exercício progressivo da autonomia, em ambiente digital, em contextos civis adequados ao desenvolvimento da criança e do adolescente não implica imputabilidade penal e suas gravosas consequências. Este parece um ponto nodal e inescapável ao debate sobre a aplicação do conceito de autonomia progressiva e nos parece que é um bom limite para compreender as situações nas quais ele é ou não aplicável. ","705539":"Para designar os parâmetros e salvaguardas que devem ser adotados para proteger as crianças no ambiente online é preciso estar a par dos riscos que podem afetar esses titulares de dados pessoais. Segundo Elora Fernandes, há uma divisão de quatro tipos de riscos que podem acometer as crianças e adolescentes no ambiente online: riscos relacionados ao contato com conteúdos danosos, riscos derivados do contato – quando elas se engajam em atividades com atores maliciosos que na maioria das vezes são adultos, riscos derivados da conduta de seus pares como situações de bullying entre outros tipos de violência e riscos derivados de relações comerciais (contratos) que elas não estão prontas para assumir ou que são acompanhados de pressões comerciais, publicidade direcionada, perda de controle sobre os dados e riscos próprios dos modelos de negócio que envolvem o tratamento massivo de dados pessoais. Quanto a esse último tipo de risco, a OCDE ampliou a sua abrangência considerando que o ambiente da internet está permeado por alto nível de comercialização de produtos e serviços, de forma que os riscos comerciais foram divididos também em cinco tipos de riscos: de marketing, perfilização comercial, financeiros e de segurança. Segundo a OCDE, essas categorias de risco ainda são permeadas por riscos relacionadas ao uso de tecnologias avançadas como a IA, IoT, análises preditivas entre outras. Dentro da tipologia de risco elencada acima estão condutas específicas já conhecidas socialmente: Tipo de Risco Situações abarcadas pelo tipo de risco Conteúdo • Conteúdo proibido • Conteúdo prejudicial • Conteúdo de ódio/extremista • Desinformação • Pornografia • Cultura de sexualização • Publicidade imprópria Conduta • Comportamento de ódio • Cyberbullying • Comunicação hostil entre pares • Assédio sexual • Distúrbios alimentares ou de outra ordem incentivados por comunidades •Comportamentos prejudiciais ou ilegais gerados pelo próprio usuário Contato • Assédio • Perseguição • Vigilância indesejada/excessiva • Violência sexual • Extorsão • Aliciamento sexual • Manipulação psicológica • Radicalização • Recrutamento para grupos extremistas Contratuais/Comerciais • Roubo de identidade • Fraude • Phishing • Tráfico para fins de exploração sexual • Transmissão de conteúdo pago abuso • Jogos de azar • Microsegmentação (perfilização) • Padrões ocultos de design modelando ou persuadindo à compras Considerando a tipologia de riscos elencada acima e a interpretação sistemática do ordenamento jurídico brasileiro e de normas internacionais que parametrizam a interpretação das leis buscando o melhor interesse de crianças e adolescentes: em primeiro lugar, todo risco associado ao tratamento de dados pessoais desse público deve ser majorado em razão de sua vulnerabilidade intrínseca; em segundo lugar, e pela mesma razão, é importante tratar os dados pessoais de crianças e adolescentes considerando serem dados de

maior criticidade. O tratamento de riscos associados ao tratamento de dados pessoais de crianças e adolescentes como de maior gravidade diz respeito ao reconhecimento desses sujeitos como titulares de dados vulneráveis. Essa vulnerabilidade decorre da grande assimetria de poder que se configura entre crianças e adolescentes e os agentes de tratamento de dados pessoais. Como decorrência, é importante que atividades nas quais sejam identificados riscos para crianças e adolescentes devem contar com a elaboração de um Relatório de Impacto ao Tratamento de Dados Pessoais. Especificamente em relação aos riscos de contato identificados acima, sugere-se a adoção de tecnologias de monitoramento que possam ser utilizadas para monitorar com maior amplitude as interações de forma a garantir um ambiente respeitável e saudável. Contudo, é preciso que essas ferramentas sejam avaliadas sob o ponto de vista da privacidade, evitando a hiper vigilância do público infanto-juvenil. Além disso, é importante que as aplicações e iniciativas direcionadas para crianças contem com medidas de transparência e design (pensando na jornada do usuário), que sejam apropriadas para a sua idade. [continuação em texto enviado por email]","708762":"Para responder a essa pergunta é preciso levar em consideração que existe uma grande dificuldade técnica e contextual de definir com precisão a idade dos usuários de aplicação da internet. Isso pode ser ultrapassado com empenho, mas não sem custo. Por isso, a exigência de adoção de padrões técnicos que podem impor custos desproporcionais a agentes de tratamento como as organizações da sociedade civil não seria razoável. O cenário é diferente para agentes de grande porte como multinacionais. Feita essa ressalva, existem diversos meios que podem ser utilizados para verificar a idade dos usuários e eles podem variar de acordo com o risco avaliado de uma atividade de tratamento de dados pessoais para os usuários. Inicialmente, podemos citar os seguintes métodos : Atividades de baixo risco • Auto-declaração - o usuário simplesmente afirma que possui determinada idade mas não há evidência que confirmação. •Medidas técnicas que desencorajam a falsificação da informação – por exemplo, uma conta matemática que uma criança é incapaz de fazer sozinha, campo aberto para preenchimento da idade ao invés de seleção de uma idade pré-definida, impedimento de submeter uma nova idade imediatamente após não conseguir acessar a aplicação com a primeira informação fornecida. Médio Risco • Tais serviços normalmente funcionam em um sistema de “atributos” onde você solicita a confirmação de um atributo específico do usuário (neste caso, idade ou faixa etária) e do serviço fornece uma resposta ‘sim’ ou ‘não’. • Confirmação de usuário da conta – se o agente de tratamento sabe que a conta está ligada a um adulto, em um serviço subscrito, por exemplo, é possível permitir que esse adulto modele a forma que a criança ou adolescente acesse o serviço, criando senhas e perfis próprios para eles. Alto Risco • Inteligência artificial – monitoramento das interações do usuário com o serviço para identificar padrões de comportamento e inferir a idade do usuário. Essa técnica deve vir acompanhada de medidas que garantam a coleta do menor número de dados possível e o bloqueio de uso dos dados para finalidades distintas da identificação de idade dos usuários. • Coleta e apresentação de documentos formais. ","708764":"Entendemos que a especificação de limitações ao uso de dados pessoais de crianças e adolescentes devem estar ligadas às finalidades que impõem riscos considerados excessivos para esse público. Por exemplo, considerando a tipologia de risco da ONU, é possível identificar uma finalidade que é problemática não só sob a ótica da Proteção de

Dados Pessoais, mas do próprio Código do Consumidor (CDC), o direcionamento de publicidade para crianças e adolescentes. A prática é proibida de acordo com o artigo 36 do CDC c/c Resolução CONANDA nº 163/2014. Nesse sentido, a prática de microsegmentação com finalidade publicitária também pode ser problemática, pois deixa de levar em consideração o melhor interesse das crianças e adolescentes. Contudo, o risco excessivo não ocorre com a prática da perfilização para outras finalidades. A exemplo da perfilização para verificação do padrão de comportamento do usuário, a fim de inferir sua idade para permitir ou não o acesso a conteúdo inapropriado ela ocorre em benefício das crianças e adolescentes. Portanto, trata-se de uma prática que, a priori, não pode ser considerada incorreta, a menos que sua finalidade esteja em contradição com o princípio do melhor interesse conforme delineado no restante da presente nota técnica. Dessa forma, compreendemos que a finalidade é a melhor forma de limitar o que pode ou não ser feito com os dados pessoais. A limitação decorrente do tipo de dado pessoal pode levar à exclusão do público infanto-juvenil a priori de espaços importantes para o seu desenvolvimento.. Nesse sentido, a limitação por finalidade deve ocorrer de forma muito específica, a fim de garantir a segurança jurídica para os agentes de tratamento e não excluir as crianças e adolescentes de determinados espaços.
","708768":"A primeira boa prática a se levar em consideração para definir as medidas que podem ser utilizadas para ampliar o controle dos pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes é a necessidade de considerar a privacidade dessas pessoas. Muitas vezes, elas usam o ambiente online para desenvolver partes de sua personalidade que não necessariamente são aceitas pelos pais ou responsáveis legais, tais como a sexualidade e a identidade de gênero. Nesse sentido, a adoção de medidas que permitam a hiper vigilância dos pais ou responsáveis esbarra na necessidade de garantir a privacidade dessas pessoas. Além disso, as crianças e adolescentes devem ser informados quanto ao monitoramento realizado pelos pais de forma que elas entendam até que ponto o que fazem é ou não totalmente privado. Dito isso, é preciso que se entenda que o controle parental é o uso de ferramentas disponibilizadas pelo arquiteto da aplicação acessada por crianças e adolescentes para limitar e modelar a forma como essas pessoas utilizam essas aplicações. Esse tipo de controle inclui práticas como a possibilidade de configurar quantas horas as crianças e adolescente podem ficar conectadas à aplicação, um horário máximo na noite para o uso da aplicação, restrições de conteúdo e da possibilidade de realizar compras sem supervisão. Ademais, os pais e responsáveis devem ser adequadamente informados sobre o direito à privacidade dos seus filhos e sobre como podem regular a aplicação para garantir esse direito. Estamos falando aqui da boa-prática de conscientização dessas pessoas para que elas exerçam direitos em nome daqueles por quem são responsáveis.
","708772":"Atualmente, é necessário consolidar a necessidade de uma linguagem que seja acessível e lúdica para que consultar as informações não seja algo maçante, especialmente para crianças e adolescentes. Nesse sentido, em resumo, as práticas que entendemos ser mais adequadas para se comunicar com esse público são: (a) Adoção de storytelling para dar transparência à coleta e uso dos dados durante a jornada do usuário e aos caminhos disponíveis para ajustar as configurações de privacidade, isso inclui a criação de personagens e de um enredo que entretenha a criança e o adolescente; (b) A adoção de vídeos para repassar as informações que, incialmente seriam repassadas em formado de texto; (c) A

Adaptação da linguagem adotada pelo controlador à gírias e modo de falar que seja regional e conectado com o dia a dia do público infanto-juvenil que ele deseja atingir; (d) Adoção de avisos maiores (em tamanho aumentado) e sem privilégio ou destaque para opções que beneficiem somente o arquiteto da aplicação (nudges); (e) Adotar exemplos que os pais consigam utilizar para explicar como os dados de seus filhos são tratados se as crianças perguntarem ou se eles sentirem necessidade de explicar; (f) Impedir que a criança e adolescente mude alguma configuração de privacidade sem supervisão. ","708775":"n/a

Contribuinte: maraisa rosa cezarino

Número: OP-753148

Data: 16/08/2024 - 17:15

Resumo: :"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] A LGPD traz uma seção específica para abordar o Tratamento de Dados Pessoais de Crianças e Adolescentes (Capítulo II, Seção III), contudo, a seção não se destina inteiramente a ambos os públicos: enquanto o art. 14, caput, §2º e §6º, aborda, de maneira geral, o tratamento de crianças e adolescentes e o princípio do melhor interesse, o art. 14, §1º, §3º, §4º e §5º aborda o tratamento de dados apenas de crianças. Observa-se que há legislações e convenções internacionais que não fazem diferenciação explícita entre crianças e adolescentes, de forma que adentra a categorização desse público indivíduos com idade inferior a uma idade determinada, como 18 ou 21 anos, para efeitos legais. Contudo, no Brasil, essa distinção é válida e existente, uma vez que há, tal como previsto na LGPD, no ECA e no Código Civil, previsões legais específicas para cada faixa etária, conforme as necessidades e autonomia de cada uma. Essa previsão não é coincidente, mas consonante ao direito à liberdade, ao respeito e à autonomia desse público, previstos no art. 15 e 17 do ECA. Assim, é essencial que a ANPD se manifeste acerca da distinção entre as salvaguardas do tratamento de dados e do princípio do melhor interesse da criança e do adolescente, de forma a prever um balanceamento entre esse princípio e a autonomia pertencente ao desenvolvimento psicossocial de cada faixa etária. De igual modo, que a Autoridade se manifeste expressamente acerca da interpretação restritiva dos incisos §1º, §3º, §4º e §5º do art. 14 para o tratamento de dados de crianças, de forma a não serem estendidos hermeneuticamente para usuários entre 13 e 18 anos incompletos, uma vez que poderá trazer insegurança jurídica e violação à autonomia progressiva desses titulares de dados.","708725":"N/A.","705523":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] Na medida em que a LGPD prevê alguns critérios e parâmetros para a obtenção do consentimento do usuário, é salutar que esses mesmos critérios sejam utilizados para a obtenção do consentimento de pais ou responsáveis legais, quando relativo ao tratamento de dados de crianças e adolescentes, bem como as hipóteses de dispensa previstas na lei. Assim o consentimento de pais ou responsáveis legais deve ser manifestado de forma livre, informada, inequívoca e para finalidade determinada (art. 5º, XII, LGPD), por escrito ou outro meio que demonstre a manifestação de vontade dos pais ou do responsável legal (art. 8º, caput, LGPD), bem como deve poder ser revogado a qualquer

momento mediante manifestação expressa dos pais ou do responsável legal, por procedimento gratuito e facilitado (art. 8º, §5º, LGPD). Contudo, com relação ao vício do consentimento (art. 8º, §3º, LGPD), é necessário que haja especial atenção e especificidade com relação aos seus limites e abordagens, tendo em vista que a previsão foi elaborada para prever a obtenção do consentimento pelo próprio titular, e não para o tratamento de dados de criança ou adolescente por meio de um terceiro que não o próprio titular. Considere, por exemplo, que a plataforma digital é primeiramente acessada pela criança, para depois ser "verificada" pelos pais ou responsável legal, que pode optar por concordar ou não com o uso da plataforma pela criança. Caso a criança forneça o consentimento do tratamento de seus dados pessoais no lugar de seu pai ou responsável legal, não haverá vício de consentimento, mas a supressão de medidas de segurança que verifiquem a obtenção do consentimento apenas pelos pais ou responsáveis legais. Assim, o art. 8º, § 3º, da LGPD deve ser interpretado com reservas no caso do tratamento de dados pessoais de crianças e adolescentes.","708742":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] A despeito da ausência de consenso na sociedade civil acerca de quais medidas e mecanismos adotados pelo agente de tratamento seriam suficientes e eficazes para verificar que o consentimento foi fornecido devidamente pelos pais ou responsável legal, é necessário que seja pavimentado um entendimento claro: não há medida ou mecanismo 100% eficaz e absoluto para realizar essa verificação. Na medida em que é possível pensar em um mecanismo altamente eficaz e com pouquíssimas chances de falha na identificação da identidade do indivíduo, como por exemplo, a implementação de mecanismo de biometria facial na plataforma digital para a coleta de consentimento, por outro lado, tal medida demonstra-se conflitante no ponto de vista do princípio da necessidade e minimização de dados, diretamente ligado à redução de coleta de dados pessoais ao mínimo necessário. O uso de tal mecanismo torna-se ainda mais arriscado se considerar que crianças podem vir a utilizar a biometria facial na tentativa de burlar o sistema ou na incompreensão do seu funcionamento, o que poderia resultar na possível coleta de dados biométricos de um público altamente vulnerável. Da mesma forma, a possível coleta da biometria de crianças pode estar atrelada a riscos de violação aos seus direitos e garantias, podendo resultar, por exemplo, no 'perfilamento' e na criação de 'deep fakes' por agentes mal-intencionados. Por conta disso é que se faz primordial estabelecer parâmetros reais que possam ser devidamente seguidos pelas empresas e organizações, de forma a não causar dúvidas ou más interpretações, bem como o aumento dos riscos de violação aos direitos das crianças e dos adolescentes. Idealmente, a identificação do usuário sob "todos os esforços razoáveis" não deve prevalecer com relação ao princípio da minimização dos dados, sendo necessário o balanceamento entre medidas de menor coleta de dados, de um lado, e maior garantia de assertividade em relação à idade do indivíduo, do outro.","708745":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] Tal como explicitado anteriormente, é essencial que haja a interpretação restritiva dos incisos §1º, §3º, §4º e §5º do art. 14 da LGPD – que abordam a obrigatoriedade de obtenção do consentimento dos pais ou responsáveis legais – para o tratamento de dados somente de crianças de até 12 anos, de forma a não serem estendidos hermeneuticamente para usuários entre 13 e 18 anos incompletos, uma vez que poderá trazer insegurança jurídica e violação à autonomia progressiva desses titulares de

dados. É importante observar que muitos países com legislação de proteção de dados pessoais consolidada não definem a obrigatoriedade de obtenção do consentimento dos pais ou responsável legal a partir de uma determinada idade. Nessa linha, nos Estados Unidos, a Children's Online Privacy Protection Act (COPPA) estabelece previsões rigorosas acerca da coleta de dados pessoais de crianças menores de 13 anos, exigindo o consentimento dos pais. Contudo, a norma não abrange explicitamente adolescentes entre 13 e 18 anos, que, na maioria dos casos, podem fornecer seu próprio consentimento para o tratamento de seus dados pessoais. Por sua vez, no art. 8 (1)(2) da RGPD, a União Europeia orienta aos seus Estados-Membros a idade de 16 anos como padrão para a dispensa de consentimento dos pais ou responsável legal, porém, estabelece que os Estados-Membros podem dispor, em suas leis próprias, uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos. Assim, não há previsão, no RGPD, de qualquer necessidade de obtenção de consentimento dos pais ou responsável legal para o tratamento de dados de maiores de 16 anos. Por fim, o Data Protection Act 2018, que resulta da implementação do RGPD no Reino Unido, estabelece que o consentimento parental é necessário somente para crianças. Assim, adolescentes entre 13 e 16 anos podem fornecer seu próprio consentimento para o tratamento de dados em serviços online, considerando-se que possuem discernimento suficiente para entender as implicações do tratamento de seus dados pessoais. Entende-se que tais exemplos são suficientes, portanto, para refutar a necessidade de coleta de consentimento dos pais ou responsáveis legais de adolescentes entre 13 e 18 anos, uma vez que adolescentes nessa faixa etária já possuem, em grande medida, acesso a informações e tecnologias que lhes permitem avaliar as implicações do uso de seus dados, bem como tratá-los como incapazes de consentir poderia resultar em violação à sua autonomia, que deve ser considerada progressiva a partir desta idade. Tal medida, contudo, não representa a supressão dos direitos fundamentais e garantias dos titulares, bem como do princípio da boa-fé e do melhor interesse, que deverão ser igualmente observados.","705539":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] Para além do princípio do melhor interesse, expressamente indicado pela LGPD, deve ser previsto e incentivado o princípio da necessidade e minimização de dados, de forma que este se sobressaia a aquele quando na finalidade de verificação de idade do usuário ou de verificação do consentimento fornecido pelos pais ou responsável legal. Além disso, recomenda-se que as configurações padrão da plataforma sejam as mais protetivas possíveis em termos de privacidade e proteção de dados, garantindo que, por padrão, a coleta e o compartilhamento de dados sejam mínimos. É o caso, por exemplo, da implementação de medidas opt-out de privacidade, que podem ser removidas pelo usuário adolescente e pelos pais ou responsável legal da criança caso desejado. Assim, o usuário adolescente ou seus responsáveis podem gerenciar as informações pessoais coletadas, modificar consentimentos e preferências de privacidade ou excluir dados pessoais quando necessário. Isso, além de empoderar os usuários da plataforma, promove a responsabilidade e autonomia digital.","708762":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] Conforme anteriormente citado, entende-se que a prática de mecanismos de alta eficiência de verificação de identidade, como biometria facial, não são a melhor opção em virtude do alto risco para os direitos e garantias dos titulares crianças e adolescentes. Em face disso, considerando que não há mecanismos 100% eficazes

para garantir a verificação da identidade e/ou idade do usuário, o princípio do melhor interesse deve combinar-se ao princípio da boa-fé, no sentido de que a informação prestada pelo usuário é verdadeira. Não obstante, a este princípio podem ser incluídos mecanismos de verificação para garantir a melhor segurança do usuário, como a solicitação de data de nascimento, o fornecimento de aviso de privacidade infantil com informações claras acerca da verificação de identidade do usuário, e medidas mais restritas, como o condicionamento do uso do usuário à confirmação do pai ou responsável legal via e-mail, no caso do tratamento de dados pessoais de crianças. Cabe adicionar que, apesar da necessidade da adesão de mecanismos e boas práticas para a verificação de identidade do usuário, deve-se tomar cuidado para que tais mecanismos não sejam sobressalentes ao princípio da boa-fé somado aos esforços considerados razoáveis para a verificação da identidade do usuário, uma vez que o dever de requisição de idade pela organização não deve resultar em esforços desproporcionais ou que causem uma violação às garantias e direitos do titular de dados, bem como a sua liberdade e autonomia.","708764":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] A ANPD deve observar que a participação de crianças em jogos, aplicações de internet ou outras atividades em plataformas digitais devem ser protegidas, dentro de um esforço considerado razoável do risco de dark patterns, isto é, práticas de design de interface e experiência do usuário (UX) intencionalmente enganosas, que têm como finalidade manipular os usuários a tomar decisões que muitas vezes não são do seu interesse, mas que beneficiam a plataforma ou empresa. No contexto de tratamento de dados pessoais de crianças e adolescentes, dark patterns podem ser especialmente prejudiciais, uma vez que são mais vulneráveis e menos capazes de identificar as práticas manipulativas. É o caso, por exemplo, do aplicativo de jogo digital que condiciona o usuário a pagar uma quantia para poder obter mais benefícios, mas não é transparente quanto ao fato desse dinheiro ser real e não o dinheiro digital fornecido pelo jogo. Para isso, deve haver limitação para que essas informações sejam fornecidas ao usuário, bem como eventual pai ou responsável legal, de forma clara e específica, sem o uso de técnicas de ‘nudging’.","708768":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] Com relação à parâmetros e salvaguardas, é possível a aplicação de controles específicos, individualmente ou em conjunto, para assegurar um ambiente digital mais seguro às crianças e adolescentes, como a adição de ferramenta de controle parental, em que os pais ou responsáveis regulam o conteúdo acessado, compartilhado, recebido ou fornecido pela criança; a adição de filtros que bloqueiam conteúdos e publicidades sensíveis, discriminatórios, ofensivos ou inapropriados para menores de 18 anos, como palavrões, jogos de azar e casas de apostas, bem como palavras ou conteúdos específicos definidos pelos pais; a restrição do uso de chats em ambientes ‘sociais’, em especial em plataformas de redes sociais; a inclusão de mecanismos “age gates” adequados para impedir o acesso do usuário a páginas, serviços e conteúdos restritos; a restrição do recebimento de mensagens de texto ou conteúdos de mídia em perfis infantis por indivíduos desconhecidos. Há plataformas digitais que, além de adotar salvaguardas, verificam a necessidade de projetar uma versão específica de suas plataformas para atender a essa demanda. É o caso, por exemplo, do Youtube Kids. Nele, os pais ou responsável legal da criança têm autonomia para decidir quais controles de segurança quer utilizar, tais como a criação de perfis personalizados para a criança vinculados

à conta do responsável e sem o uso de foto pessoal, definir limitação de tempo de uso, bloquear canais e conteúdos específicos, acessar o histórico do conteúdo acessado e do mecanismo de busca, determinar a ausência de anúncios pagos ou de acesso a jogos ou conteúdo offline, entre outros. Além disso, disponibiliza política de privacidade voltada às crianças, que explica as práticas adotadas em linguagem mais acessível. Outras empresas que fornecem avisos de privacidade infantil são a Paramount, The Walt Disney Company, TikTok, Spotify, entre outras. Por sua vez, o Disney+, plataforma de conteúdo por streaming, também possui medidas que se inserem nos parâmetros a serem observados pelas organizações. Há o oferecimento de criação de perfis infantis, desenhados desde a concepção para operar com configurações de privacidade mais restritivas, com o bloqueio a conteúdos de mídia não recomendados para a faixa etária definida. A coleta de dados é minimizada e ajustada conforme a idade do usuário, especialmente em perfis infantis, nos quais dados comportamentais para fins de personalização não são coletados. Por fim, os pais ou responsáveis legais recebem informações claras acerca de como os dados dos perfis infantis são usados, tendo controle total acerca do acesso e histórico de conteúdo.","708772":"[Contribuição apresentada pelo Comitê de Privacidade do Movimento Inovação Digital - MID] Sugere-se que, para a obtenção do consentimento “específico e em destaque” dos pais ou responsáveis legais em plataformas voltadas para o público infantil ou infantojuvenil, a organização disponibilize, antes da realização do tratamento de dados, página com o fornecimento de informações sobre o tratamento de dados infantil em linguagem simples e voltadas às características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do público, como por exemplo, com o uso de figuras ilustrativas, quadros e personagens adequados, com orientação clara para que a criança ou adolescente forneça o dispositivo digital para seus pais ou responsáveis legais antes do uso próprio ou opção de botão para que o conteúdo seja compartilhado diretamente com o contato dos pais ou do responsável legal, que deverá ler e aceitar antes da plataforma ser desbloqueada para o uso.","708775":"N/A.

Contribuinte: Mariana Ramos Carlos de Campos Reis

Número: OP-753152

Data: 16/08/2024 - 17:22

Resumo: :"Para garantir uma aplicação uniforme do princípio do melhor interesse no tratamento de dados pessoais de crianças e adolescentes, sugerimos que a ANPD considere fornecer orientações ou elaborar regulamentações específicas sobre os seguintes pontos: a) Contextualização do termo melhor interesse: a ANPD pode fornecer uma definição mais detalhada e contextualizada do que constitui o "melhor interesse" no tratamento de dados pessoais de crianças e adolescentes, incluindo standards e exemplos práticos com situações específicas que ilustram a aplicação deste princípio. b) Consulta e participação dos titulares: diretrizes sobre a participação ativa de crianças e adolescentes, bem como de seus pais ou responsáveis, no processo decisório sobre o tratamento de seus dados pessoais. Isso inclui a apresentação de métodos de comunicação adaptados à idade e compreensão dos menores,

para que possam expressar seus interesses e preocupações. c) Atendimento e preservação dos direitos fundamentais das crianças e adolescentes: deve-se deixar claro que o princípio do melhor interesse deve ser balizado não apenas por uma conduta protetiva, mas também promocional, proativa, abrangendo a doutrina da proteção integral e a prioridade absoluta e garantindo o atendimento e a preservação dos direitos fundamentais das crianças e adolescentes em todas as fases do tratamento de seus dados pessoais. d) Medidas de segurança e minimização de dados: regras específicas sobre as medidas de segurança a serem adotadas no tratamento de dados pessoais de crianças e adolescentes, como privacidade by default, além de orientações sobre a minimização da coleta de dados, garantindo que apenas informações estritamente necessárias sejam coletadas e processadas. e) Ponderação de interesses: orientações sobre como equilibrar o princípio do melhor interesse com outros interesses legítimos, como em casos em que os melhores interesses de duas crianças individuais podem entrar em conflito, ou quando agir exclusivamente no melhor interesse de uma criança pode prejudicar os direitos de terceiros envolvidos. Essas orientações específicas são essenciais para proporcionar segurança jurídica aos agentes de tratamento, ao mesmo tempo em que protegem efetivamente os direitos das crianças e adolescentes, alinhando-se com os princípios fundamentais estabelecidos pela LGPD e normas internacionais de proteção de dados pessoais. ","708725":"Sim, abaixo elencamos contextos específicos que demandam atenção especial ao princípio do melhor interesse no tratamento de dados pessoais de crianças e adolescentes: a) Publicidade direcionada: o uso de dados pessoais para publicidade direcionada a crianças e adolescentes levanta preocupações sobre manipulação e impacto psicológico, sendo importante garantir que os interesses e direitos desse público sejam protegidos contra práticas que possam explorar sua maior vulnerabilidade. b) Serviços educacionais: plataformas que oferecem serviços educacionais devem assegurar que o tratamento de dados seja estritamente necessário para fornecer esses serviços, respeitando sempre o melhor interesse dos menores. c) Plataformas de interação on-line: o tratamento de dados pessoais de crianças em plataformas de interação que oferecem jogos on-line requer cuidado especial para evitar exposição indevida, proteger a privacidade e minimizar riscos de bullying, abuso ou manipulação. d) Saúde e bem-estar: o tratamento de dados pessoais relacionados à saúde de crianças e adolescentes, inclusive aqueles com necessidades específicas, deve ser feito com cuidado especial para proteger sua integridade física e psicológica, garantindo que apenas informações estritamente necessárias sejam tratadas e que a segurança dos dados seja mantida. e) Proteção contra abuso e exploração: dados pessoais de crianças e adolescentes utilizados em contextos nos quais há risco de abuso físico, emocional ou sexual devem ser tratados com máxima cautela, garantindo medidas robustas de segurança e privacidade para proteger sua segurança e bem-estar. f) Serviços institucionais: em situações em que a coleta de dados ocorre dentro de estruturas institucionais, como em serviços sociais ou de proteção à infância, é fundamental que o tratamento de dados respeite os direitos das crianças, evitando conflitos de interesse e assegurando que o benefício direto esteja claro e seja alcançado de maneira ética. g) Pesquisas e estudos acadêmicos: quando os dados pessoais de crianças e adolescentes são usados em pesquisas ou estudos acadêmicos, é essencial garantir que o compartilhamento de dados respeite o melhor interesse das crianças envolvidas, sendo as informações anonimizadas. ","705523":"Para garantir que esse

consentimento seja válido e em conformidade com a LGPD, devem ser observados os seguintes critérios e parâmetros: a) Clareza e transparência da informação: as informações devem ser apresentadas de forma clara, acessível e compreensível, utilizando linguagem simples e direta. É fundamental destacar todos os aspectos relevantes do tratamento de dados, incluindo a finalidade, a natureza dos dados coletados e o direito de revogação do consentimento. b) Especificidade do consentimento: o consentimento deve ser granular, permitindo que pais ou responsáveis legais consintam separadamente para cada tipo de tratamento de dados específico, evitando consentimentos genéricos, que podem vir a ser considerados nulos. c) Consentimento informado e destacado: é essencial que pais ou responsáveis legais compreendam plenamente o que estão consentindo, incluindo riscos e benefícios. Nesse sentido, o pedido de consentimento deve ser apresentado em formato facilmente visível, utilizando técnicas de design como fontes maiores e cores contrastantes para garantir destaque. Ferramentas adicionais, como vídeos e infográficos, podem ser utilizadas para melhorar a compreensão. d) Facilidade de revogação do consentimento: o processo para a revogação do consentimento deve ser simples e acessível, evitando procedimentos complexos que já foram alvo de sanções administrativas pelas Autoridades Europeias. e) Validação da identidade: procedimentos adequados devem ser implementados para verificar a identidade dos pais ou responsáveis legais, garantindo que o consentimento seja obtido de indivíduos devidamente autorizados. f) Registro e evidência do consentimento: devem ser mantidos registros detalhados do consentimento obtido, incluindo data, hora e o conteúdo exato do consentimento dado, para auditoria e inspeção pela ANPD se necessário, servindo como prova sobre o consentimento dado anteriormente. g) Manutenção e atualização do consentimento: é necessário manter os consentimentos sob revisão constante e atualizá-los sempre que os propósitos ou atividades evoluírem além do especificado originalmente. O consentimento não será considerado específico o suficiente se os detalhes mudarem. Dessa forma, mesmo que o novo propósito seja considerado compatível com o propósito original, isso não anula a necessidade de consentimento específico. Ao seguir esses critérios, os controladores podem assegurar que o consentimento obtido para o tratamento de dados pessoais de crianças seja específico e em destaque, em conformidade com os requisitos da LGPD. ","708742":"A LGPD estabelece que cabe ao controlador a adoção de todos os esforços razoáveis para garantir que o consentimento foi de fato fornecido pelos pais ou responsáveis da criança, considerando as tecnologias disponíveis. Inicialmente, é importante esclarecer o que seriam considerados ‘’esforços razoáveis’’, tendo em vista que essa definição pode variar a depender dos riscos inerentes ao tratamento de dados realizado. Segundo o Information Commissioner´s Office (ICO), se o tratamento de dados for de baixo risco, como o cadastro de uma criança para receber um boletim eletrônico, um “esforço razoável” pode ser a solicitação de uma declaração de consentimento e responsabilidade parental por meio de uma caixa de seleção ou confirmação por e-mail. No entanto, para tratamentos de dados de maior risco, como em plataformas onde crianças podem publicar dados pessoais em salas de bate-papo não monitoradas, métodos mais rigorosos são necessários. Nesses casos, o controlador deverá utilizar um método mais robusto para verificar a identidade da pessoa que reivindica a responsabilidade parental e confirmar o relacionamento com a criança. Nesse sentido, a depender do nível de risco da operação de

tratamento de dados em questão, as seguintes medidas de verificação podem ser implementadas: a) Autenticação multifator (MFA): implementar um sistema de autenticação multifator que exija que os pais ou responsáveis confirmem sua identidade através de múltiplos fatores, como senhas, códigos enviados via SMS ou e-mail e biometria. b) Verificação de documentos: solicitar o envio de documentos de identidade (como RG, CPF) dos pais ou responsáveis e utilizar tecnologias de reconhecimento ótico de caracteres (OCR) para verificar a autenticidade desses documentos. c) Formulários de consentimento digital: utilizar formulários de consentimento digitais que requerem a assinatura eletrônica dos pais ou responsáveis, podendo utilizar tecnologia de assinatura digital para garantir a validade legal. d) E-mail de confirmação: enviar um e-mail de confirmação para os pais ou responsáveis após o consentimento inicial, solicitando que eles cliquem em um link para confirmar a ação. e) Processo de revisão manual: em casos em que a tecnologia não possa confirmar a identidade de maneira automática, estabelecer um processo de revisão manual onde um operador humano verifica os documentos enviados. f) Histórico de consentimento: manter um registro detalhado de todos os consentimentos fornecidos, incluindo data, hora e método de verificação utilizado pode facilitar a identificação de consentimentos fornecidos pelos pais ou responsáveis pela criança. Por fim, é importante destacar que os mecanismos adotados devem coletar apenas os dados necessários para verificar a titularidade do consentimento recebido, e não impliquem em maiores riscos de privacidade aos titulares. É, portanto, necessário que esse processo também observe as seguintes medidas: (i) minimização dos dados coletados; (ii) utilização dos dados apenas para a finalidade de verificação da identidade do titular; (iii) retenção dos dados apenas pelo período adequado; e (iv) adoção de medidas de segurança para proteção dessas informações.
","708745":"Incialmente, é importante ressaltar que, na maioria das situações, não será necessário utilizar a base legal do consentimento para justificar o tratamento de dados pessoais de crianças e adolescentes. A ANPD, por meio do Enunciado nº 1/2023, destacou que o tratamento de dados pessoais de crianças e adolescentes pode ser realizado com base nas outras hipóteses legais previstas na LGPD, desde que observado e prevalecido o seu melhor interesse, a ser avaliado no caso concreto. Assim, não há obrigatoriedade de utilizar exclusivamente o consentimento como base legal, podendo-se recorrer a bases legais alternativas como o cumprimento de obrigação legal, o exercício regular de direitos em processo judicial, legítimo interesse, entre outras previstas na legislação. Nos casos específicos em que haverá a necessidade de obtenção do consentimento para o tratamento de dados pessoais de adolescentes, especialmente no ambiente digital, este não se limita exclusivamente às disposições do direito civil sobre capacidades civis, com a regra geral de representação e assistência por pais ou responsáveis. Embora haja controvérsia doutrinária sobre esse ponto, entende-se que o legislador criou, com a redação do art. 14, § 1º, da LGPD, uma “capacidade especial” para os adolescentes – entre 13 e 18 anos – no que se refere à manifestação de seu consentimento para o tratamento de seus dados pessoais. Vale ressaltar que há disposições no Código Civil (CC) e no Estatuto da Criança e do Adolescente (ECA) que valorizam a vontade dos menores em determinadas situações, conforme previsto nos art. 16, II; art. 28, §§1º e 2º; art. 100, XII; art. 111, V; e art. 161, §3º, do ECA e art. 1.740, III, CC. Esse entendimento é reforçado pelo Relatório da Comissão Especial Destinada a Proferir

Parecer ao Projeto de Lei 4.060/2012, que posteriormente deu origem à LGPD, o qual expressa que a exigência mais rigorosa de consentimento fica adstrita ao tratamento de dados de crianças. Essa orientação se alinha com a crescente autonomia conquistada pelos adolescentes nas plataformas on-line, sendo inegável o cenário fático atual, no qual o consentimento para o tratamento de dados tem sido efetuado por maiores de 12 anos. Nesse sentido, o legislador reconhece a prática, optando por considerar jurídica e legítima uma situação amplamente aceita socialmente. É importante, contudo, não confundir o consentimento para o tratamento dos dados pessoais dado pelo adolescente de forma livre, informada e inequívoca, com a celebração de negócios jurídicos, que ainda requerem a assistência ou a representação conforme previsto nos arts. 3º e 4º do Código Civil. Portanto, é possível considerar a autonomia progressiva dos adolescentes para fornecer consentimento ao tratamento de seus dados pessoais em determinados contextos e situações, desde que garantidos os princípios de informação adequada, respeito à vontade do titular e proteção de seu melhor interesse. ","705539":"A proteção de crianças e adolescentes no ambiente digital exige a adoção de medidas abrangentes e eficazes, com a primazia do melhor interesse desses indivíduos como princípio norteador. Todas as decisões e ações relacionadas ao tratamento de seus dados devem visar, primordialmente, o seu bem-estar e segurança. A seguir, são apresentadas as principais práticas e técnicas a serem observadas: a) Privacidade por design e por padrão: a privacidade deve ser intrínseca ao design das plataformas e serviços, com a implementação de mecanismos automáticos que a garantam desde a concepção e por padrão. As plataformas digitais devem ser projetadas com interfaces intuitivas e amigáveis, configurações de privacidade claras, personalizáveis, granulares e de fácil acesso, além de notificações transparentes sobre o uso de dados e sobre as implicações das escolhas dos usuários. As configurações padrão devem priorizar a privacidade, exigindo ação explícita do usuário para compartilhar informações adicionais. Sempre que possível, a anonimização dos dados deve ser implementada para proteger a identidade dos usuários. b) Transparência e clareza: informações sobre o tratamento de dados devem ser apresentadas de forma clara, concisa e acessível, utilizando linguagem adequada à faixa etária e recursos audiovisuais quando necessário, promovendo a compreensão e o controle dos usuários sobre seus próprios dados. c) Minimização e segurança dos dados: é imperativo limitar a coleta e o uso de dados ao mínimo necessário para fins específicos e legítimos, evitando o tratamento excessivo e desnecessário. A segurança e a integridade dos dados coletados devem ser asseguradas por medidas técnicas e organizacionais robustas, protegendo-os contra acessos não autorizados, perdas e vazamentos. d) Verificação eficaz de idade: mecanismos eficazes de verificação de idade, que restrinjam a coleta de dados ao estritamente necessário e evitem a coleta de dados pessoais sensíveis são essenciais. e) Controle parental: ferramentas que empoderem os pais a monitorar e controlar o acesso de seus filhos são indispensáveis para garantir um ambiente digital mais seguro. Ao mesmo tempo, deve ser dada à criança e ao adolescente informações adequadas sobre a atividade de monitoramento. f) Educação e conscientização: investir em educação e conscientização sobre privacidade e proteção de dados é fundamental para crianças, adolescentes, pais e responsáveis. g) Técnicas de incentivo: não utilizar técnicas de incentivo para induzir ou encorajar crianças a fornecer dados pessoais desnecessários ou enfraquecer ou desativar suas proteções de privacidade. h) Canais de comunicação: oferecer

canais de comunicação acessíveis e mecanismos de reclamação eficientes asseguram que todos tenham voz e possam exercer seus direitos de forma plena. ","708762":"Para garantir que o tratamento de dados pessoais se restrinja àqueles estritamente necessários para a finalidade pretendida, a verificação de idade de usuários de plataformas digitais deve ser conduzida de maneira eficiente e segura. Existem diversas boas práticas e técnicas disponíveis e adequadas para essa finalidade, visando equilibrar a necessidade de proteção de menores com a minimização da coleta de dados, entre as quais destacam-se: a) Transparência: os usuários devem ser claramente informados sobre a necessidade da verificação de idade, como ela será realizada e quais dados serão coletados. Políticas de privacidade claras e acessíveis são essenciais para imprimir confiança e garantir que os usuários estejam cientes de seus direitos. b) Minimização de dados: adotar métodos de verificação de idade que não exigem o fornecimento excessivo de informações pessoais. Isso pode incluir o uso de questionários que testem o conhecimento ou a compreensão de conteúdos que são típicos de determinadas faixas etárias, embora esses métodos possam não ser completamente precisos. c) Verificação com uso de inteligência artificial (IA): as plataformas podem implementar sistemas de verificação baseados em inteligência artificial para análise de características faciais, voz ou padrões de comportamento online e interação do usuário para inferir a faixa etária. d) Verificações documentais: solicitar o envio de cópias de documentos de identidade, acompanhada de medidas rigorosas de segurança para proteger os dados fornecidos. e) Autenticação de terceiros: a integração com serviços de autenticação de terceiros pode confirmar a idade do usuário sem que a plataforma acesse diretamente as informações pessoais, minimizando o risco de vazamento ou uso indevido de dados. Esta terceirização, frise-se, deve ser feita com parceiros que demonstrem altos padrões de proteção de dados. f) Reconhecimento óptico de caracteres (OCR): a análise de documentos com softwares de OCR e IA para verificar a idade é uma técnica segura e precisa, mas pode envolver o acesso a dados pessoais sensíveis. Para mitigar riscos, recomenda-se que a utilização de tecnologias de reconhecimento facial garanta que as imagens sejam processadas localmente, sem armazenamento, para proteger a privacidade dos usuários. O reconhecimento facial pode fornecer uma verificação rápida e precisa, desde que sejam adotadas práticas transparentes e seguras no tratamento dos dados. h) Anonimização e descarte dos dados: após a verificação dos documentos e dados pessoais, promover a anonimização ou descarte dos dados coletados, garantindo que não sejam utilizados para outras finalidades. i) Revisão e atualização periódica: as práticas de verificação de idade devem ser revisadas e atualizadas periodicamente, acompanhando novas tecnologias e regulamentações. Para aumentar a eficácia da verificação e proteger a privacidade dos usuários, as plataformas podem combinar diferentes técnicas e boas práticas. Essas práticas e técnicas, quando implementadas de maneira proporcional e adequada à finalidade da verificação e aos riscos envolvidos, garantem a proteção da privacidade e dos direitos dos usuários, especialmente das crianças e adolescentes. ","708764":"A coleta de dados pessoais de crianças e adolescentes por plataformas digitais deve observar as seguintes limitações específicas conforme o art. 14, § 4º e outros aspectos previstos na LGPD: a) Finalidade específica e adequação: os dados pessoais de crianças e adolescentes devem ser coletados somente para finalidades específicas, explícitas e legítimas. A finalidade da coleta deve estar claramente justificada e ser

diretamente relacionada à atividade que a criança está realizando na plataforma, sendo vedado qualquer uso adicional dos dados fora dessa finalidade específica. b) Minimização de dados: apenas os dados estritamente necessários para a finalidade específica do tratamento devem ser coletados. A coleta excessiva de dados, especialmente aqueles que não são essenciais para a finalidade declarada, deve ser evitada. c) Transparência e informação adequada: as plataformas devem fornecer informações claras, acessíveis e em linguagem apropriada para crianças e seus responsáveis sobre quais dados serão coletados, para que finalidade, como serão usados, além de definir claramente o procedimento para exercício de seus direitos. d) Proibição de condicionamento de participação: os controladores responsáveis por jogos, aplicações de internet ou outras atividades não devem condicionar a participação dos titulares ao fornecimento de informações pessoais além daquelas necessárias à atividade. Isso significa que a coleta de dados deve ser limitada ao mínimo necessário para que a criança possa participar da atividade oferecida. e) Retenção limitada: os dados pessoais devem ser mantidos apenas pelo período necessário para cumprir a finalidade para a qual foram coletados. Após o término desse período, os dados devem ser eliminados de forma segura, a menos que haja uma obrigação legal para retê-los por mais tempo. Sobre a questão da criação de perfil comportamental, cabe esclarecer que não há uma proibição do tratamento de dados pessoais de crianças e adolescentes para essa finalidade. Entretanto, se o agente de tratamento pretende usar os dados pessoais das crianças para fins de criação de perfil de crianças ou para tomar decisões automatizadas sobre elas, o ICO recomenda que seja elaborado um Relatório de Impacto de Proteção de Dados Pessoais (RIPD) para estabelecer se o tratamento resultará em um alto risco para seus direitos e liberdades. Ainda, cabe destacar que a criação de perfil comportamental pode ser utilizada para uma ampla gama de propósitos, por exemplo, para sugerir conteúdo aos usuários; para determinar onde, quando e com que frequência esse conteúdo deve ser sugerido; para incentivar os usuários a comportamentos específicos; ou para identificar usuários como pertencentes a grupos específicos. Além disso, essa forma de tratamento de dados também pode ser usada para ajudar a estabelecer ou estimar a idade de um usuário ou para proteção infantil, combate ao terrorismo ou prevenção de crimes. Dada a ampla gama de possíveis usos, é fundamental que a finalidade da formação de perfis comportamentais seja claramente definida, avaliando à luz do caso concreto os potenciais riscos e benefícios ao público jovem. Ponderar o melhor interesse da criança ou adolescente, definir claramente a finalidade da formação de perfis, restringir a coleta aos dados necessários e implementar fortes medidas de segurança são passos essenciais para proteger a privacidade e os direitos desses titulares vulneráveis. ","708768":"O controle parental em plataformas refere-se às ferramentas e configurações que permitem aos pais ou responsáveis monitorar e controlar a atividade on-line de crianças e adolescentes, especialmente no que diz respeito à privacidade e segurança. Para ampliar e fortalecer o controle parental, recomenda-se a adoção dos mecanismos e boas práticas expressos a seguir: a) Configurações de privacidade simplificadas: desenvolver interfaces simples e intuitivas que permitam aos pais ajustar facilmente as configurações de privacidade e controle parental nas plataformas digitais. b) Ferramentas de controle parental avançadas: implementar e aprimorar ferramentas de controle parental que permitam restrições de conteúdo adequadas à idade, limitações de tempo de uso da plataforma e monitoramento de

atividades sem invadir a privacidade excessivamente. c) Participação ativa dos pais: incentivar e facilitar a participação ativa dos pais na supervisão das atividades on-line de seus filhos, encorajando o diálogo aberto sobre segurança digital e comportamento on-line responsável. d) Educação contínua: promover campanhas educativas para pais, responsáveis e crianças sobre a importância da proteção de dados pessoais e privacidade on-line, além de capacitar os pais para entenderem as configurações de privacidade e controle parental disponíveis nas plataformas digitais. Ainda que seja de importância o controle parental, deve-se compreender que nessa equação, há ainda um elemento primordial a ser considerado: a privacidade da criança e do adolescente. Nesse sentido, é fundamental que haja transparência sobre os controles parentais realizados. Caso uma plataforma permita, por exemplo, o monitoramento ou rastreamento parental de uma criança ou adolescente, é necessário oferecer explicações claras e adequadas à idade sobre esses recursos, garantindo que os jovens compreendam e sejam informados sobre quando sua atividade está sendo monitorada ou sua localização rastreada. Nesse sentido, cabe analisar a tabela com orientações sobre o tipo de informação que pode ser fornecida e como você fornecê-la ao público mais jovem, levando em consideração a faixa etária do usuário, disponibilizada pelo Information Commissioner´s Office no "Age appropriate design: a code of practice for online services", disponível no link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/11-parental-controls/. Por fim, promover um ambiente digital seguro inclui não apenas o controle parental eficaz, mas também o desenvolvimento de autonomia e habilidades de tomada de decisão segura na internet à medida que os jovens crescem. Isso envolve educá-las sobre a importância da privacidade, ensinando-as a proteger suas informações pessoais e a se comportar de maneira ética on-line. ","708772":"No contexto de plataformas utilizadas por crianças e adolescentes, é fundamental garantir que as informações de privacidade sejam claras, precisas, facilmente acessíveis e adequadas às idades dos usuários, permitindo que compreendam como seus dados pessoais estão sendo tratados. Com base no guia elaborado pelo Information Commissioner´s Office intutulado "Designing data transparency for children: Insights from the Children's Code transparency champions open call" (link: https://ico.org.uk/media/for-organisations/documents/2620177/designing-data-transparency-for-children.pdf), são consideradas boas práticas: a) Utilizar formatos criativos: ícones, vídeos e desenhos animados podem ser ferramentas eficazes para chamar a atenção das crianças a respeito das informações de privacidade. A título de exemplo, deve-se buscar substituir o formato escrito tradicional dos Termos e Condições de Uso e Política de Privacidade por projeções interativas que possam transmitir as informações, incluindo histórias em quadrinhos, vídeos, jogos e personagens relacionados ao tema de privacidade. b) Necessidades das crianças no centro do design: é importante envolver os menores em todas as fases de desenvolvimento do design para garantir que o serviço atenda às suas necessidades e aos seus melhores interesses. Caso isso não seja viável, é essencial obter uma compreensão mais profunda sobre as necessidades das crianças e considerá-las no momento de criação do design dos jogos. O foco é utilizar evidências e feedback direto das crianças para informar e melhorar práticas de design, promovendo transparência em conformidade com a LGPD. c) Considerar as

limitações dos responsáveis e das crianças: ser realista quanto aos níveis médios de letramento em dados de crianças e pais, fornecendo recursos adequados para ajudá-los quando não entenderem as informações de privacidade. Ao incluir, por exemplo, a opção “Não entendo” em seu design, através de uma abordagem simples, pode-se de forma eficaz testar a experiência do usuário; entender os níveis gerais de alfabetização dos usuários infantis; e disponibilizar um caminho para que solicitem informações mais ou menos complexas. d) Separar as informações de privacidade: evitar condensar todas as informações de privacidade em apenas um único local, sendo preferível uma apresentação direcionada e em locais relevantes e necessários para que efetivamente ocorra o engajamento das crianças. e) Criar espaços para conversas entre as crianças e os responsáveis: ao invés de apenas inserir caixas de seleção para obter o consentimento dos responsáveis, é preferível projetar recursos de apoio e oportunidades para que os responsáveis e as crianças possam discutir as informações de privacidade em conjunto. Deve haver, portanto, projetos que foquem mais na criação de um espaço para um diálogo genuíno entre eles e as crianças do que somente na obtenção de consentimento dos pais. f) A eficácia é fundamental: além de tornar a transparência eficaz desde a concepção do design, é necessário garantir que as crianças interajam com ela, através da inserção da privacidade em toda a jornada de utilização da plataforma. A título de exemplo, além de ter um portal com documentos de linguagem e design adequados ao público, deve-se facilitar a sua localização, abordando o tema de privacidade ao longo da jornada de uso da plataforma. De forma a assegurar a efetividade das medidas expostas acima, é recomendável a realização de pesquisas e testes de usabilidade com os usuários para garantir que as configurações de privacidade, a linguagem e as funcionalidades da plataforma sejam compreensíveis e adequadas para esse público, assegurando que interpretação dos materiais e recursos utilizados não conduzam inadvertidamente a interpretações equivocadas. Adotar essas práticas promove um ambiente digital mais seguro para crianças e adolescentes, além de reforçar a confiança dos usuários na plataforma, respeitando os princípios fundamentais de proteção de dados e privacidade. ","708775":"Não há outras sugestões.

Contribuinte: GABRIELA RIBEIRO GOMES SOTOMAYOR

Número: OP-753151

Data: 16/08/2024 - 17:24

Resumo: :"O Comitê dos Direitos da Criança da ONU propõe a observância de uma lista não exaustiva de parâmetros que possam ser utilizados para avaliação do melhor interesse do menor quando da necessidade de regulamentação ou criação de legislação a respeito do tema, de modo a garantir o pleno e efetivo gozo dos direitos reconhecidos na Convenção sobre os Direitos da Criança da ONU, elencando os seguintes aspectos a serem observados: a) opinião da criança; b) identidade da criança; c) preservação do ambiente familiar e manutenção de relações; d) cuidados, proteção e segurança da criança; e) situação de vulnerabilidade; f) direito da criança à saúde; g) direito da criança à educação. É evidente que, além de manter em vista parâmetros orientadores, é crucial considerar as peculiaridades de cada caso

concreto. Segundo o Comitê, as circunstâncias específicas se relacionam com as características específicas das crianças envolvidas, tais como, a idade, o sexo, o nível de maturidade, a experiência, a pertença a um grupo minoritário, a existência de uma deficiência física, sensorial ou intelectual, ou o contexto social e cultural em que a criança se encontra inserida. Outra questão intimamente ligada ao princípio do melhor interesse, refere-se à necessidade de estabelecer diretrizes para que as organizações assegurem a transparência no tratamento de seus dados, de modo que esses grupos compreendam claramente como seus dados serão utilizados. De acordo com o entendimento do ICO - Information Commissioner's Office, é crucial que o tratamento dos dados pessoais de crianças seja em linguagem adequada e possibilite a compreensão do menor, de modo a assegurar um tratamento igualitário, promovendo controle e escolha individuais. A autoridade ainda recomenda que sejam redigidas informações de maneira concisa, clara e adequada, adaptando-se versões distintas ao grupo etário específico. É igualmente importante definir diretrizes para que desenvolvedores de serviços online, assegurem o princípio do melhor interesse ao tratar de dados pessoais de crianças e adolescentes. A respeito do tema, o ICO, destacou no Código da Criança, um conjunto de 15 princípios que os provedores de serviço online devem seguir para salvaguardas de dados de crianças e adolescentes. No mesmo sentido, a CNIL - Commission Nationale de l'informatique et des Libertés publicou 8 recomendações para aumentar a proteção das crianças online. A AEPD- La Agencia Española de Protección de Datos, também já divulgou documento que contempla ações prioritárias para promover a proteção das crianças e adolescentes no uso da internet. Adicionalmente, os arts. 3º e 6º do ECA disciplinam, respectivamente, sobre o princípio do melhor interesse, cuja finalidade é a proteção de forma integral e com absoluta prioridade dos direitos fundamentais de crianças e adolescentes e que na interpretação daquela lei, deve-se levar em conta os fins sociais e a condição peculiar dessa categoria de titulares, como pessoas em desenvolvimento. Embora tenham sido discutidos alguns aspectos que necessitam de regulamentação específica pela ANPD, é essencial considerar outros pontos relevantes conforme supracitado. Sendo, portanto, fundamental que a ANPD estabeleça diretrizes claras para orientar a sociedade e organizações no tratamento de dados de crianças e adolescentes. Isso inclui fornecer orientações práticas sobre a aplicação do princípio do melhor interesse, assegurando a proteção adequada dos dados pessoais da categoria vulnerável de titulares. Além disso, é crucial desenvolver materiais educativos e oferecer orientações para pais e responsáveis abrangendo uma variedade de temas, elucidando cenários de aplicação da preservação do melhor interesse do menor, visando assegurar os direitos fundamentais da criança e do adolescente, considerando o art. 227 da Constituição Federal e nos arts. 3º e 6º do ECA. ","708725":"Existe uma linha de atuação das Varas da Infância que define que a aplicação do melhor interesse da criança e do adolescente está relacionada ao seu bem-estar físico, emocional e social. Logo, não podemos também impor um modelo que o isole do mundo, que o distancie da realidade e do contexto digital e tecnológico que faz parte da sua vida com a sociedade, para ser, estar e pertencer. Deve-se sim ter mecanismos de proteção, prestação de auxílio, socorro, vigilância, supervisão e principalmente, educação, para formar as habilidades necessárias para o uso ético, seguro e responsável, essa, inclusive, é um dos principais raciocínios abordados pelo Instituto Peck de Cidadania Digital

(https://ipcd.org.br/), organização sem fins lucrativos que tem como missão educar as famílias brasileiras, promovendo a Ética e Segurança Digital e contribuindo para a construção de um ambiente digital sustentável. É fundamental que a ANPD estabeleça orientações acerca do melhor interesse de crianças e adolescentes, sobretudo no tratamento de informações pessoais online de crianças nas plataformas digitais (como exemplo: Facebook, Instagram, Tik Tok e similares), que buscam comercializar algum tipo de serviço ou produto direcionado para esse público. Nesse sentido, a ANPD deve estabelecer parâmetros claros, que orientem as organizações em relação ao tratamento de informações para um site ou serviço online, a exemplo da Lei de Proteção da Privacidade Online das Crianças (COPPA), criada pela Comissão Federal de Comércio nos Estados Unidos (FTC), que traz diretrizes sobre triagem etária de usuários, situações em que deverá haver o bloqueio total da participação de crianças ou a necessidade de se obter o consentimento parental verificável em casos em que crianças façam o uso da plataforma, por exemplo.. No que se refere ao tratamento de dados pessoais de crianças e adolescentes para fins de marketing, para que as organizações desenvolvam campanhas direcionadas a esses públicos, é crucial estabelecer medidas de proteção prévias, principalmente às crianças que são particularmente vulneráveis a abusos por parte de profissionais de marketing e podem não entender os impactos de segurança e privacidade que envolve o tratamento de seus dados pessoais. Isso visa garantir que os dados pessoais dos menores não sejam utilizados de modo que não observe o melhor interesse. Segundo o ICO, é essencial proporcionar proteção específica às crianças e adolescentes durante o tratamento de seus dados, considerando sua capacidade limitada de compreender as finalidades do processamento e as possíveis consequências envolvidas. No que tange à proteção das crianças e adolescentes no ambiente online, embora exista um projeto de lei (PL 2.628/2022) em tramitação no Brasil, propondo a proibição de criação de contas para menores de 12 anos, a vedação de publicidade infantil e a exigência de mecanismos de verificação de idade pelos provedores de serviços online, é essencial, para que esses parâmetros de verificação sejam previamente estabelecidos e padronizados pela ANPD, de modo que os provedores possam cumprir as determinações sem divergências significativas. A respeito desse tema, no âmbito internacional, são estudadas diferentes abordagens de verificação de idade, tais como, autodeclaração, uso de documentos oficiais e métodos de cascada. As principais recomendações do ICO nesses casos, se referem a assegurar à conformidade com a Lei, avaliar riscos de proteção de dados e basear-se em boas práticas de transparência e minimização de dados, bem como limitação da finalidade. Adicionalmente, a COPPA, por exemplo, traz recomendações para as organizações em relação a triagem de idade para os usuários, por meio de tela de idade, em que o sistema permite que o usuário insira livremente o mês e ano de nascimento e adoção de cookies, para evitar que a crianças pressionem o botão de voltar para inserir uma idade diferente. É fundamental conscientizar esse público, produzir materiais interativos sobre privacidade infantil, que incentivem a participação do usuário, facilitando a exploração de conteúdos de forma a promover engajamento e compreensão clara e acessível.","705523":"A informação sobre o tratamento deve ser apresentada de maneira acessível, em linguagem simples e facilmente compreensível tanto pelo menor, quanto pelo responsável. Recomenda-se, na mesma linha de atuação da ICO - Information Commissioner's Office, que para o

consentimento parental específico é necessário que o campo em que o titular ou o responsável possa atuar de forma afirmativa para consentir pelo tratamento de dados apresente as seguintes informações: identidade do controlador, as finalidades e as atividades do tratamento e o direito de revogar o consentimento. O consentimento deve ser obtido antes de coletar as informações do menor e deve ser destacado no contexto em que é solicitado. Isso significa que ele não deve ser abordado de forma genérica, com outros termos e condições de forma a se perder entre outras informações. Deve estar granularizado de outras autorizações ou consentimentos, de modo que sua importância e significado sejam evidentes e não possam ser inadvertidamente ignorados. Por fim, recomenda-se que ANPD busque orientar as instituições com exemplos de métodos não exaustivos que possibilitem a obtenção do consentimento parental verificável, e que assegurem que a pessoa que fornece o consentimento seja realmente o responsável pelo menor. Importante, no entanto, que a ANPD forneça recomendações de forma a assegurar a experiência do usuário – por exemplo, desenvolvendo informações em camadas amigáveis e consentimentos just-in-time, incluindo a concessão de opções de consentimentos granulares para diferentes tipos de tratamentos. ","708742":"Para assegurar a autenticidade e a validade do consentimento fornecido, podem ser utilizadas tecnologias como assinaturas eletrônicas, identificação por meio de login seguro com autenticação de dois fatores ou outras técnicas de verificação de identidade. Essas medidas ajudam a confirmar que o consentimento foi dado pelo titular dos dados ou por seu representante legal de forma legítima. Além disso, é recomendável o uso de registros de consentimento digitalmente seguros e auditáveis, que permitam rastrear quando e como o consentimento foi obtido. Isso inclui registrar detalhes como a data, a hora, o método de obtenção do consentimento e quaisquer informações relevantes que demonstrem conformidade com a LGPD. Para facilitar a verificação de consentimento pelos pais ou responsáveis, os controladores podem oferecer ferramentas e interfaces que permitam revisar, modificar ou retirar o consentimento a qualquer momento de maneira simples e direta. Essas opções devem ser claramente indicadas e acessíveis dentro da plataforma digital. Podendo ser tido como parâmetro o entendimento da Federal Trade Commission (FTC), órgão responsável pela regulamentação do COPPA (Children's Online Privacy Protection Act), que estabeleceu alguns mecanismos para a obtenção do que eles denominaram "consentimento parental". Essas medidas incluem: a notificação do titular do cartão de crédito/débito vinculado ao dispositivo utilizado para o cadastro ou compra on-line, fornecimento de número de telefone para que o responsável possa ligar gratuitamente para um central e conceder o consentimento, a coleta do consentimento do responsável via videoconferência; dentre outros mecanismos.","708745":"Desde o Relatório da Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei 4.060/2012, que posteriormente deu ensejo à Lei Geral de Proteção de Dados Pessoais (LGPD), o entendimento vinha no sentido de que a exigência do consentimento parental deve ficar restrita ao tratamento de dados de crianças. Contudo, importante que a interpretação da LGPD esteja em harmonia com o ordenamento jurídico brasileiro, no caso, o Código Civil vigente. Ocorre que, nos termos do art. 2º do Estatuto da Criança e do Adolescente – ECA, considera-se adolescente, a pessoa entre 12 e 18 anos de idade. E que, nos termos do Código Civil brasileiro, os absolutamente incapazes (pessoa até 16 anos) deve ser representado pelo responsável para os atos da vida civil, enquanto os

relativamente incapazes (pessoa entre 16 e 18 anos) deve ser assistido para a prática de ato ou negócio jurídico. Nesse sentido, em consonância com as referidas legislações, recomenda-se que a ANPD firme entendimento de que, especialmente no ambiente digital, a obtenção do consentimento deve observar as disposições do direito civil a respeito das capacidades civis, bem como o ECA. Assim, em determinadas situações em que o consentimento seja a base legal aplicável (lembrando que pelo Enunciado CD/ANPD nº 1/2023 o tratamento poderá ser realizado com base nas hipóteses tanto do art. 7º quanto do 11 da LGPD), o adolescente entre 12 e 16 anos, por ser absolutamente incapaz, deve ser representado pelos pais ou responsáveis e o adolescente entre 16 e 18 anos, por ser relativamente incapaz, deverá ser assistido pelos pais ou responsáveis. Vale ressaltar, no entanto, que ainda que as disposições do Código Civil e do ECA sejam observadas, o requisito adicional do princípio do melhor interesse deverá prevalecer, sendo critério fundamental para avaliação de operações de tratamento envolvendo esses titulares, conforme determina o art. 14 da LGPD. ","705539":"Com foco no melhor interesse das crianças e dos adolescentes e com vista na proteção de dados pessoais, é imprescindível que sejam observados uma série de princípios postulados na LGPD, além da tríplice já especificada nesta tomada de subsídio (finalidade, adequação e necessidade). A transparência (ao titular e aos pais e/ou responsáveis legais) é essencial, devendo ainda ser considerada a faixa etária do público-alvo a qual a plataforma pretende alcançar, para definição de como as informações serão fornecidas, já que deve haver uma preocupação do controlador em relação à compreensão desses titulares que, em decorrência da natural falta de maturidade, nível de conhecimento e até mesmo certas limitações, merecem um tratamento mais cauteloso. O uso de recursos audiovisuais, como vídeo resumo do aviso de privacidade com reprodução obrigatória para utilização da plataforma, por exemplo, ou métodos interativos como a gamificação podem ser considerados excelentes opções para fornecer as informações sobre o tratamento dos dados desses titulares em desenvolvimento. O princípio da não discriminação assume um papel essencial – e de certa forma, ambíguo - nesta discussão. Ao passo que os dados pessoais não possam ser tratados de forma discriminatória, a exclusão digital também deve ser evitada, uma vez que não participar destes movimentos tecnológicos pode gerar uma discriminação no meio em que as crianças e adolescentes estão inseridos. Plataformas digitais que podem tratar dados de crianças e adolescentes, mesmo estipulando que menores de 18 anos não deveriam se registrar, devem aumentar o seu nível de segurança diante a presença de titulares de categorias especiais. Assim, destacam-se os princípios da segurança e da prevenção, que estão relacionados às medidas técnicas e administrativas que são adotadas pelo controlador para proteger os dados tratados e prevenir a ocorrência de danos. Como medida de segurança, destacam-se os meios de verificação da faixa etária do usuário, bem como obtenção do consentimento parental, nos casos em que seja necessário. É fundamental que estas plataformas e aplicações busquem métodos eficazes para triagem da idade do usuário. Entretanto, deve-se considerar a intenção do legislador quando da definição dos parâmetros e salvaguardas que serão adotados pelas plataformas digitais. O art.14 da LGPD, ao especificar que o tratamento de dados de crianças (excluindo os adolescentes desta determinação) somente poderá ser tratado mediante o consentimento dos pais e responsáveis, assim o fez por uma razão. Nessa linha, a General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, artigo 8.º, item 1,

apresenta a obrigatoriedade de se obter o consentimento dos pais ou responsáveis para o tratamento dos dados de crianças e adolescentes com idade menor à 16 (dezesseis) anos, autorizando, entretanto, os Estados-Membros a fixarem limite inferior, restrito a 13 (treze) anos de idade. Ainda que as crianças devam ser tratadas de modo diferente dos adolescentes, considerando o nível de maturidade de cada um destes grupos, bem como a interação com a sociedade por meio do ambiente digital, ambas merecem o respeito a privacidade e que seus dados pessoais sejam protegidos e tratados sempre em seu melhor interesse. Nesse sentido, importante que a ANPD dispõe de medidas como, por exemplo, (i) vinculação da conta da criança e do adolescente ao perfil dos pais/responsáveis legais; (ii) impossibilidade de manter o perfil aberto ao público; (iii) adoção de um "chip kids" no celular de menor de idade (recomendável ou obrigatório pelo menos para condição de criança, como já ocorre em outros países), (iv) canal de socorro ("apito digital") para atender de forma diferenciada, mais célere, com colaboração com autoridades, ocorrências envolvendo menores de idade e (ivii) outras medidas fortes de verificação de idade são salvaguardas que podem ser adotadas a fim de conferir maior proteção às crianças e adolescentes. As medidas protetivas devem ser redobradas quando se trata de dados pessoais circulando em redes sociais. Isto pois as informações ali inseridas não são tratadas apenas pelo controlador.","708762":"É fundamental que estas plataformas e aplicações busquem métodos eficazes para triagem da idade do usuário. A confirmação poderá ser: (i) auto declaratória, permitindo com que o usuário forneça livremente o mês e o ano de nascimento, adotando-se adicionalmente meios técnicos para impedir a alteração da idade após tentativa frustrada de acesso; (ii) pelos pais ou responsáveis, com a confirmação de idade de dependentes por usuário titular, quando for o caso; ou (iii) se aplicável, mediante a exigência de apresentação de documento oficial de identificação do menor e do responsável legal. Além disso, como boa prática, é importante que o controlador evite encorajar crianças a falsificar suas informações de idade, como por exemplo afirmando que menores de idade não podem participar ou devem obter autorização antes dos pais para participar. Adicionalmente, incluir uma caixa de seleção para que o usuário indique que não é criança ou adolescente, também não é recomendável. Ademais, a criação de perfis infantis em aplicativos de jogos e redes sociais, por exemplo, vinculados aos perfis dos pais e responsáveis é uma medida que pode ser adotada pelos agentes de tratamento como forma de proteção dos dados pessoais. ","708764":"O controlador que coleta dados de crianças por plataformas digitais, deve observar as seguintes limitações: Examinar cuidadosamente os dados pessoais que pretende tratar desse público, de modo que realize a coleta em conexão com cada atividade que oferece, de modo a assegurar que está coletando somente as informações estritamente necessárias para participar de determinada atividade, em observância ao princípio da necessidade e finalidade; Em observância à Resolução nº 245 do Conanda (Conselho Nacional dos Direitos da Criança e do Adolescente), o controlador não deve tratar dados de crianças e adolescente para fins comerciais, como criação e definição de perfis comportamentais, de consumo e segmentação mercadológica, tampouco para direcionamento de publicidade ou ampliação de seu alcance; Ainda em observância à Resolução nº 245 do Conanda, o controlador não deve utilizar qualquer mecanismo de vigilância e monitoramento digital de crianças e adolescentes associado a ferramentas de automação e tratamento de dados pessoais; Adotar mecanismos

para triagem etária e, caso o controlador identifique que um usuário é uma criança, que adote o fluxo de obtenção da representação parental; Divulgar claramente suas práticas de coleta, uso e tratamento dos dados pessoais da criança em sua Política de Privacidade, para que os pais ou responsáveis possam tomar uma decisão informada sobre a participação da criança na plataforma digital. Aliás, em breve análise do cenário internacional, destacamos a norma Age Appropriate Design Code formulada pela Information Commissioner's Office (ICO) que possui seis pilares: (i) o melhor interesse da criança deve ser uma consideração primária ao projetar e desenvolver serviços online; (ii) altos níveis de privacidade devem ser definidos por padrão; (iii) apenas uma quantidade mínima de dados pessoais deve ser coletada e mantida; (iv) os dados das crianças não devem ser compartilhados, a menos que haja uma razão convincente para fazê-lo; (v) os dados pessoais das crianças não devem ser usados de maneiras que possam ser prejudiciais ao seu bem-estar; (iv) a geolocalização deve ser desligada por padrão.","708768":"Para ampliar o controle dos pais ou responsáveis, os controladores devem adotar mecanismos que: Permita filtrar/limitar o acesso de crianças e adolescentes a determinados sites, palavras e imagens específicas; Impossibilite que a criança ou adolescente compartilhe informações pessoais; Permita que os pais ou responsáveis limitem o tempo de uso da plataforma digital, por meio de configurações de horário e dia para acesso; Disponibilizar funcionalidades para que os pais ou responsáveis monitorem as atividades online, permitindo a visibilidade de quais sites a criança ou adolescente acessou. Vale ressaltar que, Nnono Reino Unido, o assunto foi regulamentado pela Information Commissioner's Office (ICO), que, dentre outras iniciativas, desenvolveu um Código de Boas Práticas para a prestação de serviços online para crianças. O Código aborda questões relacionadas a controle parental, sendo certo que, se o serviço online permitir que um pai ou responsável monitore a atividade online de seu filho ou rastreie sua localização, a plataforma deve fornecer um aviso claro para a criança durante o período do monitoramento. Isto porque as ferramentas de controle parental, por um lado, auxiliam pais (e responsáveis) na promoção e defesa do melhor interesse de seus filhos, mas, por outro, podem inclusive impactar na privacidade destes, cuja expectativa se amplia à medida do seu crescimento, e que está intrinsecamente relacionado ao desenvolvimento do senso próprio de identidade e da sua intimidade. ","708772":"A transparência deve ser abrangente em todos os estágios: as informações devem ser apresentadas de maneira clara e acessível, considerando o desenvolvimento das crianças conforme tornam-se maduras. A transparência deve estar diretamente vinculada ao princípio da conscientização e ao respeito à autonomia dos menores, adaptado à medida de sua capacidade. Nesse contexto, é relevante promover uma "alfabetização digital" para pais e responsáveis, direcionando, cada vez mais, para uma interação com os menores, estimulando uma crescente consciência das implicações do ambiente digital. Neste sentido, a ICO e as Nações Unidas incentivam a construção de aplicações "child friendly", que facilitem o acesso ao direito dessa categoria de titulares, incentivando o seu exercício e a sua compreensão, especialmente diante de decisões automatizadas e no uso de Inteligência Artificial, razão pela qual, as Nações Unidas defendem a inclusão de crianças e adolescentes no processo de desenvolvimento, compreendendo suas necessidades e estabelecendo as devidas salvaguardas. A Data Protection Commission (DPC – autoridade de proteção de dados da Irlanda) também traz o

conceito como “child-oriented transparency”, sublinhando a importância crucial do design na implementação de padrões rigorosos de proteção, os quais devem ser incorporados como padrão em todo o processo. Cabe destaque ao Código de Boas Práticas para a prestação de serviços online para crianças , desenvolvido pela Information Commissioner’s Office (ICO), que exige que (i) as configurações sejam de “alta privacidade” por padrão, a menos que haja um motivo convincente para não fazê-lo; (ii) as medidas de transparência e informações de privacidade fornecidas aos usuários em políticas ou outros documentos sejam concisos e em linguagem clara, adequada à idade da criança, além de fornecer explicações adicionais específicas sobre como dados pessoais são usados no momento em que o uso é ativado; (iii) os dados das crianças não sejam compartilhados como regra, salvo se a organização mostrar uma razão convincente para fazê-lo; (iv) os serviços de geolocalização sejam desativados por padrão, além de fornecer um sinal claro de que a geolocalização está ativa quando for necessário coletar; (v) as empresas desenvolvam avaliações de impacto da proteção de dados para identificar e mitigar os riscos aos direitos e liberdades das crianças, considerando as diferentes idades, capacidades e necessidades de desenvolvimento. Por fim, entendemos que, além de adotar um nível de proteção e respeitar os princípios, padrões e regras estabelecidos pelas legislações de proteção de dados aplicáveis, recomendável uma abordagem prática e eficaz voltada para esse público específico, sendo necessário adaptar produtos e serviços à nova realidade de proteção de dados pessoais e promover uma atuação multissetorial em prol de critérios como segurança, responsabilidade, transparência e privacidade.","708775":"Importantes que as questões abaixo relacionadas ao tratamento de dados pessoais de crianças e adolescentes sejam melhor esclarecidas pela ANPD: Distinção entre o consentimento do art. 14 e as regulamentações de saúde e pesquisas clínicas aplicáveis; Tratamento de dados de crianças e adolescentes em redes sociais.

Contribuinte: GABRIEL HERINGER ZIGONI OLIVEIRA

Número: OP-753174

Data: 16/08/2024 - 17:42

Resumo: :"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO) O En. CD/ANPD nº 01/23 deixa claro que a verificação do melhor interesse da criança e do adolescente depende de uma avaliação de cada caso concreto, não sendo possível estabelecer, de antemão, requisitos excessivamente pormenorizados a serem atendidos em toda e qualquer atividade de tratamento. No mesmo sentido, o Comentário Geral nº 14, de 2013, do Comitê de Direitos da Criança da ONU, afirma que o “interesse maior” da criança abrange (i) um direito, (ii) um princípio jurídico fundamental interpretativo e (iii) uma regra processual. Nota-se a existência de uma tomada de decisão diante de situações concretas, a partir de um exercício de interpretação balizado por regras que evitem abusos, protegendo os diretos das crianças e adolescentes, sem, contudo, que se considere a criação de um arcabouço regulatório minucioso e exaustivo. Tal abordagem revela-se equilibrada, na medida em que dá contornos concretos ao conceito, ou, em verdade, ao princípio do melhor interesse, segundo o qual se deve proteger o menor; sem,

porém, impedi-lo de participar da vida em sociedade e desfrutar, com isto, de oportunidades de desenvolvimento. A superproteção dos jovens pode, caso adotada, impedi-los de desenvolver capacidades valorosas. Nesse sentido, é o relatório da UNICEF "Crescendo em um mundo conectado: compreendendo riscos e oportunidades para crianças na era digital", publicado em novembro de 2019. O documento constata que os menores de idade que participam de mais atividades online possuem mais habilidades digitais do que aqueles que têm menor participação; e, além disto, que menores com pais menos restritivos têm mais chances de se envolverem em atividades online, não apenas jogando games ou assistindo vídeos, mas também participando de atividades que desenvolvam sua criatividade e curiosidade por novos conhecimentos. Ainda de acordo com o mesmo documento, "é importante ter em mente que o risco nem sempre conduz a danos. Crianças expostas a riscos online podem não sofrer danos se tiverem conhecimentos e resiliência para lidar com a experiência". Portanto, proteger as crianças e os adolescentes e garantir seu melhor interesse não significa limitar suas oportunidades de consumir e produzir conteúdo, bem como informar-se e expressar-se no mundo digital. O relatório conclui que legisladores e reguladores devem adotar uma abordagem equilibrada e integrada no que se refere à regulamentação do uso da internet por menores de idade, de forma a reduzir os riscos aos quais esse grupo é submetido, mas sem limitar, como já mencionado, as oportunidades positivas para seu desenvolvimento presentes no mundo digital. Nesse contexto, o Guia orientativo publicado por esta r. ANPD sobre o tratamento de dados pessoais a partir da base legal do legítimo interesse, especificamente no que diz respeito ao tratamento de dados de crianças e adolescentes, traz orientações e procedimentos suficientemente claros, que evitam a violação de direitos e permitem um exame detalhado das situações enfrentadas por cada agente de tratamento. Referido Guia não difere, tampouco se revela menos denso que as normas complementares ao GDPR, norma matriz da Lei Geral de Proteção de Dados, nem de sua versão publicada no Reino Unido. Além disto, a ANPD sempre poderá estabelecer restrições específicas ao tratamento de dados pessoais de crianças e adolescentes a partir de suas decisões em casos concretos, de modo que, ao deixar de estabelecer, em norma, comandos gerais e abstratos pormenorizados, não estará eliminando a possibilidade de intervir de forma mais minuciosa quando necessário, fixando precedentes importantes que certamente terão repercussão sobre a conduta dos agentes regulados. Diante do exposto, a ABERT entende que o aumento da densidade normativa, a partir da instituição de mais instruções e comandos em sede da regulamentação, tende a exceder o grau indicado no Comentário Geral nº 14 da ONU e refletido no próprio En. nº 01/23 do CD desta própria ANPD, atuando contra o melhor interesse de crianças e adolescentes. (Contribuição completa segue por e-mail). ","708725":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). O tratamento dos dados pessoais é necessário para que crianças e adolescentes possam ter acesso a serviços que lhes permitem se entreter, aprender e, enfim, interagir no mundo online e fora dele. Alguns desses serviços trazem, sim, maiores riscos, a serem considerados diante do melhor interesse de crianças e adolescentes. A ANPD caminhou no sentido de estabelecer que o tratamento de dados pessoais de crianças e adolescentes deve ser enquadrado, em termos práticos, como de alto risco, impondo aos agentes de tratamento a necessidade de elaboração de relatório de

impacto, a partir do qual deverão avaliar “riscos específicos para esse público e as medidas de segurança que deverão ser implementadas para as mitigações apropriadas”. A posição brasileira é até mais estrita do que a adotada no continente europeu e no Reino Unido, uma vez que, por lá, o tratamento de dados de crianças e adolescentes não é considerado, por si, um tratamento de alto risco e os critérios adicionais a serem preenchidos para que passe a ser são mais específicos e, portanto, menos presentes nas diversas atividades de tratamento a serem analisadas. Ao tornar a elaboração de relatório de impacto à proteção de dados pessoais uma rotina obrigatória para os agentes que tratem dados pessoais de crianças e adolescentes, a ANPD dá um impulso importante para que o melhor interesse de crianças e adolescentes seja preservado, na medida em que faz recair sobre tais agentes o ônus de indicar quais riscos são causados pelas atividades de tratamento que tem em vista e quais as medidas de mitigação desses riscos identificados estão sendo adotadas, tanto do ponto de vista da segurança de dados quanto da transparência das informações repassadas aos titulares ou a seus responsáveis. Nesse contexto, o guia sobre a hipótese de tratamento fundada em legítimo interesse e o guia sobre tratamento de dados pessoais de alto risco são plataformas importantes para que a ANPD continue a abordar situações que demandem maior rigor dos agentes de tratamento. Para além disto, é também necessário que se tenha em vista que a proteção ao melhor interesse não está ancorada apenas na legislação de proteção de dados, nem poderia estar, na medida em que a proteção integral de crianças e adolescentes demanda uma atenção muito mais abrangente. Nesse sentido, são as leis e regulamentos que dispõem sobre o acesso de crianças e adolescentes a certos serviços e a conteúdos, disponíveis online , como o Estatuto da Criança e do Adolescente e as normas sobre classificação indicativa. Tais normas estão além da LGPD e precedem-na em uma cadeia de barreiras jurídicas de proteção. A partir dos mecanismos de controle parental e da própria orientação conferida aos pais a partir da classificação indicativa, as associadas têm conseguido balizar o acesso a seus serviços (sejam aplicações de streaming ou sites acessíveis por navegadores) sem a devida autorização e supervisão dos responsáveis por crianças e adolescentes, evitando, em grande parte, o tratamento de dados desses menores de forma contrária a seu melhor interesse. Portanto, nem sempre a realização do melhor interesse dos menores demandará inovações na regulamentação lastreada na LGPD, mas, sim, em outras formas de intervenção, amparadas em outras instâncias estatais e na própria família. É inegável, contudo, que existem campos para avanços no que diz respeito a outros serviços, como redes sociais, cada vez mais populares entre crianças e adolescentes. Ainda que a regulação de contorno desses serviços esteja por vir, é evidente que a regulamentação ligada à legislação de proteção dos dados pessoais se fará, como já se faz, de suma importância. Nessa seara, a implementação de mecanismos de validação da maioridade do responsável indicado para abertura de contas por menores em tais aplicações desponta como uma medida de proteção proporcional e que deveria ser considerada pela ANPD como parte de sua avaliação dos cuidados tomados por agentes de tratamento no sentido da concretização do melhor interesse de crianças e adolescentes. (Contribuição completa segue por e-mail)","705523":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). O consentimento, para adolescentes compreendidos na faixa etária entre 12 e 16 anos, deve ser concedido por meio de acesso à página exclusivamente voltada para este fim, de modo que as

pessoas diretamente interessadas, notadamente o menor titular de dados e seus pais ou responsáveis possam reconhecer sua finalidade, não restando dúvidas sobre (i) o que se trata aquela solicitação e (ii) para qual finalidade o consentimento está sendo solicitado. A página que solicitará o consentimento deverá apresentar características destacadas das demais, que ressaltem a finalidade daquela requisição. Por também ser direcionada a pessoa menor, a página deve apresentar linguagem simples, clara e acessível a este público, afastando-se de rebuscamentos da linguagem jurídica eminentemente técnica. Deve-se considerar, ainda, as regras gerais, pelas quais essa solicitação de consentimento seja limitada pela (i) minimização de dados estritamente necessários ao tratamento; (ii) exclusiva finalidade pretendida – obtenção do consentimento dos pais ou responsáveis e (iii) transparência das informações, adequada e compatível ao público-alvo daquela solicitação. Por fim, a solicitação de consentimento deve ser acompanhada da respectiva política de privacidade.
","708742":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). Não há dúvidas que a viabilização e a verificação do consentimento de pais ou responsáveis por crianças e adolescentes devem se orientar pelos princípios que norteiam o tratamento de dados pessoais, conforme a LGPD, recebendo especial atenção o princípio da necessidade, pelo qual é limitado o tratamento "ao mínimo necessário para a realização de suas finalidades". Por sua vez, o princípio da necessidade deve ser analisado dentro de parâmetros do que é razoável e proporcional, de modo que eventual tratamento, ainda que sob o fundamento de manutenção do melhor interesse da criança, seja realizado sem excessos, restringindo-se ao estritamente necessário para determinada finalidade. Isso posto, entende-se que ao controlador devem ser facultadas diferentes alternativas para a verificação (i) da idade do titular de dados, assim como (ii) da identidade dos pais ou responsáveis. Essa medida tem como fundamento a conjunção do resguardo dos direitos de crianças e adolescentes, ao mesmo tempo em que proporciona ao controlador a possibilidade de identificar o mecanismo mais adequado, dentro de seu contexto comercial e suas limitações operacionais, sem que incorra em uma coleta de dados pessoais excessiva. Nesse contexto, dentre as diversas alternativas possíveis, são sugeridas as seguintes, tendo em vista atingirem a finalidade esperada, sem que excedam aos limites razoáveis de tratamento de dados: (i) no caso da oferta de produtos e serviços digitais gratuitos, a verificação poderá ser realizada a partir da confirmação da validade do CPF e se pertence à pessoa maior de idade (ii) no caso de oferta de produtos e serviços digitais pagos, a verificação estará condicionada ao método de pagamento escolhido, sendo automaticamente notificado seu titular, reconhecido como pessoa em plena capacidade civil. Admitindo-se somente a título de argumentação, verifica-se que eventual confirmação por meio de chamada de vídeo ou mesmo a obrigação de encaminhamento de fotografia dos pais ou responsáveis apresentando documento de identificação civil, além de não se conformarem diante da minimização de dados pessoais, seriam desproporcionais, uma vez que resultariam em uma coleta excessiva de dados pessoais – desnecessária para os fins pretendidos – além de onerar demasiadamente os controladores a partir de obrigação que demandará altos investimentos para a garantia da segurança da operação. Essas sugestões são apresentadas dentro de uma análise sistêmica que considera, principalmente, o melhor interesse da criança e do adolescente – como priorizado no "Manifesto por uma melhor governança de dados de

crianças", publicado pelo Fundo das Nações Unidas para a Infância (UNICEF)" -, uma vez que são propostas medidas para resguardar seus direitos, ao tempo em que não são criados empecilhos à participação na vida digital. Dessa forma, são concedidas novas oportunidades positivas de desenvolvimento dessas pessoas no mundo digital.
","708745":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). A autonomia progressiva dos adolescentes titulares de dados deve ser respeitada também em alinhamento com o seu melhor interesse, como disposto no art. 14, caput, da LGPD. Nesse contexto, faz-se necessário considerar, para a análise mais adequada desse cenário, o disposto no Enunciado nº 692 da IX Jornada de Direito Civil, pelo qual é ratificado que os conceitos de criança e adolescente, dispostos no art. 14, da LGPD, devem ser interpretados à luz do art. 2º, do ECA. Assim, para as matérias atinentes à proteção de dados pessoais, serão consideradas adolescentes todas as pessoas entre 12 anos completos e 18 anos incompletos, possuindo aquelas a partir de 16 anos capacidade para conceder seu consentimento no tratamento de dados pessoais, o que, por sua vez, relativiza os regimes de capacidade dispostos no Código Civil brasileiro. Conforme justificativa do Enunciado nº 692, a LGPD, então, "reconhece a redução gradual da autoridade parental face ao amadurecimento do menor", principalmente diante de sua inserção digital precoce, ficando sedimentado o entendimento de que "à medida do crescimento, o adolescente adquire paulatinamente a capacidade de discernir e decidir, devendo ser respeitada a dimensão da responsabilidade consequente do ato a ser praticado". Ainda sob essa perspectiva, há de se ressaltar que a desnecessidade de um consentimento por parte de pais e responsáveis, principalmente nos casos de adolescentes a partir dos 16 anos, revela-se como medida para incentivo à fluidez na utilização dos meios digitais, visto que, em diversas oportunidades, esse consentimento é realizado como mera formalidade para permitir o uso por adolescentes. Em linhas gerais, dispensar o consentimento, nesses casos, configura-se como medida de desburocratização para a interação desses jovens com as plataformas. Reconhecendo a interpretação trazida pelo ECA, ao tempo em que se resguarda a autonomia progressiva, é importante verificar que essa não é uma política exclusiva brasileira, vez que, por exemplo, tanto os Estados Unidos da América, Reino Unido quanto a União Europeia autorizam que o adolescente, a partir de seus 13 anos, conceda seu consentimento sem a necessidade de uma assistência ou representação. Nessa esteira, valemo-nos do Comentário Geral nº 25 da Organização das Nações Unidas sobre os Direitos das Crianças em Relação ao Ambiente Digital, pelo qual é reiterada a importância do desenvolvimento progressivo, enquanto um princípio que permite a pessoa menor adquirir competências e compreender suas ações e suas consequências no meio digital, dentro de seus limites de responsabilidade. Como observado, dentro desta gradação estabelecida, a partir do amadurecimento, a decisões tomadas por adolescentes passam a prescindir de assistência ou representação. Portanto, conciliando o melhor interesse com a autonomia progressiva, ao tempo em que se garante um desenvolvimento maior de sua autonomia, ao adolescente também é permitido o acesso aos meios digitais em suas expressões mais tecnológicas e modernas, sendo ofertados espaços de acesso à cultura, educação e informação, por exemplo. ","705539":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). Como mencionado na resposta à questão II.2, é necessário que se tenha em vista que a

concretização do melhor interesse de crianças e adolescentes não está ancorada apenas na legislação de privacidade e proteção de dados, nem poderia estar, na medida em que sua proteção integral demanda uma atenção muito mais abrangente. Nesse sentido, leis e regulamentos que dispõem sobre o acesso de crianças e adolescentes a certos serviços e a conteúdos, como o ECA e as normas sobre classificação indicativa, são parte importante desse sistema mais amplo de salvaguardas. Tais normas estão além da LGPD e precedem-na em uma cadeia de barreiras jurídicas de proteção. No caso específico de jogos eletrônicos e aplicações streaming, são oferecidos mecanismos personalizáveis de controle parental, além do "modo infantil", em que grande parte do catálogo de conteúdos deixa de ser disponibilizado, tomando por base que uma criança estará diante da tela. Todas essas medidas acabam contribuindo para que se evite um acesso indevido a determinados serviços e conteúdo e, por conseguinte, para que atividades de tratamento de dados sejam evitadas, senão em absoluto, mas em grande parte. Ainda que a regulamentação e as orientações apoiadas na LGPD não sejam capazes de disciplinar propriamente as condições de acesso de crianças e adolescentes a serviços e conteúdos online, elas podem ser de grande valia ao disporem sobre as medidas de transparência a serem adotadas na comunicação com menores e seus responsáveis, bem como nos mecanismos de verificação da maioridade daqueles que validam a criação de contas junto aos provedores desses serviços e conteúdos. A esse passo, vale lembrar que o controlador deve ter diferentes alternativas para a verificação (i) da idade do titular de dados, assim como (ii) da validade do CPF indicado que pertença à pessoa maior de idade de modo a que se conjugue a proteção dos direitos de crianças e adolescentes, ao mesmo tempo em que proporcione ao controlador a possibilidade de identificar o mecanismo mais adequado, dentro de seu contexto comercial e suas limitações operacionais, sem que incorra em uma coleta de dados pessoais excessiva. Mais destalhes a esse respeito seguem na resposta à questão II.2. Enquanto jogos eletrônicos e aplicações de streaming incorporam avanços significativos no sentido de controle parental e verificação da maioridade daqueles que se apresentam como responsáveis por crianças e adolescentes, existem campos para avanços no que diz respeito a outros serviços, como redes sociais, cada vez mais populares entre crianças e adolescentes. Nessa seara, a implementação de tais mecanismos desponta como uma medida de proteção proporcional e que deveria ser considerada pela ANPD como parte de sua avaliação dos cuidados tomados por agentes de tratamento no sentido da concretização do melhor interesse de crianças e adolescentes.
","708762":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). Conforme exposto na resposta à questão II.2, entende-se que ao controlador devem ser facultadas diferentes alternativas para a verificação (i) da idade do titular de dados, assim como (ii) da validade do CPF indicado que pertença à pessoa maior de idade. Essa medida tem como fundamento a conjunção do resguardo dos direitos de crianças e adolescentes, ao mesmo tempo em que proporciona ao controlador a possibilidade de identificar o mecanismo mais adequado, dentro de seu contexto comercial e suas limitações operacionais, sem que incorra em uma coleta de dados pessoais excessiva. Nesse contexto, dentre as diversas alternativas possíveis, são sugeridas as seguintes, tendo em vista atingirem a finalidade esperada, sem que excedam aos limites razoáveis de tratamento de dados: (i) no caso da oferta de produtos e serviços digitais gratuitos, a verificação poderá

ser realizada a partir da confirmação da validade do CPF a ser indicado no ato de solicitação de acesso e se o CPF pertence à pessoa maior de idade; (ii) no caso de oferta de produtos e serviços digitais pagos, a verificação estará condicionada ao método de pagamento escolhido, sendo automaticamente notificado seu titular, reconhecido como pessoa em plena capacidade civil. Admitindo-se somente a título de argumentação, verifica-se que eventual confirmação por meio de chamada de vídeo ou mesmo a obrigação de encaminhamento de fotografia dos pais ou responsáveis apresentando documento de identificação civil, além de não se conformarem diante da minimização de dados pessoais, seriam desproporcionais, uma vez que resultariam em uma coleta excessiva de dados pessoais – desnecessária para os fins pretendidos – além de onerar demasiadamente os controladores a partir de obrigação que demandará altos investimentos para a garantia da segurança da operação. Essas sugestões são apresentadas dentro de uma análise sistêmica que considera, principalmente, o melhor interesse da criança e do adolescente – como priorizado no "Manifesto por uma melhor governança de dados de crianças", publicado pelo Fundo das Nações Unidas para a Infância (UNICEF)" -, uma vez que são propostas medidas para resguardar seus direitos, ao tempo em que não são criados empecilhos à participação na vida digital. Dessa forma, são concedidas novas oportunidades positivas de desenvolvimento dessas pessoas no mundo digital. ","708764":"Sem contribuições. ","708768":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). A comunicação transparente com os próprios pais e responsáveis é o primeiro mecanismo a assegurar a proteção dos menores sob sua tutela. Em segundo lugar, mecanismos de validação da maioridade do responsável, tratados ao longo das respostas às demais questões, são de suma importância para que se tenha certeza de que o agente de tratamento está estabelecendo um diálogo com um indivíduo capaz de efetivamente responder por crianças e adolescentes. Adicionalmente, pais e responsáveis devem ter ao seu alcance, nos casos em que se revelar possível, mecanismos de supervisão, como escolha de conteúdo e funcionalidades a serem acessadas em aplicações, relatórios sobre as atividades de seus filhos, entre outras, sempre tendo em vista os limites técnico-operacionais de cada serviço e a regulação específica de cada setor de atividade econômica, que, em alguns casos, já terá disciplinado de forma competente a matéria, notadamente no que diz respeito à adoção de medidas de controle e supervisão. ","708772":"CONTRIBUIÇÃO DA ABERT (ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO). Com demonstrado na resposta às questões anteriores, um dos principais vetores para a concretização do melhor interesse de crianças e adolescentes é a comunicação de forma transparente e apropriada com os pais e responsáveis legais. Eles devem ter ao seu alcance informações claras sobre as atividades conduzidas pelos agentes de tratamento e, para além disto, nos casos em que se revelar possível, mecanismos de supervisão, como escolha de conteúdo e funcionalidades a serem acessadas em aplicações, relatórios sobre as atividades de seus filhos, entre outras. No entanto, é crucial que a ANPD considere os limites técnicos dos diversos serviços, e como já exposto, a regulação específica de cada setor de atividade econômica, que, em muitas das vezes, já tratará sobre o fornecimento de informações a pais e responsáveis e a implementação de medidas de controle e supervisão.","708775":"Sem contribuições.

Contribuinte: Rodolfo Salema

Número: OP-753175

Data: 16/08/2024 - 17:49

Resumo:
:"","708725":"","705523":"","708742":"","708745":"","705539":"","708762":"","708764":"","708768":"","708772":"","708775":".

Contribuinte: Luíza Fernandes Malheiro

Número: OP-753187

Data: 16/08/2024 - 18:11

Resumo: :"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Entendemos que o próprio termo "melhor interesse do menor" requer maior detalhamento por parte da ANPD, a começar pela sua própria definição. Para tanto, consideramos fundamental que a definição de "melhor interesse do menor": i. seja analisada de forma casuística, tendo em vista o contexto específico no qual ocorrerá o tratamento de dados dos menores; ii. considere as características específicas do menor cujos dados serão tratados; e iii. seja equilibrada com outros direitos desses menores. Exemplo 1: Processos que visam garantir a segurança do menor contra fraudes financeiras, como através de mecanismos de autenticação de identidade, também devem ser contemplados no que se entende por melhor interesse do menor. Exemplo 2: Contemplar no melhor interesse do menor o envio de comunicações distintas aos menores sobre o tratamento dos seus dados no contexto de abertura de uma conta corrente. Isso porque podemos ter, de um lado, uma criança de 5 anos (que tem suas capacidades e autonomia de certa forma limitadas, para a qual pode ser recomendada uma política de privacidade mais lúdica e acessível), e, de outro, de um adolescente de 16 anos (que já conta com maior independência e gerência sobre os seus atos). De maneira similar, fazemos referência ao seguinte trecho do Guia Orientativo sobre Legítimo Interesse da ANPD: "A documentação referente ao tratamento poderá, ainda, conter a análise efetuada pelo controlador, em especial o teste de balanceamento, incluindo a indicação sobre a natureza dos dados pessoais tratados, a demonstração da legitimidade do interesse do controlador ou de terceiro, a sua ponderação com os direitos dos titulares e a compatibilidade com as suas legítimas expectativas, e se tratando de dados pessoais de criança ou adolescentes, as evidências da observância e prevalência do seu melhor interesse." Com base no trecho acima, ressaltamos também a importância de diferenciar as etapas e requisitos de análise do melhor interesse do menor vs. a análise da base legal do legítimo interesse para tratamento de dados de menores.","708725":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Sim. Destacamos casos de publicidade (incluindo publicidade personalizada) que podem fomentar comportamentos positivos em prol do melhor interesse do menor. Embora o envio de publicidade para menores seja visto como negativo por

determinados stakeholders, existem casos em que esse envio pode contribuir para atividades que estejam em harmonia com o melhor interesse de crianças e adolescentes. É o caso, por exemplo, do envio de e-mail marketing para menores referente a serviço de investimento voltado a fomentar a educação financeira desse público alvo. Também ressaltamos os casos de tratamento de dados de menores para fins de desenvolvimento de modelos de riscos relacionados à necessidade de cumprimento de obrigações legais e regulatórias (como AML e fraude). Outro exemplo importante diz respeito à sobreposição do melhor interesse do menor em relação ao interesse dos próprios pais e responsáveis legais. É o caso, por exemplo, da coleta de dados adicionais de menores a fim de evitar a criação de contas laranjas criadas por responsáveis legais mal intencionados.","705523":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Inicialmente, destacamos o entendimento já firmado pelo Enunciado nº 1/2022 da ANPD, conforme o qual foi estabelecido que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base em qualquer uma das hipóteses de tratamento previstas na LGPD, desde que observado e prevalecente o seu melhor interesse. Além disso, ressaltamos que a LGPD não estabelece qualquer hierarquia entre as hipóteses de tratamento de dados pessoais nela previstas. Por essa razão, e em observância ao tema desta Seção, reafirmamos que o consentimento não necessariamente é a base legal mais adequada, tampouco a única aplicável, para o tratamento de dados pessoais de menores no ordenamento jurídico nacional. Passando à análise dos critérios para obtenção do consentimento específico e em destaque (conforme previsto pelo art. 14, § 1º da LGPD), seria importante que a ANPD estabelecesse critérios que contemplem aspectos como (i) o uso de linguagem acessível para indicar quais os dados pessoais tratados e qual a finalidade do seu uso, bem como que o menor precisará do consentimento parental para ter os seus dados tratados; (ii) o uso de aspectos visuais que facilitem a obtenção desse consentimento em destaque. Exemplo: uso de checkbox específico para a coleta do consentimento parental durante o fluxo de onboarding do menor.","708742":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Antes mesmo de definir quais as medidas e mecanismos a serem adotados pelos controladores para verificar que o consentimento para o tratamento de dados de menores foi fornecido pelos seus pais ou responsáveis legais, entendemos que critérios como tecnologia disponível, porte do controlador e criticidade decorrente do tratamento dos dados dos menores devem ser levados em consideração para avaliação da legitimidade desse consentimento. Isso porque a adoção de algumas dessas medidas pode implicar na necessidade de implementação de processos e custos adicionais, que não necessariamente se alinham ao porte da empresa e mesmo ao risco trazido pelo tratamento em pauta. Para fins ilustrativos, apresentamos algumas das medidas passíveis de serem aplicadas a fim de verificar se o consentimento foi de fato fornecido pelos pais ou representantes legais dos menores: (i) envio de e-mail para os pais/responsáveis legais a fim de confirmar o consentimento supostamente fornecido por eles no app para a criação da conta do menor; (ii) solicitar documento aos pais/responsáveis legais após fornecerem o consentimento para o tratamento do menor, a fim de confirmar a sua identidade.","708745":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): A obtenção do consentimento de adolescentes deve seguir o ordenamento jurídico estabelecido pelo Código Civil, levando em conta a autonomia progressiva desses titulares. Dessa forma, é possível reconhecer a capacidade evolutiva desses menores, e ao mesmo tempo proteger os seus dados

pessoais, e assim assegurar o melhor interesse dos adolescentes. ","705539":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Destacamos como recomendação a adoção de experiências com diferentes funcionalidades para diferentes faixas etárias, a fim de mitigar riscos específicos para os menores, como compras excessivas e divulgação de conteúdo inadequado. Esse tipo de medida está em linha com o California Age-Appropriate Design Code Act, que determina que: "as empresas devem levar em conta as necessidades únicas das diferentes faixas etárias, incluindo os seguintes estágios de desenvolvimento: 0 a 5 anos de idade ou 'pré-alfabetização e alfabetização inicial'; 6 a 9 anos de idade ou 'anos fundamentais do ensino primário'; 10 a 12 anos de idade ou 'anos de transição'; 13 a 15 anos de idade ou 'início da adolescência'; e 16 a 17 anos de idade ou 'aproximando-se da idade adulta'". Vale ressaltar que a adoção dos princípios de tratamento de dados trazidos pela LGPD já apresenta uma proteção robusta aos dados pessoais dos menores e ao seu melhor interesse, razão pela qual devem ser respeitados no desenvolvimento de medidas que visem mitigar os riscos decorrentes do tratamento de dados pessoais no contexto de uso de plataformas digitais. ","708762":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Para fins de verificação de idade do menor, idealmente devem ser utilizados fluxos que contemplem tanto o melhor interesse do menor, no sentido de assegurar a sua real idade, quanto a proteção dos seus dados pessoais. Um exemplo é a verificação de dados pessoais de menores junto a fontes oficiais (sejam públicas ou particulares) para confirmar a idade indicada pelo menor. Destacamos que os critérios que apresentamos na seção referente à verificação do consentimento parental também devem se aplicar para fins de verificação etária, quais sejam: tecnologia disponível, porte do controlador, e criticidade decorrente do tratamento dos dados dos menores.","708764":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): A adoção dos princípios de tratamento de dados pessoais previstos na LGPD são capazes de indicar as limitações a serem observadas pelas plataformas digitais na coleta de dados pessoais de menores. Por exemplo: quando uma determinada plataforma induz um menor a oferecer dados pessoais para obter acesso a determinadas ferramentas, temos uma atividade que contraria, por exemplo, o princípio da necessidade. Em relação à formação de perfis comportamentais, consideramos que nem sempre representam algo prejudicial ao melhor interesse do menor. É o caso, por exemplo, da criação de perfis comportamentais de menores por determinada instituição financeira, a fim de avaliar os seus comportamentos para fins de prevenção à fraude.","708768":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Conforme mencionamos nas seções anteriores, nem sempre o controle de pais e responsáveis legais sobre o tratamento dos dados pessoais dos menores sob sua responsabilidade vai ao encontro do melhor interesse do menor. Justamente por essa razão, entendemos que essas medidas de controle devem ser proporcionais às capacidades e necessidades das faixas etárias dos menores, diminuindo gradativamente em relação ao aumento da sua idade. De todo modo, algumas medidas passíveis de serem aplicáveis enquanto boas práticas são: (i) envio de notificações aos pais ou responsáveis legais para informá-los sobre a realização de transações financeiras das crianças sob a sua responsabilidade; (ii) criação de dashboard de privacidade na qual os pais ou responsáveis legais podem selecionar os controles sobre o tratamento de dados pessoais dos menores sob a sua responsabilidade, mantendo os controles acionados por

padrão.","708772":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): É recomendável a adoção de mecanismos que (i) transmitam informações sobre o tratamento de dados de forma adequada ao público (como vídeos, gamificação etc); e (ii) sejam capazes de atrair a sua atenção e consolidar a absorção das informações que lhe são apresentadas (como materiais lúdicos e ilustrados). Um exemplo recente e bastante divulgado no mercado é a Política de Privacidade da Lego, apresentada em seu site no formato de vídeo curto, instrutivo e ilustrado com brinquedos da própria marca, a fim de aproximar o seu conteúdo do seu público-alvo e facilitar a sua absorção.","708775":"Contribuições da Zetta (CNPJ 37.253.906/0001-28): Aproveitamos para ressaltar a necessidade de consolidação, por parte da ANPD, do entendimento apresentado no seu Enunciado nº 1/2022, no sentido de que o tratamento de dados pessoais de menores pode ser justificado por qualquer uma das bases legais da LGPD, bem como da ausência de hierarquia entre as bases legais trazidas pela LGPD. Isso trará um ambiente de maior segurança jurídica para o tratamento de dados de crianças e adolescentes, criando assim a possibilidade de mais espaço para o desenvolvimento de iniciativas inovadoras e efetivas para viabilizar o tratamento desses dados em prol do melhor interesse dos seus titulares. Por exemplo: é possível que uma iniciativa de coleta de dados de menores para fins de combate à fraude e baseada no consentimento não seja tão eficaz pelo fato de os menores terem a possibilidade de revogar esse consentimento, o que reforça o argumento já defendido de que o consentimento não necessariamente é a base legal mais adequada para o tratamento de dados de crianças e adolescentes. Também seria interessante que a ANPD, por meio de guias orientativos, apresentasse exemplos de medidas que considera como recomendáveis para um adequado tratamento de dados de menores em consonância com o seu melhor interesse, especialmente aquelas endereçadas a temas como consentimento parental, verificação de idade, medidas de transparência e autonomia progressiva do menor. Do compromisso da Zetta com a proteção integral de crianças e adolescentes A Zetta reconhece a proteção integral e o melhor interesse como princípios jurídicos fundamentais a nortearem todas as atividades de tratamento de dados pessoais de crianças e adolescentes por parte de suas associadas. Neste sentido, relembramos a Convenção sobre Direitos das Crianças, adotada em 1990 pela Organização das Nações Unidas, ratificada pelo Brasil e por mais 195 países, que dispõe que todas as ações relativas às crianças devem considerar primordialmente o seu melhor interesse. Ressaltamos, ainda, a centralidade do art. 227 da Constituição Federal que preconiza o princípio da proteção integral de crianças e adolescentes, atribuindo à família, à sociedade e ao Estado assegurar a essas pessoas com absoluta prioridade direitos e garantias fundamentais. E, por fim, a existência do Estatuto da Criança e do Adolescente, que, igualmente, faz menção ao princípio da proteção integral em seus artigos 1º e 3º.

Contribuinte: Laryssa de Menezes Silva

Número: OP-753195

Data: 16/08/2024 - 18:24

Resumo: :"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708725":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","705523":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708742":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708745":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","705539":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708762":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708764":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708768":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708772":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br","708775":"As contribuições do Google e do YouTube foram encaminhadas ao e-mail normatizacao@anpd.gov.br

Contribuinte: GUSTAVO VIEIRA DE SOUSA

Número: OP-753200

Data: 16/08/2024 - 18:27

Resumo: :"A ANPD utilizou diretrizes da OCDE e da ONU para definir o "melhor interesse" da criança e do adolescente no Guia de Legítimo Interesse. No entanto, essas orientações são vagas para uma atuação segura dos agentes de tratamento. Embora a amplitude e abstração do princípio sejam naturais, pois não se trata de um conceito fechado e definido ex ante, a ANPD pode criar diretrizes e parâmetros para melhor esclarecer, com algum nível de concretude, o que constitui o melhor interesse desses titulares no âmbito do tratamento de dados pessoais, assegurando consistência e eficácia na aplicação das normas de proteção de dados. Portanto, é crucial que a ANPD parametrize de forma mais objetiva o "melhor interesse" da criança e do adolescente na proteção de dados pessoais. Seria essencial conferir maior concretude utilizando mecanismos como exemplos e situações hipotéticas que considerem nuances específicas e esforços tecnicamente disponíveis, mantendo flexibilidade para diferentes contextos e modelos de negócio. Vale ressaltar que, por exemplo, a ANPD já manifestou na Nota Técnica nº 6/2023/CGF/ANPD que a restrição de acesso aos produtos e serviços do TikTok para crianças (indivíduos com até 12 anos) seria uma forma de garantir o melhor interesse. Seria relevante, para fins de orientação geral e clareza ao mercado, esclarecimentos acerca dos motivos pelos quais determinadas restrições auxiliam na concretização do princípio, na visão da autoridade. A tensão entre o princípio da minimização de dados pessoais e a eficácia dos mecanismos de verificação e detecção de idade é um bom exemplo da relevância deste tipo de esclarecimento. Atender ao melhor interesse - como adotar medidas para impedir o acesso a conteúdos ou plataformas inadequados para sua idade - pode exigir a coleta de mais dados pessoais. Por isso, é crucial que os agentes compreendam com algum nível de clareza quais são as balizas concretas que a ANPD considerará na análise

deste tipo de cenário, para que possam determinar a melhor forma de implementação de ferramentas. Sem clareza sobre se a autoridade considerará esses mecanismos válidos - ou se entenderá mecanismos mais invasivos como contrários ao princípio da minimização - o mercado dificilmente saberá como agir. Assim, é crucial garantir que os controladores não sejam penalizados por eventual flexibilização do princípio da minimização, quando justificada pelo melhor interesse da criança e do adolescente. Além disso, é importante que as orientações da autoridade sobre o que constitui o melhor interesse da criança e do adolescente em situações específicas sejam fornecidas não só por meio de casos concretos, mas principalmente através de guias e outros documentos com eficácia geral. Isso oferece maior segurança jurídica, permitindo que os agentes se antecipem e ajustem suas práticas conforme parâmetros estabelecidos. Além disso, dessa forma, os agentes não precisam esperar por casos específicos para agir e podem se preparar com antecedência - o que contribui para a construção de uma cultura de proteção de dados no Brasil. Também, essa forma de atuação auxilia a estabelecer um level playing field no mercado, evitando que agentes com políticas menos protetivas continuem a operar sem maiores consequências. O TikTok destaca que a análise do "melhor interesse" deve considerar múltiplas dimensões, não se limitando à proteção de dados, mas também tendo em vista a segurança, acesso à informação, direito de brincar e se conectar, entre outros. Deve-se também levar em conta as diferentes características e experiências de um grupo heterogêneo (idade, gênero, deficiências, localização geográfica, origem étnica e perfil socioeconômico), tendo flexibilidade suficiente para ser adaptável ao desenvolvimento dos vários indivíduos que o compõem.","708725":"Em alguns contextos, é mais fácil identificar o comportamento esperado dos agentes de tratamento em relação ao princípio do melhor interesse. No entanto, sua aplicação pode ser mais complexa em outros casos, onde é difícil equilibrá-lo com os demais princípios da LGPD. O TikTok gostaria de trazer dois exemplos que considera particularmente desafiadores. O primeiro refere-se ao direcionamento de publicidade e, o segundo, ao direcionamento de conteúdo: ambas são práticas que tendem a ser vistas com maus olhos, como contrárias ao melhor interesse da criança e do adolescente, a partir de premissas equivocadas. Na realidade, ambas podem assegurar precisamente esse melhor interesse. 1. Publicidade: ainda que o TikTok não realize o perfilamento de usuários entre 13 e 17 anos com base em seus interesses, comportamento, gênero e idade para fins de publicidade,a criação de perfis com a referida finalidade exemplificaria a complexidade de harmonizar o melhor interesse da criança e do adolescente com os demais princípios da LGPD para plataformas digitais em geral. Isso porque, para plataformas que o fazem, o perfilamento para esse fim poderia vir a proteger menores, tornando os anúncios mais adequados e evitando que conteúdos inapropriados para a idade sejam exibidos para o público mais jovem. Considerando fatores como idade, a personalização garante uma filtragem mais precisa e segura, tornando a experiência online mais relevante e adaptada às necessidades dos usuários mais jovens. As diretrizes da ANPD devem esclarecer essa complexidade, garantindo que a publicidade respeite a autonomia dos adolescentes e leve em consideração sua vulnerabilidade, assegurando uma experiência online segura e adequada. O mesmo valeria para o direcionamento de conteúdo para usuários mais jovens, como detalhado abaixo. 2. Perfilamento para direcionamento de conteúdo. Cabe lembrar a diferença entre o

perfilamento para fins de publicidade (coleta e análise de dados para direcionar anúncios) e perfilamento para conteúdo (coleta e análise de dados para direcionar conteúdo relevante ao usuário, sem fins publicitários). O perfilamento para direcionamento de conteúdo também pode atender ao melhor interesse, pois pode direcionar conteúdos adequados à idade dos usuários e impedir que conteúdos inadequados sejam exibidos. Por exemplo, o TikTok criou a ferramenta “Níveis de Conteúdo”, que tem como objetivo evitar que vídeos considerados inapropriados para menores de 18 anos sejam exibidos para usuários mais jovens. Nesse sentido, os vídeos são classificados e exibidos de acordo com o grau de maturidade dos usuários. Os vídeos denunciados e revisados por moderadores podem receber classificação 18+ e não serão exibidos para os usuários entre 13 e 18 anos. Com esses níveis, usuários e seus pais podem limitar determinados tipos de conteúdo e personalizar a experiência de visualização, evitando que temas maduros cheguem a usuários entre 13 e 18 anos. Esse tipo de iniciativa protege os mais jovens e pode se beneficiar de práticas de perfilamento. Como dito, a questão do melhor interesse pode ser menos óbvia nestes contextos, por isso é crucial que a autoridade forneça diretrizes e balizas para avaliar e mitigar riscos. É importante equilibrar os benefícios do perfilamento com os potenciais riscos, sendo essencial fornecer orientação sobre como avaliar e mitigá-los, garantindo que a publicidade direcionada considere a autonomia progressiva do adolescente e seu grau de vulnerabilidade.","705523":"De acordo com a Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade. Conforme os posicionamentos da ANPD, incluindo o Enunciado nº 01/2023 e o Guia de Legítimo Interesse, o consentimento nem sempre é a base legal mais adequada para o tratamento de dados pessoais destas crianças e adolescentes, sendo admitidas outras bases legais para o tratamento de seus dados pessoais. Além disso, o próprio Enunciado menciona o risco de oneração excessiva dos responsáveis e a necessidade de colaboração multissetorial para a proteção efetiva de crianças e adolescentes. Especificamente no caso do tratamento de dados pessoais de crianças, caso o consentimento parental seja considerado a base legal mais adequada, cabe destacar que os adjetivos "específico e em destaque" (art. 14, §1º) diferem dos adjetivos "livre, informado e inequívoco" mencionados na LGPD. Essa diferença pode gerar inseguranças jurídicas significativas para os agentes regulados. Especificamente: A ANPD deve esclarecer o conceito de “específico”: O critério deve possibilitar que o consentimento seja dado com um nível de granularidade adequado ao caso, desde que o usuário seja informado de forma transparente (informações claras, precisas e facilmente acessíveis) sobre o fluxo de tratamento de seus dados pessoais. Isso se justifica em prol de uma exigência de transparência que seja eficaz, visto que a granularidade do consentimento - no sentido de detalhamento de forma extremamente compartimentalizada - não significa necessariamente maior clareza ao titular e/ou uma decisão mais informada. ANPD deve esclarecer o conceito de “em destaque”: a autoridade deve garantir que o conceito seja flexível o suficiente para considerar tanto os meios técnicos disponíveis quanto a diferentes naturezas e propósitos dos produtos ou serviços. Assim, deve estabelecer parâmetros mínimos sem impor uma padronização rígida, permitindo que os regulados se adaptem aos seus contextos específicos. Considerando a impossibilidade da criação de regras rígidas e

inflexíveis dada a vasta discrepância entre produtos e serviços, seria importante que a autoridade fornecesse diretrizes claras sobre quais métodos não são considerados adequados e suficientes para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais. Isso ajudaria a evitar ambiguidades e inseguranças jurídicas para agentes de tratamento. Além disso, é fundamental que a autoridade, ao estabelecer parâmetros, tenha em mente a necessidade de se respeitar o princípio da autonomia progressiva que, conforme reconhecido no Estatuto da Criança e do Adolescente ("ECA") e na Convenção sobre os Direitos da Criança, estabelece que crianças e adolescentes devem ter sua capacidade de decisão respeitada e ampliada conforme amadurecem. Neste contexto, é importante ter em vista que é possível que o consentimento no caso concreto não seja ofertado unicamente por responsáveis, mas pelo próprio menor. A autonomia progressiva sugere que, em vez de uma abordagem única para todas as idades, os critérios para obter consentimento devem ser adaptados de acordo com o desenvolvimento e a maturidade. Portanto, ao definir critérios ou parâmetros para a obtenção do consentimento, a autoridade deve considerar fatores como idade e compreensão para participação do menor (à medida que os menores amadurecem, eles devem ser mais envolvidos no processo de consentimento, respeitando sua crescente autonomia). Por exemplo, o Age Appropriate Design Code (ou "Children's Code"), elaborado pelo Information Commissioner's Office (ICO) do Reino Unido, que contém diretrizes para a proteção e privacidade online de crianças e adolescente, reconhece a autonomia progressiva da criança e do adolescente ao estabelecer diferentes parâmetros recomendados para o controle parental conforme faixa de idades.","708742":"O TikTok reforça a possibilidade, já reconhecida pela ANPD, da adequação de outras bases legais para além do consentimento para o tratamento de dados de menores, em especial o de adolescentes, o que pode ser extraído da própria LGPD. Especificamente no caso do tratamento de dados pessoais de crianças, para definir parâmetros de adoção para viabilizar e verificar que o consentimento foi fornecido pelos responsáveis, a ANPD deve levar em conta os esforços razoáveis, baseados na tecnologia disponível, recursos, nível de risco, naturezas e propósitos dos serviços e produtos. A autoridade não deve estabelecer medidas rígidas, mas sim diretrizes flexíveis e adequadas à forma como interagem o titular e o agente de tratamento, o que pode variar de acordo com o modelo de negócio em questão. Além disso, deve esclarecer parâmetros para que esse consentimento possa ser obtido de maneira que respeite a privacidade, garantindo que os métodos sejam práticos e adequados. No Guia da ICO, "Children 's Code Guidance and Resources - Age Appropriate Application" a autoridade deixa claro que é importante considerar esforços razoáveis para obter o consentimento parental. O Guia também esclarece que o consentimento deve ser obtido da maneira menos intrusiva possível, coletando o mínimo de identificadores pessoais. Um exemplo semelhante é a "Children 's Online Privacy Protection Act," dos EUA ("COPPA"). [...] A European Data Protection Board, por sua vez, [...] não especifica métodos exatos para obter o consentimento parental, mas recomenda uma abordagem proporcional baseada na minimização de dados. A verificação da idade adequada e da autoridade parental deve levar em consideração o nível de risco associado ao tratamento de dados e a tecnologia disponível, exigindo esforços adequados dos responsáveis pelo tratamento. Assim, as medidas de verificação devem evitar a coleta excessiva de dados pessoais, reconhecendo a dificuldade de verificar consentimento

quando a identidade da criança ou a responsabilidade parental são incertas. Uma medida que pode ser adotada pelos controladores é a indicação clara, nos Termos de Uso, dos requisitos para a representação dos pais, considerando a autonomia progressiva dos menores. Além disso, devem adotar mecanismos de transparência, permitindo que se compreenda os Termos de Uso dos serviços, respeitando seu desenvolvimento cognitivo e emocional. Seria mais produtivo se a autoridade indicasse e justificasse, através de exemplos, quais métodos não considera adequados em determinados contextos, ao invés de buscar definir rigidamente os mecanismos mais apropriados. Essa alternativa reconhece a impossibilidade de padronizar mecanismos para serviços tão variados, mas ainda fornece parâmetros claros aos agentes de tratamento, permitindo uma abordagem mais flexível. Assim, facilitaria a implementação em uma ampla gama de produtos, aumentando a eficácia da proteção. O TikTok destaca o risco de medidas excessivamente onerosas dificultarem a obtenção de consentimento efetivo para crianças e adolescentes (quando for a base legal adequada para o tratamento de dados), levando à "fadiga do consentimento". Vale salientar que a plataforma do TikTok é apenas para adolescentes maiores de 13 anos. Desta forma, entendemos que seria mais efetivo oferecer uma experiência gradativa, por meio da qual os pais (e/ou responsáveis) e também os usuários mais jovens, teriam acesso a informações claras e acessíveis, podendo realizar escolhas mais factíveis e ter um maior controle do tratamento de seus dados pessoais e de sua respectiva experiência. Daí a importância de explorar outras bases legais e garantir que as medidas para obter consentimento parental sejam proporcionais e práticas. Conforme reconhecido pela ANPD em seu Estudo Técnico Preliminar, a fadiga do consentimento questiona a efetividade do consentimento parental como única base legal e sua adequação para garantir a proteção ao melhor interesse da criança. [A contribuição completa do TikTok está na documentação enviada por e-mail à Coordenação-Geral de Normatização da ANPD devido à limitação de caracteres na plataforma Participa+ Brasil.]","708745":"Primeiramente, é preciso diferenciar o consentimento enquanto base legal e a concordância relativa a uma relação contratual estabelecida entre o agente de tratamento e o titular. A LGPD não altera a capacidade dos menores de idade de celebrar um contrato legal válido, de modo que o agente de tratamento poderá utilizar qualquer uma das bases legais disponíveis para tratar os dados pessoais de adolescentes. A autonomia progressiva, conforme positivada pela legislação brasileira, deve levar a uma redução gradual da interferência parental, respeitando a crescente capacidade dos adolescentes de exercerem seus direitos de forma independente. Portanto, é possível que adolescentes forneçam consentimento no ambiente digital sem a necessidade de representação ou assistência expressa dos pais, alinhando-se ao princípio do melhor interesse. A própria jurisprudência admite que a representação ou assistência possa ser tácita para atos corriqueiros da vida civil no ambiente digital. O melhor interesse será corretamente refletido ao se considerar a autonomia e o desenvolvimento progressivo desses jovens, o que pode prescindir a representação ou assistência expressa a depender do contexto, ato e risco em questão. Nesse sentido, o regime de incapacidades do Código Civil não é o melhor parâmetro para o direito à autonomia progressiva. Isso se verifica por duas razões: O Estatuto da Criança e do Adolescente define "criança" como a pessoa até 12 anos e "adolescente" como aquela entre 12 e 18 anos. Já o Código Civil estabelece que menores de 16 anos são absolutamente incapazes de exercer pessoalmente os atos da vida civil e devem ser

representados. Não prescreve, contudo, a forma como uma representação deve ser obtida. Neste ponto, vale destacar ainda que, em termos de representação/assistência, a ausência de exigência de autorização expressa é frequentemente considerada em situações envolvendo adolescentes em transações rotineiras ou interações online, especialmente em plataformas que oferecem os serviços como o do TikTok. [...] Tratar todos os indivíduos de 12 a 16 anos como uma massa homogênea e plenamente incapaz pode criar obstáculos ao seu melhor interesse. Tradicionalmente, a teoria civilista via as crianças como seres passivos, necessitando de controle adulto. No entanto, essa visão está sendo desafiada pela ideia de que os jovens devem ser vistos como capazes de tomar decisões juridicamente relevantes. [...] Para o Código Civil, aqueles com mais de 16 e menos de 18 anos são relativamente capazes, podendo praticar atos da vida civil desde que assistidos. No entanto, falta clareza sobre o que está incluído na definição de "atos da vida civil". Como o Código Civil não foi concebido no contexto digital, é necessário adaptá-lo à realidade moderna do uso de plataformas digitais. A capacidade civil e as formas de assistência para adolescentes devem ser mais flexíveis, especialmente em relação às atividades online consideradas "atos corriqueiros". [...] Um adolescente acessar uma plataforma digital para jogar, criar conteúdo ou interagir com amigos em redes sociais deve ser visto de maneira diferente de realizar uma transação financeira de grande porte, embora, para o Código Civil, ambas as atividades sejam "atos civis". [...] Há uma presunção de que os pais estão cientes e concordam com os "atos corriqueiros" realizados pelos menores na internet, como o acesso a plataformas com mecanismos de proteção, regidas por termos que os pais conhecem e validaram. [...] há uma compreensão implícita de que os menores se envolvem em atividades online com algum nível de conhecimento ou autorização dos pais. Essa abordagem legal espera que os pais orientem e monitorem o uso da internet pelos adolescentes de forma abrangente, mas não invasiva, [...] sob supervisão geral e indireta dos responsáveis, sem a necessidade de aceitação formal e reiterada para qualquer interação. [A contribuição completa do TikTok está na documentação enviada por e-mail à Coordenação-Geral de Normatização da ANPD devido à limitação de caracteres na plataforma Participa+ Brasil.]","705539":"O TikTok destaca que, para tais orientações, é crucial que a autoridade considere os diferentes níveis de maturidade e autonomia dos usuários em desenvolvimento, que exigem níveis variados de proteção. Portanto, as configurações de privacidade para menores devem ser adaptáveis ao conteúdo apropriado para a idade e ao desenvolvimento dos diferentes indivíduos. A resposta sobre controle parental (III.4.) contém mais informações sobre como o TikTok implementa essas diretrizes através da sincronização familiar e guias dedicados aos pais e responsáveis. O TikTok possui alguns mecanismos que esclarecem o que considera serem boas práticas. Em respeito à autonomia progressiva, as ferramentas de privacidade devem também acompanhar o crescimento e maturidade do usuário. Por exemplo: Configuração de privacidade da conta (visibilidade da conta): Para usuários entre 13-15 anos: as contas são configuradas como privadas por padrão, restringindo quem pode segui-las, ver seus vídeos, ler suas biografias e interagir com seus conteúdos. Para usuários entre 16-17 anos: há a opção de escolha, mas se optar por não escolher, a conta é definida como privada. Envio de mensagens diretas: Para usuários entre 13-15 anos: não é permitido. Para usuários entre 16-17 anos: configura-se como desligadas por padrão, mas o usuário pode alterar para “amigos” e “amigos sugeridos”

(seguidores que o usuário segue de volta e pessoas provavelmente conhecidas). Para usuários +18: é possível, embora configura-se como padrão que as mensagens possam ser enviadas e recebidas por amigos. Downloads de vídeos criados pelos usuários: Para vídeos criados por usuários entre 13-15 anos: por padrão e sem possibilidade de alteração, outros usuários não podem fazer o download dos vídeos. Para vídeos criados por usuários entre 16-17 anos: por padrão, outros usuários não podem fazer o download dos vídeos, mas caso o usuário tenha optado por uma conta pública há a possibilidade de ativá-lo. Criação de adesivos a partir dos vídeos dos usuários: Vídeos criados por usuários entre 13-15 anos: ninguém pode criar adesivos. Vídeos criados por usuários entre 16-17 anos com contas públicas: por padrão, o controle é ativado apenas para "amigos". Hospedagem de LIVES: só é permitido para usuários com mais de 18 anos. Limite de tempo de tela: Usuários entre 13-17: por padrão, esta configuração fica definida como uma hora. Notificações silenciosas: há autonomia para os pais definirem um cronograma para silenciar as notificações para contas de adolescentes. No entanto, por padrão: Para usuários entre 13-15 anos: notificações são desativadas a partir das 21h. Para usuários de 16-17 anos: notificações são desativadas a partir das 22h.Ferramentas de recomendação e de interação com conteúdo: Conteúdos criados por usuários entre 13-15 anos: Não aparecem no feed "Para Você". As configurações de comentários são restritas apenas para amigos, sem possibilidade de alteração. A configuração "Sugerir sua conta para outros" está desativada por padrão, e, mesmo quando ativada, contas de adolescentes não são recomendadas a adultos. Conteúdos criados por usuários entre 16-17 anos: passam a ser elegíveis para estarem no feed "Para Você". O ANEXO II apresenta, de forma visual [...] as medidas de design adotadas pelo TikTok para promover e assegurar níveis adequados de privacidade e proteção de dados aos seus usuários. Por fim, [...] o TikTok possui diversas medidas de transparência, direcionadas tanto para os pais e responsáveis, quanto aos próprios adolescentes usuários (ver resposta III.5). Essas são algumas medidas - não exaustivas - que o TikTok implementou para garantir a privacidade e melhor interesse dos adolescentes que utilizam a plataforma. No entanto, chama atenção para o fato de que a autoridade deve levar em conta a necessidade de parâmetros flexíveis e adaptáveis para diferentes produtos e serviços, considerando a disponibilidade tecnológica, a natureza e o propósito de cada um. Além disso, é essencial considerar o princípio do melhor esforço ao implementar essas medidas, garantindo que as soluções adotadas sejam práticas e proporcionais às capacidades e recursos de cada empresa.","708762":"O TikTok destaca que orientações claras da ANPD são necessárias para a segurança jurídica, dada a multiplicidade de disposições e atores na regulamentação. Parâmetros claros e flexíveis são cruciais para garantir práticas eficazes e proporcionais, respeitando a proteção dos dados dos menores e sua autonomia progressiva. (...) O TikTok chama atenção para alguns temas que a ANPD deve levar em conta na formulação destas orientações. Em primeiro lugar, o fato de que a verificação da idade dos usuários apresenta desafios técnicos que podem variar significativamente conforme a natureza do serviço. As orientações devem reconhecer que não há um único método de verificação superior a outros, pois a escolha depende do contexto específico, incluindo a finalidade e a natureza do tratamento dos dados, bem como o modelo de negócios envolvido. Além disso, não há um mecanismo infalível ou sempre superior em todos os contextos. As orientações da ANPD devem considerar a necessidade de avaliar o

cenário e a razoabilidade das ferramentas de verificação de idade para garantir sua eficácia e pertinência, considerando ainda a tecnologia atualmente disponível que seja minimamente segura para tal finalidade. (...) A possibilidade de as crianças burlarem verificações, como usar o celular dos pais, exemplifica a falibilidade inerente dessas medidas. Exigir que plataformas imponham controles exageradamente rígidos além da busca ativa de menores (o que já é uma realidade para muitas plataformas que se preocupam em manter menores de 13 anos fora da plataforma) tende a ser desproporcional e tecnicamente desafiador. (...) Adicionalmente, impor uma responsabilidade jurídica à plataforma que contrarie a decisão dos pais ou responsáveis pode ser desproporcional. (...) Por fim, a autoridade deve considerar que as medidas de verificação de idade representam um desafio para toda a indústria e levantam potenciais riscos à privacidade. Há debates importantes sobre a necessidade de equilibrar os riscos dos mecanismos de verificação de idade. Por exemplo, a Electronic Frontier Foundation (EFF) indicou, em 2023, que “os sistemas de verificação de idade são sistemas de vigilância” e, por isso, colocou-se contrária a leis que obriguem a sua implementação. Conforme já indicado anteriormente, seria importante que a autoridade levasse em consideração, por exemplo, o princípio da minimização de dados em conjunto com o do melhor interesse, visto que ferramentas mais robustas podem implicar em maior coleta de dados, embora em certos casos garantam mais segurança e proteção. O TikTok, inclusive, possui um sistema de verificação de idade neutro (que exige a inserção da data exata do nascimento pelo titular) para acesso à sua plataforma - destinada para usuários com mais de 13 anos - que busca equilibrar esses riscos. [Para referência visual das ferramentas de verificação de idade para o acesso à plataforma ver o ANEXO III]. Destaca-se que a empresa busca equilibrar os riscos à privacidade com a necessidade de mecanismos de detecção eficazes. O TikTok tem sido proativo na remoção de usuários menores de 13 anos, implementando uma combinação de tecnologia e trabalho humano para detectar e remover eventuais contas de menores de 13 anos presentes na plataforma, dando o devido cumprimento aos Termos e Condições de Uso. Além da identificação de menores, usuários podem denunciar contas, as quais serão revisadas por uma equipe devidamente capacitada para identificar e remover contas de usuários mais jovens que tenham eventualmente ingressado na plataforma. Há também verificação de idade para funcionalidades específicas na plataforma, nos casos em que o TikTok identificou um risco maior aos usuários mais jovens e tomou medidas para implementar níveis adicionais de verificação de idade. [Considerando a limitação de caracteres na plataforma Participa+ Brasil, a contribuição completa do TikTok com relação a essa pergunta pode ser acessada por meio da documentação enviada por e-mail à Coordenação-Geral de Normatização da ANPD.]","708764":"O TikTok entende que a coleta de dados pessoais de crianças e adolescentes não deve ser limitada para além daquelas proibições já explícitas na legislação (ou seja, finalidades ilícitas), ao menos não de forma absoluta e sem consideração contextual. Eventuais restrições devem levar em consideração violações ao melhor interesse desses titulares. Conforme já ressaltado, o fornecimento de balizas sobre o melhor interesse ajudaria a esclarecer esse ponto. Com relação à natureza dos dados, a LGPD e outras legislações não trazem qualquer tipo de limitação ao tratamento de dados de crianças e adolescentes (nem mesmo caso envolvam dados pessoais sensíveis, por exemplo). Desde que os agentes de

tratamento indiquem uma base legal apropriada, adotem as medidas necessárias para garantir o cumprimento das obrigações da LGPD com relação a esses dados e que a atividade de tratamento seja compatível com o melhor interesse, não deve haver restrições para o tratamento de dados desses titulares. Já com relação às finalidades do tratamento, o TikTok reforça que a formação de perfis comportamentais não deve ser considerada como uma atividade de tratamento que representa risco inerente aos usuários, inclusive no caso de crianças e adolescentes. Conforme já indicado na pergunta I.2., o perfilamento para fins de direcionamento de conteúdo - i.e., para oferecer conteúdo relevante ao usuário, sem fins publicitários - pode permitir que os usuários entrem em contato somente com conteúdos apropriados à sua faixa etária, evitando que os adolescentes se exponham a conteúdo mais maduro quando da utilização desses serviços e produtos. Nesse sentido, a prática de perfilamento pode desempenhar papel fundamental na segurança de menores de idade, em conformidade com seu melhor interesse. Em concreto, a implementação dos "Níveis de Conteúdo" no TikTok é um exemplo. Para usuários entre 13 e 18 anos, o TikTok implementa medidas para que o conteúdo seja exibido de acordo com o nível de maturidade do titular. Em respeito à autonomia progressiva, essa ferramenta permite que adolescentes explorem e interajam com a plataforma de maneira adequada ao seu estágio de desenvolvimento, respeitando sua capacidade crescente de tomar decisões informadas e independentes. Ao limitar conteúdo mais maduro, o perfilamento protege os jovens enquanto apoia seu desenvolvimento, garantindo que a experiência online seja segura e apropriada para sua idade e maturidade. Alguns mecanismos disponíveis no modo de “sincronização familiar” (i.e., controle parental, conforme explicado na questão abaixo) também dependem de mecanismos que consigam adequar o conteúdo ao público-alvo - tais como os filtros necessários para possibilitar que os pais e responsáveis limitem a exposição de seus filhos adolescentes a conteúdo que pode não ser apropriado ou adequado para eles (i.e., configuração “modo restrito”). Nesse sentido, restrições a atividades de perfilamento devem ser impostas devido à violação do melhor interesse da criança e do adolescente, conforme as leis do panorama regulatório brasileiro, e não simplesmente pela realização da atividade em abstrato.","708768":"O TikTok entende que medidas de proteção de privacidade para menores devem ser adaptáveis aos níveis de maturidade e autonomia de cada usuário em desenvolvimento, respeitando a autonomia progressiva. Assim, as configurações de privacidade não devem ser excessivamente rígidas, mas flexíveis e adequadas, permitindo ajustes que correspondam ao conteúdo apropriado para a idade, ao estágio de desenvolvimento do usuário e ao modelo de negócio em questão. Essa abordagem reconhece que diferentes idades e níveis de compreensão requerem diferentes níveis de proteção e interação, levando em conta a autonomia progressiva e, portanto, o melhor interesse da criança e do adolescente, conforme exige a legislação brasileira. O já citado Guia da ICO menciona a Convenção das Nações Unidas sobre os Direitos da Criança (UNCRC), que indica reconhecer o direito do menor de acordo com suas capacidades em evolução, de ter voz em assuntos que a afetam. No capítulo sobre controle parental, o Guia exemplifica essa abordagem, indicando, dentre outros fatores, que é necessário que pais e responsáveis sejam transparentes com as crianças e adolescentes caso os controles parentais estejam ativados e caso estejam sendo rastreados e/ou monitorados. (...) Como exemplo deste tipo de

mecanismo, o TikTok possui a ferramenta de sincronização familiar, que permite a vinculação das contas dos pais às dos filhos adolescentes, facilitando a gestão de configurações relacionadas a conteúdo, privacidade e bem-estar. Com esta ferramenta, pais, mães ou responsáveis podem configurar controles específicos visando à segurança do usuário adolescente. Este modo de sincronização familiar permite que pais e responsáveis personalizem configurações, como o tempo de tela diário. Os responsáveis podem ajustar o tempo de uso, aplicá-lo a todos os dispositivos do adolescente e definir um código de acesso para uso adicional após o limite ser atingido. Além disso, a ferramenta permite a ativação do Modo Restrito, que reduz a visualização de conteúdos potencialmente inadequados para certos públicos, como temas maduros ou complexos. Ao ativar este modo, algumas funcionalidades da plataforma são desabilitadas. (...) O TikTok também reforça a importância da promoção da cultura de diálogo dos pais e responsáveis com os menores, e o papel que a ANPD pode desempenhar nesse contexto. Incentivar os pais e responsáveis a discutir e explicar a ativação dessas configurações com os adolescentes é fundamental, pois a proteção da segurança, privacidade e autonomia progressiva do menor também é responsabilidade da família, conforme determina o Artigo 5 da Convenção sobre os Direitos da Criança1. Tendo isso em vista, o TikTok elabora guias direcionados especificamente aos pais e responsáveis, com linguagem clara e transparente, facilitando a navegação na plataforma e o entendimento das ferramentas e mecanismos disponíveis para auxiliá-los em seu dever de supervisão. Especificamente, o Guia para Pais e Responsáveis explicitamente incentiva a discussão dos recursos de Controle Parental com os adolescentes e explica a decisão de ativá-los. (...) Outro exemplo de boa prática é a exibição de uma tela de aviso, para usuários entre 13 e 18 anos, que incentiva os adolescentes a manterem seus pais ou responsáveis legais informados sobre o uso do aplicativo. Ao exibir o aviso de forma clara e proeminente, a tela funciona tanto como um lembrete de que os pais e responsáveis legais devem ser informados sobre o uso do TikTok, quanto como uma ferramenta educacional para os usuários menores. O aviso enfatiza efetivamente a importância da supervisão parental e contribui para uma experiência online segura para menores. Para uma referência visual de algumas das medidas implementadas pelo TikTok para manter o ambiente seguro e de apoio para famílias e adolescentes, ver o ANEXO IV. [Considerando a limitação de caracteres na plataforma Participa+ Brasil, a contribuição completa do TikTok com relação a essa pergunta pode ser acessada por meio da documentação enviada por e-mail à Coordenação-Geral de Normatização da ANPD.]","708772":"O TikTok entende que, com relação à transparência e ao fornecimento de informações simples, claras e acessíveis, há algumas boas práticas que podem ser observadas pelos mais diversos agentes de tratamento de forma adaptável a seus modelos de negócios, natureza do produto/serviço e tendo em vista as tecnologias disponíveis. A primeira delas consiste no entendimento de que a Política de Privacidade (“PP”), embora instrumento fundamental e indispensável, não precisa ser exibida constantemente para o usuário e/ou ao seu responsável legal, como fonte exclusiva de informação sobre tratamentos, sob o risco de resultar em fadiga. A exibição contínua da PP pode causar desatenção e desinteresse, reduzindo a eficácia da comunicação e a compreensão das informações importantes. O usuário pode ignorar alertas críticos, comprometendo a transparência e a confiança no tratamento de dados. Para evitar essa sobrecarga e garantir

uma comunicação efetiva, o TikTok entende como mais eficiente apresentar a PP e outras informações em momentos específicos e relevantes (e.g., relacionados diretamente a um determinado tratamento), assegurando que o usuário esteja atento e receptivo às informações necessárias. As informações fornecidas aos usuários ou pais precisam ser específicas e facilmente compreensíveis. Assim, apenas aumentar a quantidade de informações não garante maior transparência, especialmente se estiverem diante de informações complexas. O TikTok, em particular, opta por manter a PP visível e em local de fácil acesso, na página inicial da plataforma. A empresa não apenas deixa a PP visível, mas também fornece um link para a "Central de Privacidade", que direciona o usuário a uma página explicando, de forma breve e simples, a preocupação da empresa com a privacidade, contextualizando-o antes de direcioná-lo à PP. Outros meios além da PP são bem-vindos e corroboram com o dever de transparência. Ausente a proibição legal de que a PP seja o único meio para fornecer transparência, informações adicionais sobre o tratamento de menores podem ser incluídas em documentos separados, como artigos na central de transparência e ajuda, ou mesmo notícias veiculadas pelos agentes, que indiquem como os dados tratados estão associados a finalidades legítimas, específicas, explícitas e informadas ao titular. A especificidade da transparência pode ser desenvolvida em outros recursos, especialmente durante a utilização de produtos e serviços pelos adolescentes, através de notificações, por exemplo. A transparência fornecida deve ser adequada aos usuários. Para isso, o TikTok entende que meios como portais podem facilitar a compreensão das informações por adolescentes, em particular ao incorporar ícones visuais, vídeos, áudios, conteúdo interativo e linguagem simplificada e cotidiana a este público. É também importante dar suporte e fornecer transparência apropriada aos pais e responsáveis legais, para que tenham acesso a informações sobre as práticas de tratamento de dados pessoais realizadas, recursos de supervisão parental, entre outros. Nesse contexto, o TikTok reconhece a importância de permitir que os agentes de tratamento sejam criativos na elaboração de instrumentos de transparência. Ressalta-se, no entanto, que a autoridade deve levar em conta que a transparência deve observar os limites técnicos e os segredos comerciais e industriais dos agentes de tratamento. Fornecer informações excessivas sobre as ferramentas de tratamento de dados de menores pode permitir que agentes mal-intencionados burlem mecanismos de segurança, colocando em risco a segurança desses usuários. Portanto, é necessário estabelecer uma transparência adequada, visando os melhores interesses desses titulares. Por fim, é importante manter uma parceria constante com pais, responsáveis legais e os próprios adolescentes para melhorar os recursos de transparência disponíveis, visando aumentar a compreensão das definições de privacidade e segurança.","708775":"Por fim, o TikTok entende que há um outro ponto que merece atenção da autoridade no que diz respeito a orientações de tratamento de dados pessoais de crianças e adolescentes: É necessário que a autoridade se manifeste sobre os requisitos para a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a identificação de tratamentos de dados pessoais de alto risco. Atualmente, a existência de dados pessoais de crianças e adolescentes é considerada um critério para classificar um tratamento de dados como de alto risco. No entanto, estabelecer automaticamente essa classificação pode trazer consequências negativas e ineficiências. Por exemplo, tratamentos de dados que não deveriam ser considerados de alto risco podem ser inadvertidamente classificados dessa forma apenas por envolverem dados de menores. Isso

pode resultar em processos excessivamente rigorosos e desnecessários para certos tratamentos de dados, sobrecarregando os controladores e desviando recursos que poderiam ser melhor empregados em áreas realmente críticas. Portanto, é crucial que a autoridade forneça orientações claras e específicas sobre como identificar e tratar dados pessoais de crianças e adolescentes, evitando generalizações que possam levar a ineficiências e classificações equivocadas.

Contribuinte: Isabella de Castro Satiro Aragão

Número: OP-753211

Data: 16/08/2024 - 18:42

Resumo: :"A elaboração de um Relatório de Impacto à Proteção de Dados (“RIPD”) é mencionada como uma ferramenta para auxiliar na avaliação do melhor interesse da criança e do adolescente. No entanto, a regulamentação pode ser necessária para detalhar os requisitos específicos do RIPD no contexto de dados de crianças e adolescentes, incluindo quais riscos devem ser avaliados e como as medidas de mitigação devem ser implementadas. Ademais, embora o guia sugira a adoção de medidas de mitigação de risco, faltam detalhes sobre quais medidas são consideradas adequadas em diferentes situações. A ANPD poderia regulamentar padrões mínimos de segurança e mitigação de riscos específicos para o tratamento de dados de crianças e adolescentes. O Guia Orientativo menciona que o melhor interesse da criança deve ser considerado em todas as decisões que afetem crianças e adolescentes. No entanto, não detalha os critérios específicos ou métodos para avaliar o melhor interesse no contexto do tratamento de dados pessoais, de modo que a regulamentação poderia fornecer orientações mais claras e melhores práticas. Em certas situações, o melhor interesse do menor pode não estar alinhado com os interesses dos pais. Portanto, é essencial fornecer orientações mais claras a respeito dos limites que separam o melhor interesse da criança ou do adolescente da autonomia e dos interesses parentais. Essa distinção é fundamental para garantir que as decisões tomadas considerem adequadamente os direitos e bem-estar dos menores, ao mesmo tempo em que respeitam a autoridade dos responsáveis. É fundamental oferecer uma orientação mais clara sobre a autonomia progressiva dos menores relativamente capazes na utilização da base legal para a execução de contratos. De acordo com o Artigo 166 do Código Civil, contratos assinados por indivíduos absolutamente incapazes são nulos. Portanto, é imprescindível estabelecer diretrizes que abordem as especificidades e implicações de um contrato assinado por um relativamente incapaz, de modo a proteger os direitos desses menores e garantir a validade das suas decisões contratuais em situações adequadas. Por fim, um guia orientativo deve ser elaborado para esclarecer quem é responsável por definir o que constitui o melhor interesse da criança, além de fornecer exemplos práticos desse conceito. É igualmente importante incluir situações excepcionais nas quais o melhor interesse do menor pode não prevalecer, garantindo assim uma compreensão abrangente e contextualizada. Essa orientação ajudará profissionais e responsáveis a tomar decisões mais informadas e equilibradas, reconhecendo as nuances e complexidades envolvidas na proteção dos direitos das crianças e adolescentes. ","708725":"Sim, temas como profiling, tratamento automatizado

de dados, sharenting/oversharing, e situações que podem resultar em discriminação exigem uma abordagem mais cuidadosa. ","705523":"Para obter o consentimento "específico e em destaque" dos responsáveis legais, o controlador deve verificar se quem assina em nome do menor tem a capacidade legal para fazê-lo. Além disso, para que o consentimento seja válido, todas as informações sobre produtos, serviços e fornecedores devem ser claras, com atendimento acessível ao consumidor e respeito ao direito de arrependimento. A implementação de uma ação afirmativa específica, como a prática do "clique separado", pode garantir que o consentimento seja apresentado de forma destacada e em específico. ","708742":"Entre as medidas e mecanismos que os controladores devem adotar para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança estão: · adoção de perguntas específicas de verificação de idade; · implementação de sistemas de autenticação seguros; · confirmação por E-mail dos pais ou responsáveis. Porém, as medidas devem ser baseadas em riscos, quanto mais arriscado, mais criterioso deve ser o método de verificação. ","708745":"A autonomia progressiva deve ser reconhecida a partir dos 16 anos, em consonância com as disposições estabelecidas em outras normas que regulamentam a capacidade civil. Essa autonomia é fundamental para que os jovens possam exercer um maior controle sobre suas decisões e atividades, especialmente no que diz respeito ao tratamento de seus dados pessoais. ","705539":"É crucial que as medidas sejam factíveis e viáveis dentro do contexto operacional e tecnológico das empresas. A.

Princípios/Parâmetros 1. Princípios da LGPD: Os princípios da finalidade, necessidade e adequação são fundamentais para nortear o tratamento de dados pessoais de crianças e adolescentes. 2. Proteção da Privacidade desde a Concepção: incorporar a proteção de dados nas práticas de desenvolvimento de produtos e serviços desde sua concepção, garantindo a segurança e privacidade dos dados dos usuários. B.

Salvaguardas 1. Verificação de Idade e Restrição de Acesso (sem coleta massiva de dados) 2. Limitação na Coleta e Formação de Perfis Comportamentais 3. Disponibilização de mecanismos de controle parental 4. Disponibilização de recursos educacionais sobre privacidade e segurança cibernética 6. Treinamento de Funcionário 7. Canais de Denúncia e Suporte 8. Certificações de Segurança e Privacidade reconhecidas 9. Notificações Claras e Consentimento Informado: Garantir que as notificações sobre o tratamento de dados sejam claras, concisas e compreensíveis para os usuários mais jovens 10. Opções de Privacidade Configuráveis: Oferecer aos usuários jovens a capacidade de configurar suas preferências de privacidade de forma clara e intuitiva. Isso pode incluir controles de privacidade granulares que permitam ajustar quem pode acessar seus dados, quais informações são compartilhadas e como são utilizadas. 11. Autenticação Multifatorial: Implementar a autenticação multifatorial como uma camada adicional de segurança para garantir que apenas usuários autorizados possam acessar dados pessoais sensíveis. Esse método de verificação de identidade reduz significativamente o risco de acesso não autorizado. ","708762":"1. Perguntas de Verificação de Idade: Solicitar ao usuário que forneça sua data de nascimento ou responda a perguntas relacionadas à sua idade, práticas comumente usadas pelas grandes plataformas. 2. Confirmação por E-mail dos Pais ou Responsáveis: 3. Confirmação Presencial de Adultos de Confiança: Permitir que outros adultos de confiança, como avós, professores ou tios/tias, participem no processo de verificação de idade. Os exemplos mencionados anteriormente

deveriam ser incluídos em um guia orientativo. A resolução poderia estabelecer parâmetros claros, indicando que, quanto mais arriscado for o tratamento de dados pessoais, mais rigorosos devem ser os meios de verificação adotados. O nível máximo de exigência deve ser reservado para produtos e serviços que são expressamente proibidos para menores. Essa abordagem garantirá uma proteção mais eficaz dos direitos dos jovens, assegurando que os tratamentos de dados pessoais sejam realizados de maneira responsável e em conformidade com a legislação vigente. ","708764":"A transparência e informação deve guiar a coleta de dados, por exemplo, com indicação expressa sobre o tratamento de dados das crianças e adolescentes na política de privacidade das plataformas digitais. Outro ponto relevante é a formação de perfis comportamentais de crianças e adolescentes. Essa prática deve ser tratada com especial cautela. Por isso, é essencial garantir que a formação de perfis não viole a privacidade ou gere impactos negativos nos usuários mais jovens. Além disso, o tratamento inadequado de dados também pode levar à perpetuação de preconceitos e à discriminação, exacerbando desigualdades sociais e prejudicando grupos vulneráveis. ","708768":"No ato de coleta do consentimento, além da veiculação de informações na forma do art. 14, §6º, da LGPD, um mecanismo que poderia ser utilizado é a apresentação apartada de cada uma das finalidades às quais se está fornecendo consentimento, favorecendo um consentimento informado e a obtenção granular deste. Para tanto, é possível o uso de checkboxes, para que o pai ou responsável conceda o consentimento a cada uma das finalidades individualmente, selecionando as caixas de seleção individualmente. Com isso, aquele que consente com o tratamento de dados terá um controle mais amplo sobre as finalidades para as quais tal atividade será realizada. A ampliação desse controle sobre o tratamento de dados pessoais de crianças e adolescentes pode ser ampliado, também, no momento ulterior à coleta do consentimento. Para tal finalidade, os agentes de tratamento podem adotar mecanismos que ampliem o conhecimento de pais e responsáveis sobre os direitos assegurados aos titulares dos dados pessoais objeto de tratamento e a forma de exercício desses direitos. Para isso, é possível que, antes da conclusão da coleta do consentimento, seja exibida mensagem específica veiculando tais informações de forma simples, clara e acessível (14, §6º, da LGPD), além de indicar como os pais e responsáveis podem voltar a consultar tais informações após a coleta do consentimento. Ademais, o mecanismo da checkboxes também poderia ser utilizado, para que o pai ou responsável sinalize, individualmente, a ciência quanto a cada uma das informações veiculadas. Nesse sentido, a realização de campanhas e disponibilização pública de materiais informativos em linguagem simples e acessível, com formatos diversos, que permitam que pais e responsáveis adquiram e aprofundem o conhecimento acerca do processo de consentimento de tratamento de dados de crianças e adolescentes, bem como dos direitos dos titulares dos dados. Em ferramentas de controle parental, a disponibilização de configuração de privacidade para restringir determinados recursos do aplicativo pode também ser uma boa prática. ","708772":"Dentre as boas práticas que podem ser adotadas em prol da transparência, pode-se citar a indicação destacada, na coleta de consentimento, dos tipos de dados coletados e a forma de sua utilização. Para tanto, além dessa especificação, se cabível, deverão ser indicados exemplos e situações práticas que ilustrem as informações indicadas, permitindo que esse seja adequadamente assimilada pelos pais e responsáveis, assim como pelas crianças e adolescentes. Quanto às boas práticas na

veiculação de informações, pode-se citar o uso de recursos visuais na veiculação de informações durante a coleta de consentimento, como o uso de fontes de tamanho adequado, com destaques e, se necessário, tabelas, ilustrações e recursos audiovisuais que auxiliem a compreensão das informações veiculadas. Nesse sentido, a disponibilização de materiais públicos e informativos, em formatos diversos (Por exemplo, curta animado, quadrinhos e banners) – escrito, ilustrado e audiovisual – e com linguagem acessível, com informações sobre o processo de tratamento de dados pessoais de crianças e adolescentes também colaboraria para tal fim. Por exemplo, curta animado, quadrinhos e banners. Ademais, também nessa linha, pode-se citar a possibilidade de disponibilização de canais de contato por onde pais e responsáveis possam elucidar eventuais dúvidas acerca do tratamento de dados pessoais de crianças e adolescentes pelo agente de tratamento titular do canal. O informe adequado de eventuais atualizações da política de tratamento de dados dos agentes de tratamento. Assim, eventuais atualizações poderiam ser comunicadas aos pais ou responsável, por e-mail ou outros canais, com indicação simples, clara e acessível das alterações feitas. Por fim, é essencial que os marcadores utilizem uma linguagem simples e acessível, a fim de sintetizar as informações contidas no termo de consentimento do site. Dessa forma, qualquer pessoa, independentemente de sua escolaridade ou idade, poderá compreender o que está concordando. Essa abordagem garante que os usuários possam tomar decisões claras e informadas sobre o uso de seus dados pessoais, promovendo um ambiente digital mais transparente e responsável. ","708775":"N/A

Contribuinte: Bruna Borghi Tomé

Número: OP-753216

Data: 16/08/2024 - 18:46

Resumo: :"A ANPD ressaltou a importância de adotar o princípio do melhor interesse nas discussões sobre a proteção de crianças e adolescentes, mas não definiu claramente o escopo desse princípio. Embora tenha se baseado em diretrizes da OCDE e da ONU para delinear o 'melhor interesse' de crianças e adolescentes, essas orientações ainda não oferecem segurança suficiente para que os controladores de dados atuem com confiança no contexto da proteção de dados pessoais, conforme o Guia do Legítimo Interesse. Portanto, é crucial que a autoridade aproveite a oportunidade para esclarecer o que constitui o melhor interesse de crianças e adolescentes no âmbito da proteção de dados, especialmente considerando as particularidades da interpretação deste princípio nesta seara. Por exemplo, ao avaliar mecanismos de verificação de idade, que muitas vezes requerem maior coleta de dados para maior precisão, surge a questão: o que deve prevalecer como o melhor interesse da criança e do adolescente? Mecanismos mais precisos ou a adesão rigorosa ao princípio da minimização de dados? O Comentário Geral n.º 25 da Convenção sobre os Direitos da Criança da ONU destaca a importância de considerar as particularidades de cada contexto específico nessa definição. Diante das diversas realidades e desigualdades socioeconômicas que afetam o acesso de crianças e adolescentes aos meios de comunicação, bem como os diferentes contextos e modelos de negócios, é fundamental que a ANPD dê maior concretude ao

conceito de melhor interesse. Isso poderia ser feito por meio de exemplos práticos e situações hipotéticas, elucidando os critérios que serão aplicados na proteção de dados de crianças e adolescentes no ambiente digital. Sugere-se que a ANPD continue a fornecer orientações claras sobre o que constitui o melhor interesse da criança e do adolescente em situações específicas, especialmente por meio de guias e documentos com eficácia geral. Esses documentos, alinhados com o conceito de crianças e adolescentes estabelecido pelo ECA, ofereceriam maior segurança jurídica, permitindo que os agentes ajustem suas práticas de acordo com parâmetros estabelecidos.","708725":"Considerando os diferentes contextos socioeconômicos não apenas de crianças e adolescentes, mas também de seus pais e responsáveis, é fundamental que a Autoridade dê especial atenção ao definir o melhor interesse em situações concretas. A diversidade dessas realidades traz consigo múltiplas possibilidades de garantir, ou não, a observância desse princípio, o que, dada a sensibilidade do tema, requer uma abordagem cuidadosa. Em certos cenários, o princípio do melhor interesse precisa ser equilibrado com outros princípios da LGPD — como a tensão entre acurácia e minimização de dados, por exemplo. Esses são os casos que exigem um esforço adicional de esclarecimento por parte da Autoridade. Além disso, dado que a cultura de proteção de dados pessoais no Brasil ainda está em processo de consolidação, é natural que haja dificuldades em compreender e aplicar os parâmetros que a ANPD usará em situações práticas. Por isso, é de suma importância que sejam estabelecidas diretrizes claras para orientar os agentes na tomada de decisões em diferentes contextos. Isso inclui, por exemplo, orientações específicas sobre as regras que as redes sociais devem seguir na coleta e armazenamento de informações, sobre mecanismos de verificação e identificação de idade, e nas particularidades do uso de dados pessoais de crianças e adolescentes para fins de direcionamento de conteúdo. Nesse contexto, é crucial distinguir a personalização do conteúdo exibido da publicidade direcionada, visto que, nesse caso, a personalização visa, em muitos casos, proteger as crianças e adolescentes.","705523":"Vale destacar que o consentimento nem sempre será a base legal mais adequada para o tratamento de dados pessoais de crianças e adolescentes, conforme indicado pela ANPD em documentos como o Enunciado nº 01/2023 e o Guia de Legítimo Interesse. No entanto, quando o consentimento parental é necessário, ele deve ser adequado ao contexto específico entre o titular, o responsável legal e o agente de tratamento. Isso implica que diferentes situações demandam abordagens personalizadas. Por exemplo, em interações que ocorrem exclusivamente offline, não faria sentido exigir um consentimento digital "específico e em destaque", assim como o inverso. Além disso, é importante notar que os termos “específico e em destaque” não têm o mesmo significado que “livre, informado e inequívoco” na LGPD. Por isso, a ANPD precisa esclarecer a que se refere a especificidade — se está relacionada às finalidades do tratamento, ao titular em particular, ou ao conjunto de dados. No que tange ao “destaque”, isso geralmente significa que a informação deve ser destacada em relação a outras. Contudo, seria útil que a ANPD detalhasse se isso envolve a utilização de elementos visuais específicos, como cores e fontes que garantam uma diferenciação clara. Exemplos de boas práticas poderiam incluir o uso de pop-ups, banners destacados, animações ou ícones chamativos, alertas com cores contrastantes, entre outros, para assegurar que o consentimento seja claramente visível.","708742":"Quando o consentimento é adotado como base legal,

especialmente no tratamento de dados pessoais de crianças e adolescentes, é fundamental que sua obtenção seja a menos invasiva possível em termos de privacidade, conforme reconhecido por autoridades internacionais. A Children's Online Privacy Protection Rule (COPPA), sob a administração da FTC, apesar de estabelecer o consentimento dos pais ou responsáveis como regra, também prevê exceções claras e objetivas. A ANPD deve levar em consideração os esforços razoáveis empreendidos pelos controladores para obter e verificar o consentimento parental, utilizando métodos acessíveis e proporcionais ao contexto específico. Por exemplo, no setor financeiro, onde a validação biométrica já é amplamente utilizada, a documentoscopia — que consiste na análise de documentos para comprovar a identidade — pode ser uma solução viável. Este método, recomendado pelo COPPA, envolve a verificação de uma foto de uma identificação oficial enviada pelo pai ou responsável, comparada com uma segunda foto utilizando tecnologia de reconhecimento facial. Além disso, é crucial que a autoridade reconheça que não existem mecanismos infalíveis, e todos estão sujeitos a algum nível de vulnerabilidade. O IBRAC destaca a importância de considerar este aspecto ao determinar a responsabilidade dos agentes de tratamento em casos de falhas nos mecanismos de consentimento. Imposições desproporcionais e onerosas aos agentes de tratamento podem comprometer a eficácia dos processos e serem ignoradas pelos usuários, contrariando os objetivos da LGPD. Considerando que a cultura de proteção de dados no Brasil ainda está em desenvolvimento, é prudente que a autoridade evite estabelecer parâmetros excessivamente rígidos, cuja conformidade possa ser inviável, sem prejuízo de revisões futuras. A obtenção do consentimento dos pais ou responsáveis deve observar os princípios de razoabilidade, proporcionalidade e minimização, garantindo que o esforço exigido para obtê-lo não seja excessivo ou desnecessário. É essencial oferecer uma variedade de mecanismos para que o controlador possa escolher o que melhor se adapta à sua realidade específica, sem causar impacto negativo significativo em suas operações. Assim, o processo de consentimento pode ser ajustado às necessidades operacionais do controlador, assegurando, ao mesmo tempo, a proteção e os direitos dos menores envolvidos.","708745":"Embora a obtenção do consentimento seja uma base legal importante para o tratamento de dados pessoais de crianças e adolescentes, nem sempre será a mais apropriada, dependendo do caso concreto. Compreender esse elemento como o único possível pode levar a restrições excessivas, mesmo quando o tratamento é realizado no melhor interesse da criança. Um exemplo dessa necessidade de ponderação é o posicionamento da ANPD no Enunciado nº 1/2023. Esse enunciado estabelece que é possível utilizar as hipóteses legais previstas no art. 7º da LGPD, incluindo o legítimo interesse, para o tratamento de dados pessoais de crianças e adolescentes, além das disposições do art. 11 da mesma lei, sempre observando o princípio do melhor interesse da criança ou adolescente. Tal posicionamento é reforçado no Guia de Legítimo Interesse, que oferece orientações para controladores sobre a interpretação e a aplicação prática dessa hipótese legal, precedida da realização de um teste de balanceamento. No entanto, se o consentimento for a base legal escolhida para o tratamento de dados de crianças e adolescentes, é crucial que a autoridade reguladora considere alguns aspectos. Primeiro, a legislação brasileira apresenta diferentes definições e capacidades legais para crianças e adolescentes, o que pode causar ambiguidades na aplicação do consentimento como base legal. O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) define

"criança" como a pessoa até 12 anos e "adolescente" como aquela entre 12 e 18 anos. O Código Civil Brasileiro estabelece que menores de 16 anos são absolutamente incapazes de exercer pessoalmente os atos da vida civil e aqueles com mais de 16 e menos de 18 anos são relativamente capazes, podendo praticar atos da vida civil desde que assistidos. A definição exata de "atos da vida civil" não é clara, criando uma zona cinzenta que pode complicar a aplicação do consentimento como base legal, especialmente em situações que exigem um entendimento preciso das capacidades legais desses menores. Segundo, o melhor interesse deve refletir a autonomia progressiva e o desenvolvimento desses indivíduos, podendo tornar desnecessária a representação ou assistência pelos pais ou responsáveis legais. Conforme reconhecido pelo Estatuto da Criança e do Adolescente (ECA), a autonomia progressiva estabelece que crianças e adolescentes devem ter sua capacidade de decisão respeitada e ampliada à medida que crescem e amadurecem. Isso cria um cenário complexo, em que as disposições do Código Civil, ao tratar menores de 16 anos como uma massa homogênea incapaz, podem obstruir o melhor interesse da criança e do adolescente. Em contraste, outras jurisdições, como o Reino Unido, permitem que crianças a partir dos 13 anos forneçam seu próprio consentimento para o processamento de dados no contexto de serviços online, conforme definido no Age Appropriate Design Code (Best interests of the child; Annex B). Além disso, o GDPR permite que os Estados Membros da União Europeia estipulem, por lei, uma idade inferior a 16 anos para o tratamento de dados pessoais de menores sem autorização do responsável legal, desde que essa idade não seja inferior a 13 anos. Portanto, em alinhamento com os padrões internacionais de obtenção de consentimento como base legal e em respeito à autonomia progressiva dos menores, é importante que o posicionamento da ANPD reflita adequadamente o desenvolvimento individual e as capacidades crescentes de decisão dos jovens. Ademais, se a obtenção de consentimento seguir as disposições do direito civil sobre representação e assistência de pais ou responsáveis dos adolescentes, é crucial que a autoridade reguladora esclareça alguns requisitos. Por exemplo, não há uma disposição específica no ordenamento jurídico brasileiro sobre como deve ser obtida a representação ou assistência e se, de fato, é necessária a obtenção de autorização explícita dos pais ou responsáveis por menores. Assim, é importante que a ANPD esclareça em quais situações o consentimento dos pais ou responsáveis é indispensável.","705539":"A ANPD deve fornecer orientações claras aos controladores sobre como equilibrar a minimização de dados com o melhor interesse de crianças e adolescentes, estabelecendo parâmetros precisos para a coleta adequada de informações e as medidas de segurança necessárias para protegê-las. Isso inclui diretrizes sobre o uso de técnicas como pseudonimização e criptografia, bem como a importância de realizar avaliações de impacto à proteção de dados para identificar e mitigar riscos. Além disso, é fundamental que a ANPD ofereça diretrizes de boas práticas às plataformas digitais sobre como comunicar de forma clara e acessível a menores e seus responsáveis quais dados estão sendo coletados, a finalidade dessa coleta e como esses dados serão utilizados e protegidos. Nesse contexto, é relevante mencionar a Resolução nº 245 de 2024, do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA), que estabelece como as plataformas devem incorporar os direitos de crianças e adolescentes ao longo de todo o ciclo de vida de seus produtos. Entre os princípios orientadores estão a não discriminação, a primazia dos direitos da criança e do adolescente, o respeito à liberdade de

expressão e consciência, o acesso à informação, a autonomia progressiva, e o desenvolvimento da personalidade, dignidade, honra e imagem. Na implementação das medidas de privacy by design e privacy by default, é crucial que a autoridade reguladora oriente os agentes de tratamento sobre como equilibrar essas medidas com o respeito ao direito à autonomia progressiva das crianças e adolescentes. Um exemplo a ser considerado é o Age Appropriate Design Code do Reino Unido, que recomenda configurações padrão de "alta privacidade", a menos que haja uma justificativa forte para o contrário, sempre levando em conta o melhor interesse da criança. A ANPD deveria avaliar a viabilidade de adotar medidas mais protetivas como padrão, ao mesmo tempo oferecendo flexibilidade aos usuários para ajustá-las conforme necessário. Em alinhamento com o melhor interesse da criança, a ANPD poderia também sugerir medidas que permitam supervisão parental adequada, garantindo que os pais desempenhem um papel ativo na proteção dos dados dos menores, especialmente em ambientes digitais. Por fim, a autoridade deve orientar sobre a implementação de canais eficazes para o recebimento de denúncias relacionadas ao uso indevido de contas de crianças, além de mecanismos ágeis para a remoção dessas contas e a proteção dos dados envolvidos.","708762":"É essencial reconhecer que as técnicas disponíveis no mercado para verificação de idade são variadas, assim como os modelos de negócios e setores onde são aplicadas. Elas diferem em termos de eficácia, invasão à privacidade e segurança dos dados dos titulares, e esses fatores devem ser cuidadosamente avaliados em sua implementação, considerando os trade-offs envolvidos. Por exemplo, a autodeclaração, onde o próprio titular informa sua idade sem verificação externa, pode comprometer a acurácia. Outras técnicas, que buscam determinar a idade por meio de inferências, utilizando questionários, históricos de navegação ou análise do comportamento online, embora mais precisas, podem apresentar riscos de discriminação ao associar faixas etárias com habilidades como leitura, compreensão, proficiência linguística e referências culturais. A verificação de idade através de cartão de pagamento tem a vantagem de utilizar uma infraestrutura já existente e confiável. O sistema valida o cartão sem necessariamente processar um pagamento, embora alguns verificadores possam realizar um micropagamento que é imediatamente cancelado. Esse método pode ser utilizado até mesmo em sites gratuitos para restringir o acesso de menores. No entanto, como os sistemas de pagamento não foram concebidos para verificar atributos como a idade do titular, sua eficácia é limitada. Ainda assim, é uma barreira útil, pois, conforme a legislação brasileira, menores de idade não podem ser titulares de cartões de crédito, o que reduz a probabilidade de uso indevido por crianças e adolescentes. Contudo, essa abordagem apresenta limitações, especialmente devido à penetração desigual do uso de cartões de crédito no Brasil, o que poderia restringir o acesso a plataformas para populações sem acesso a esse meio de pagamento. Independentemente da técnica utilizada, é importante destacar que nenhum mecanismo de verificação de idade é infalível, especialmente considerando a capacidade de menores de idade de contornar essas barreiras, muitas vezes com a ajuda, consciente ou não, de pais e tutores. Portanto, ao invés de estabelecer regras rígidas, é crucial promover boas práticas que considerem as vantagens e limitações de cada sistema. Por fim, é fundamental que uma política prioritária seja a educação de pais e responsáveis sobre os riscos de segurança e privacidade enfrentados por crianças e adolescentes no uso de plataformas digitais.","708764":"Ao tratar os dados de

crianças e adolescentes, é fundamental que as informações sobre o tratamento sejam comunicadas de maneira clara e adaptada ao público-alvo, utilizando uma apresentação, design e linguagem que facilitem a compreensão do uso dos dados, especialmente na criação de perfis comportamentais. Vale destacar que essa prática pode atender ao melhor interesse dos menores ao direcionar conteúdos apropriados para sua idade. Por exemplo, no setor financeiro, a personalização de perfis pode ser utilizada para adaptar programas educativos ao nível de entendimento e interesse dos jovens, tornando o aprendizado mais eficaz. Além disso, perfis comportamentais podem identificar padrões incomuns ou riscos de fraude, protegendo os menores contra atividades financeiras prejudiciais. É importante lembrar que a LGPD não impõe restrições automáticas ao tratamento de dados de menores, desde que as bases legais sejam respeitadas e medidas de segurança adequadas sejam implementadas. Nesse contexto, a coleta de dados de crianças e adolescentes não deve ser limitada por padrão, exceto quando necessário para proteger seus melhores interesses. Em setores como o financeiro, a coleta de dados, incluindo a formação de perfis comportamentais, pode trazer benefícios significativos ao proporcionar segurança e ajudar os menores a desenvolver habilidades financeiras de forma segura e informada. O IBRAC destaca que o tratamento de dados deve ser analisado caso a caso, levando em consideração os riscos específicos associados à natureza dos dados e ao modelo de negócio envolvido. Por fim, é essencial que essas práticas sejam implementadas de maneira responsável e transparente, equilibrando a proteção dos dados pessoais com a promoção da autonomia e do desenvolvimento dos menores. O objetivo é garantir que o tratamento de dados, longe de ser prejudicial, possa contribuir positivamente para o bem-estar e a segurança de crianças e adolescentes, sempre respeitando os princípios da LGPD e o melhor interesse desses titulares.","708768":"A autonomia progressiva, conforme prevista no Estatuto da Criança e do Adolescente (ECA), exige que a capacidade de decisão das crianças e adolescentes seja respeitada e ampliada conforme seu crescimento e amadurecimento. Nesse contexto, é fundamental que a ANPD reconheça as especificidades desse setor e promova soluções que permitam a participação gradual e supervisionada dos jovens, transformando o controle parental em uma supervisão responsável, até que esses jovens alcancem a maioridade com uma autonomia financeira consolidada. As medidas de proteção à privacidade para menores devem ser adaptáveis aos diferentes níveis de maturidade e autonomia de cada usuário, respeitando o princípio da autonomia progressiva. Em vez de configurações de privacidade excessivamente rígidas, é crucial que essas medidas sejam flexíveis, permitindo ajustes que considerem o conteúdo apropriado para a idade, o estágio de desenvolvimento do usuário e o modelo de negócio em questão. Essa abordagem reconhece que diferentes idades e níveis de compreensão demandam graus variados de proteção e interação, sempre em conformidade com o melhor interesse da criança e do adolescente, conforme a legislação brasileira. A ampliação do controle por parte dos pais e responsáveis deve ser vista como uma assunção de maiores responsabilidades no uso de jogos e aplicativos de internet, considerando aspectos psicológicos e sociológicos. O controle parental deve ser entendido como uma medida voltada à segurança, e não como um estado constante de vigilância. O controle parental deve ser transparente. Recomenda-se que as crianças e adolescentes sejam informados de maneira clara sobre a existência e os limites desse controle, como, por exemplo, esclarecendo que os

pais ou responsáveis não teriam acesso a mensagens privadas trocadas com terceiros. O respeito à privacidade dos menores é essencial para garantir seu livre desenvolvimento, especialmente no caso de membros da comunidade LGBTQIAP+, conforme mencionado por alguns adolescentes no podcast Hard Fork, discutindo o livro de Jonathan Haidt. Por fim, é altamente recomendável disponibilizar controles parentais de fácil compreensão e utilização, que permitam aos pais monitorar o uso de aplicativos e jogos, independentemente da marca ou do sistema operacional dos dispositivos usados por seus filhos.","708772":"coletados, utilizados e protegidos. O Artigo 12 do General Data Protection Regulation (GDPR) da União Europeia exemplifica essa necessidade, exigindo que as informações fornecidas às crianças sejam acessíveis e compreensíveis. Esse artigo especifica que o controlador deve usar uma linguagem clara e simples, apresentando as informações de maneira concisa, transparente e de fácil acesso, seja por escrito, por meios eletrônicos ou, se solicitado, oralmente, desde que a identidade do solicitante seja confirmada. Essas informações devem estar presentes na Política de Privacidade dos agentes de tratamento e devem ser disponibilizadas em locais de fácil acesso. Para promover uma transparência adequada, é recomendável que os agentes de tratamento ofereçam portais e outros meios específicos que facilitem a compreensão das informações por crianças e adolescentes. Por exemplo, o Age Appropriate Design Code sugere o uso de explicações em pequenos pedaços, ou "bite-size", para ajudar os menores a entenderem como seus dados pessoais são utilizados. Além disso, para garantir o melhor interesse das crianças e adolescentes, é igualmente importante fornecer suporte e transparência apropriada aos pais e responsáveis legais. Eles devem ter acesso a informações claras sobre as práticas de tratamento de dados pessoais e os recursos de supervisão parental disponíveis. As plataformas devem manter pais e filhos informados sobre quaisquer mudanças nas práticas de tratamento de dados, comunicando claramente atualizações nas políticas de privacidade e termos de serviço. Oferecer canais de suporte e feedback para que os usuários possam esclarecer dúvidas ou expressar preocupações sobre privacidade e tratamento de dados é uma prática recomendada. Entretanto, é crucial que a ANPD considere os limites técnicos e a necessidade de proteger segredos comerciais e industriais dos agentes de tratamento ao exigir transparência. A divulgação excessiva de informações sobre as ferramentas de tratamento de dados de menores pode comprometer a segurança, facilitando a ação de agentes mal-intencionados. Assim, a transparência deve ser equilibrada, garantindo que as medidas de proteção dos dados das crianças e adolescentes permaneçam eficazes e seguras.","708775":" É crucial que a autoridade reguladora forneça orientações mais claras sobre as medidas de "privacy by default" que devem ser adotadas pelos agentes de tratamento ao processarem dados de crianças e adolescentes. Embora a legislação atual não imponha restrições específicas sobre o tratamento de certos tipos de dados pessoais, como geolocalização, perfilamento e publicidade direcionada, é importante que os controladores recebam diretrizes sobre quando esses tratamentos devem estar sujeitos a configurações de privacidade padrão. Além disso, é necessário integrar melhor esse tema com os requisitos para a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a identificação de tratamentos de dados pessoais de alto risco. A presença de dados de crianças e adolescentes deve ser um critério relevante para determinar a necessidade de um RIPD, juntamente com outros fatores, como o uso de tecnologias inovadoras,

perfilamento em larga escala, dados biométricos e rastreamento online. A regulamentação do tratamento de dados para fins de publicidade direcionada a crianças e adolescentes também é um aspecto fundamental. É essencial que esse tratamento seja disciplinado por critérios claros, garantindo que a publicidade seja apropriada para o público-alvo, além de assegurar transparência e o consentimento informado dos pais ou responsáveis. Por fim, é importante considerar o impacto das tecnologias emergentes, como a inteligência artificial, no tratamento de dados de crianças e adolescentes. Pode ser necessário estabelecer regulamentações adicionais para enfrentar os desafios específicos que essas tecnologias apresentam, garantindo que seu uso seja adequado e que os direitos das crianças e adolescentes sejam protegidos de maneira eficaz.

Contribuinte: MARCELA MATTIUZZO

Número: OP-753287

Data: 16/08/2024 - 20:06

Resumo: :"Em seu Guia Orientativo sobre a base legal do legítimo interesse, a ANPD dispõe, brevemente, sobre o melhor interesse da criança, reconhecendo se tratar de um conceito plurívoco e cuja observância deve ser prioritária em todas as operações de tratamento de dados pessoais de crianças e adolescentes. Dada a centralidade do conceito para a efetiva garantia dos direitos de crianças e adolescentes, seria interessante que a ANPD produzisse material que detalhe e sistematize as orientações já dadas aos controladores de dados pessoais no referido Guia, buscando conferir-lhes amplitude suficiente para que se apliquem plenamente a qualquer operação de tratamento de dados pessoais de crianças e adolescentes e não apenas àquelas que tenham por base legal o legítimo interesse do controlador. Nesse material, a ANPD poderia aprofundar o que deve ser entendido por tratar os dados de crianças e adolescentes em seu melhor interesse, como dispõe o art. 14, caput da LGPD, usando o Comentário Geral N. 14 como fio norteador e esclarecendo que o conceito abrange, no mínimo i) a priorização, em absoluto, da proteção dessas pessoas nas operações de tratamento de dados pessoais, devendo o controlador avaliar previamente se, na prática, poderá realizar o tratamento de dados pessoais de crianças e adolescentes e adotar medidas procedimentais para o resguardo dos seus direitos (como a elaboração de RIPD), implementar medidas de mitigação de riscos, adaptar os seus produtos e serviços para que incorporem os direitos das crianças e adolescentes em seu design e a monitorar a efetividade dessas medidas, prestando contas à sociedade; e ii) o respeito e a promoção dos direitos garantidos a essas pessoas à luz de suas circunstâncias concretas, levando em conta as suas opiniões e os insumos fornecidos por especialistas, especialmente nas situações em que houver possíveis conflitos de direitos. Destaca-se que a ANPD, no Guia relativo à base legal do legítimo interesse, determina que os controladores devem demonstrar “o que foi considerado como sendo o melhor interesse da criança ou do adolescente”, orientação que, apesar de absolutamente pertinente, poderia ser mais explorada, a partir de parâmetros nacionais e internacionais. Em termos sucintos, é preciso que a ANPD detalhe a aplicação da garantia do melhor interesse, que se desdobra tanto em deveres de conduta para os controladores

quanto na aferição das medidas que melhor atenderão à efetivação e proteção plena dos direitos das crianças e dos adolescentes a partir da consideração de suas circunstâncias concretas. O Instituto Alana, na contribuição apresentada à Coordenadoria Geral de fiscalização desta Autoridade no processo fiscalizatório nº 00261.000297/2021-75, detalha a forma como o melhor interesse deve ser compreendido, ficando à disposição desta Coordenadoria para apresentar insumos mais aprofundados sobre outros pontos não detalhados naquela ocasião, como a aferição do melhor interesse em casos concretos. Além disso, é preciso que a Autoridade forneça parâmetros que esclareçam quais controladores deverão adotar diligências para respeitar o melhor interesse de crianças e adolescentes. Não basta, nesse sentido, que se vinculem a essas obrigações somente os controladores que afirmem tratar dados desse grupo de pessoas; aqueles que, na prática, realizam ou possam realizar operações de tratamento que afetem crianças e adolescentes, ainda que não intencionalmente, devem estar adstritos à avaliação dos impactos da operação e ao dever de cuidado para com as crianças e os adolescentes, que tanto deverá ser maior quanto maiores os potenciais riscos aos direitos de titulares oferecidos pelo tratamento. Por fim, é imprescindível que a ANPD busque fornecer orientações concretas sobre situações nas quais a forma de melhor atender ao melhor interesse de crianças e adolescentes não é clara ou envolve o balanceamento de diferentes direitos. Como exemplos, citam-se as discussões sobre a verificação etária e as relacionadas à criptografia, conforme será explorado mais detalhadamente na resposta ao item 3.3. ","708725":"Sim. A seguir, são enumerados contextos e situações que demandam maior atenção à luz das principais questões envolvidas e falta de regulamentação específica, conforme demonstrado abaixo: Dados Estudantis: no âmbito educacional, o tratamento de dados desses indivíduos é particularmente sensível. A ANPD deve estabelecer diretrizes para garantir que as informações dos estudantes sejam tratadas com rigor, respeitando a privacidade e os direitos dos mesmos. Nesse sentido, Organizações. Educacionais têm como obrigação informar aos responsáveis sobre como os dados são coletados, armazenados e utilizados, incluindo: (i) a participação da comunidade escolar (ii) a garantia real do consentimento pelos responsáveis; (iii) por respeito ao princípio da transparência, quais os dados serão usados e as suas finalidades; e (iv) quais medidas de segurança são necessárias para a proteção dos dados dos estudantes. Reconhecimento facial em escolas: a implementação desses sistemas em escolas para controle de acesso e segurança, sem a devida regulamentação, pode resultar em violação. Em escolas do Paraná, isso gerou preocupações quanto à violação de direitos e a conformidade com a legislação. Pesquisa realizada pelo APP-Sindicato e o Instituto IPO destaca várias falhas e riscos associados a essas tecnologias: (i) falta de consulta pública; (ii) desconsideração à LGPD e ECA; (iii) ausência de avaliação de impactos na coleta de dados; (iv) política de consentimento inadequada; (v) custos de implementação totalmente questionáveis; (vi) limitações técnicas e preocupações quanto à proteção de dados sensíveis, como etnia e gênero, resultando em discriminação e exclusão de grupos vulneráveis. Reconhecimento Facial na Segurança Pública: o uso de tecnologias de reconhecimento facial na segurança pública traz preocupações graves quanto à violação da privacidade e de outros direitos individuais. Como exemplo, cita-se a ação civil pública ajuizada contra o Metrô de São Paulo em razão da implementação de sistemas de reconhecimento facial na linha vermelha, na qual destacam-se

os riscos associados a essa tecnologia e as implicações legais de seu uso, como: (i) violação da privacidade em espaços públicos; (ii) discriminação devido às altas taxas de erro de etnia e gênero e afetando desproporcionalmente crianças e adolescentes de comunidades vulneráveis; (iii) inibição na liberdade de expressão e a participação em manifestações públicas; (iv) ausência da transparência e clareza da coleta de dados e (v) riscos de abusos por autoridades. Casos de exposição de dados em aborto legal: Casos em que crianças e adolescentes tiveram seus dados expostos na Internet por realizarem abortos legais, que resultaram em danos irreparáveis, tendo, como exemplo, o caso ocorrido após uma publicação que divulgou ilegalmente o nome da criança e o hospital onde o procedimento iria ser realizado. Perfilamento comercial: o perfilamento comercial de crianças e adolescentes é prática que colide com o seu melhor interesse, na medida em que se volta à manipulação de comportamentos e indução abusiva ao consumo. Sendo prática corrente nos modelos de negócios de grandes empresas atuantes no ambiente digital, como fornecedoras de redes sociais e jogos online, necessário que a ANPD publique enunciado reconhecendo expressamente a ilegalidade e abusividade da prática, em linha com a normatização vigente em outras jurisdições. Redes sociais e jogos online: nas redes sociais, a exposição a conteúdos inadequados, assédio e bullying são riscos que se relacionam ao tratamento de dados pessoais dos usuários e que demandam mecanismos eficazes para a proteção integral, incluindo uma noção de supervisão parental que apoie a autonomia progressiva ao mesmo tempo que proteja crianças e adolescentes do risco de violências intrafamiliares. Em jogos online, a coleta de dados para monetização e a proteção contra dependência e interações prejudiciais são questões críticas, que precisam ser reguladas com urgência. ","705523":"Para a obtenção do consentimento “específico e em destaque” de pais ou responsáveis legais, conforme exigido pelo §5º do Art. 14 da Lei Geral de Proteção de Dados Pessoais (LGPD), é essencial observar uma análise dos deveres de conduta de proteção, informação e lealdade qualificados pelo art. 6º, caput e art. 14 e §§, em especial, 1º, 2º e 6º. Tratando-se de atividade de impacto a direitos de crianças e adolescentes, a LGPD exige esforços qualificados de garantia de informação e demais direitos dos responsáveis legais (art. 14, §6º LGPD) e de toda a sociedade no exercício de sua responsabilidade compartilhada constitucionalmente (art. 14, §2º, LGPD; art. 227, CF/88). O art. 14, §2º, exige informações públicas e detalhadas sobre: i) dados coletados de criança e adolescentes, ii) forma de uso e iii) procedimentos para exercício de direitos de titulares. O art. 14, §6º exige, do controlador, a adoção de medidas procedimentais, como consideração das características das crianças, adolescentes e responsáveis para conseguir prover informações simples, claras e acessíveis às suas necessidades. Indica também o uso de recursos audiovisuais para garantia da compreensão. O que tem-se é a qualificação de deveres anexos dos controladores visando à plena compreensão do tratamento de dados pessoais que afetam os direitos e melhor interesse de crianças e adolescentes pelos responsáveis legais e a sociedade, inclusive no estabelecimento de compreensão para legitimidade da base legal do consentimento. A Autoridade Nacional de Proteção de Dados (ANPD) tem um papel fundamental em promover e consolidar um ambiente normativo e regulatório que valorize a acessibilidade, o uso de linguagem simples, e a consideração das necessidades específicas de pessoas com deficiência como orientações centrais para a construção de uma Internet inclusiva, criativa e justa. É primordial orientar

controladores na garantia de: Linguagem Simples, Recursos Audiovisuais e Facilitação da Compreensão: Devem ser utilizados recursos audiovisuais que facilitem a compreensão das informações, especialmente para públicos que possam ter dificuldades de leitura ou entendimento. Esses recursos podem incluir vídeos, áudios, infográficos e outras formas de comunicação visual e a priorização de orientações sobre técnicas de hierarquia da informação e padrões de acessibilidade em prol da devida compreensão de todos, sem discriminação. Transparência "On-Time" no digital e fora das telas: As informações devem ser fornecidas no momento certo, coibindo que sejam relegadas a termos complexos, extensos e fictícios. Coibição, em absoluto, de táticas manipulativas de design na interface de plataformas. Práticas como o mascaramento de informações, redações enganosas, obstruções e indução de escolhas de compartilhamento de dados pessoais com o uso de cores atrativas exploram e manipulam a vulnerabilidade das pessoas (crianças, adolescentes e famílias) e causam um falso sentimento de escolha informada quando, na prática, as estratégias ampliam a assimetria informacional e de poder entre titulares e agentes de tratamento de dados e ferem a autodeterminação informacional. Exigibilidade proporcional ao risco do tratamento e à capacidade econômica do controlador. Quanto maior o potencial de impacto negativo aos direitos de crianças e adolescentes, maior a capacidade econômica do controlador e maior a sua capacidade tecnológica, mais exigíveis e rigorosos devem ser os esforços para assegurar que o consentimento seja devidamente qualificado e baseado em uma compreensão mútua. Não é aceitável, ainda, que grandes empresas de análise de dados e distribuição de fluxo de informações cumpram suas obrigações de forma a mascarar realidades, entregar informações desorganizadas ou dificultar a compreensão de riscos e atividades de tratamento por toda a sociedade. Ônus da Prova para os Controladores. As empresas têm a responsabilidade de demonstrar que o consentimento obtido atende a todos os requisitos legais e éticos. A verificação deve ser transparente e auditável, garantindo que a ANPD e outros órgãos possam assegurar o cumprimento dos direitos dos titulares de dados. ","708742":"Comprovação da Responsabilidade Legal: Os controladores devem implementar mecanismos que comprovem que a pessoa que fornece o consentimento é, de fato, o responsável legal pela criança. No artigo “How do They Know It’s a Child?”, a organização 5rights mapeia contextos de uso e pontos de atenção à privacidade e proteção de dados pessoais para autenticação de identidade. Para contribuir com o importante debate, o Instituto Alana preparou um quadro anexo que mapeia métodos de garantia etária, incluindo verificação, estimativa e autenticação, elaborado a partir do documento. Destaca-se a necessidade de garantir medidas procedimentais na garantia de direitos no tratamento de dados pessoais da pessoa responsável e da criança e do adolescente que possa vir a ser efeito de procedimento adotado de autenticação para garantia de consentimento. Indica-se, nesse sentido: Adoção de "Todos os Esforços Razoáveis": A aplicação desse conceito implica em um conjunto de práticas e medidas que vão além do mínimo exigido, considerando as melhores práticas do mercado e as tecnologias disponíveis em prol do desenvolvimento integral. Isso inclui a revisão periódica dos processos de verificação, a atualização contínua das ferramentas de segurança e a adaptação dos métodos de verificação para acompanhar as evoluções tecnológicas e as mudanças regulatórias. Também exige investimentos para coibir riscos inerentes ao modelo de negócios e colaborar no desenvolvimento de soluções técnicas que reforcem a proteção de

dados de crianças e adolescentes. Múltiplos Meios de Verificação: Considerando a diversidade tecnológica e social, os controladores devem oferecer meios alternativos para a autenticação, adaptados ao público-alvo e ao contexto de tratamento. Tal forma coíbe o risco de que medida exclusiva de autenticação implique exclusão de oportunidade no ambiente digital e a análise deve ser amparada com lastro de avaliação do melhor interesse no caso concreto. Coibição da Geração de Perfis Comportamentais familiares com dados de garantia etária: Ao conectar dados de contas de adultos com contas de crianças, cria-se o risco de perfilamento comportamental, o que vulnerabiliza ambas as partes. Dados usados para verificação de consentimento devem ser restritos a essa finalidade, coletados no mínimo escopo necessário. Prevenção, Segurança e Proteção: Para proteger as informações durante a verificação de identidade e idade, devem ser empregadas técnicas robustas de segurança, como criptografia de ponta a ponta, assegurando a proteção dos dados na coleta, transmissão e armazenamento.. Retenção e minimização: Os dados coletados para verificação de consentimento devem ser retidos apenas pelo tempo necessário para comprovar a validade e conformidade com as exigências legais. É recomendada a priorização de tecnologias que garantam a eliminação dos dados, mas que permitam a certificação da validade do procedimento. Além disso, deve-se documentar todo o processo para garantir auditabilidade e transparência perante órgãos reguladores e os titulares de dados. Responsabilidade por autenticação que dependa de serviço de terceiros. Em caso de violações decorrentes de falhas no serviço de autenticação fornecido por terceiros, o controlador continua responsável perante os titulares e a ANPD. É fundamental que o controlador mantenha mecanismos rigorosos de controle e supervisão sobre as diligências de parceiros comerciais e públicos, documentando riscos e benefícios ao escolher serviços de terceiros. ","708745":"A possibilidade de flexibilização do regime de capacidades do Código Civil para a obtenção do consentimento de adolescentes para o tratamento de seus dados pessoais é debate que contrapõe a autonomia progressiva dessas pessoas à sua segurança, ou, ainda, a proteção de sua privacidade interpessoal à proteção de sua privacidade comercial. Havendo possíveis interpretações distintas da legislação que podem afetar, de maneiras diversas, a esfera de direitos dessas pessoas, imprescindível que o exercício hermenêutico seja pautado pela garantia do melhor interesse, buscando-se a interpretação legal que garanta a proteção e efetivação dos direitos dos adolescentes na maior extensão possível. Dada a complexidade da questão, o Instituto Alana entende serem necessários debates mais profundos a nível nacional entre todos os stakeholders para que a interpretação da lei que melhor atende aos direitos e interesses de crianças e adolescentes seja consagrada pela ANPD. Sugere-se, assim, que sejam realizadas consultas públicas e tomadas de subsídio especificamente sobre este tema, priorizando a participação e escuta de crianças e adolescentes. De partida, contudo, parece possível afirmar que admitir uma flexibilização absoluta das normas do Código Civil, para que, em toda e qualquer situação, o consentimento dos adolescentes possa ser dado sem a representação ou assistência parental, não atende ao seu melhor interesse e pode colocar a proteção de seus direitos em xeque, além de não ser congruente com a legislação vigente no Brasil. Conforme explicam Bruno Miragem e Cláudia Lima Marques em parecer concedido ao Instituto Alana sobre o tema, se a regra geral posta pelo Código Civil é pela necessidade de representação ou assistência parental, admitir que ela não se aplique às operações de

tratamento de dados pessoais seria admitir que essas operações geram efeitos jurídicos menos relevantes às esferas de direitos dos adolescentes do que outros negócios jurídicos "tradicionais". Essa leitura, contudo, é incongruente com a LGPD, que, justamente reconhecendo os possíveis impactos agravados do tratamento de dados pessoais de crianças e adolescentes sobre os direitos dos titulares, cria tutela específica e protetiva para eles em seu art. 14. Por outro lado, não se ignora a necessidade de que determinadas operações de tratamento de dados pessoais de adolescentes se deem desacompanhadas da representação ou assistência parental, sob pena de ferir-se a autonomia dessas pessoas em situações nas quais o acompanhamento dos pais sobre as atividades on-line não necessariamente atende ao seu melhor interesse. Assim, para que se chegue a um ponto de equilíbrio e que se pensem em exceções à regra geral do Código Civil de maneira razoável e que privilegie a proteção integral dos direitos e melhor interesse de crianças e adolescentes, sugerem-se o aprofundamento dos debates e a realização de esforço regulatório específico para este tema. ","705539":"Diversos documentos, de caráter normativo ou não, nacionais e internacionais, fornecem orientações sobre as medidas a serem implementadas por plataformas digitais cujo acesso por crianças e adolescentes é provável, no sentido de garantir a proteção de seus dados pessoais. Citam-se, como exemplos, i) O Comentário Geral N. 25 sobre os direitos da criança em relação ao ambiente digital, do Comitê dos Direitos da Criança da ONU, em especial seus parágrafos 67 a 78; ii) O Age Appropriate Design Code desenvolvido pelo ICO, autoridade regulatória do Reino Unido; iii) O Kids Online Safety Act (KOSA), dos Estados Unidos; iv) o Digital Services Act, da União Europeia; v) o IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, do IEEE; e vi) o Termômetro do Acesso Apropriado à Idade, do IP.Rec. A partir desses parâmetros e de elementos relevantes à realidade brasileira, a ANPD pode desenvolver material voltado para controladores que realizem o tratamento de dados pessoais de crianças e adolescentes, no qual, além de fornecer detalhes acerca da aplicação da garantia do melhor interesse (vide resposta ao item 1.1), pode apresentar parâmetros e salvaguardas a serem implementados para assegurar elevados níveis de privacidade e mitigar os riscos relativos à utilização dessas plataformas, no espírito de construir um Código de Design aplicável aos produtos e serviços digitais disponíveis no Brasil. Como exemplos desses parâmetros, citam-se, tomando-se como referência os documentos mencionados: • Elaboração de relatório de impacto à proteção de dados (RIPD) sempre que o tratamento de dados de crianças e adolescentes contiver elementos que ofereçam riscos aos seus direitos fundamentais; • Monitoramento periódico dos impactos e riscos oferecidos pelo produto ou serviço e transparência na divulgação dos resultados; • Vedação do perfilamento de crianças e adolescentes para fins atentatórios ao seu melhor interesse, sobretudo para o direcionamento de publicidade comportamental; • Vedação de técnicas de "nudge" que induzam crianças e adolescentes a comportamentos prejudiciais a seus próprios direitos e interesses; • Configurações padrão (por "default"), as mais protetivas possíveis, para a privacidade quando o usuário for, ou tiver chances consideráveis de ser, uma criança ou um adolescente; • Redução da coleta de dados pessoais ao mínimo necessário para oferecimento do produto ou serviço e proteção dos direitos dos titulares e anonimização dos dados; • Adequação de interfaces ao estágio de desenvolvimento progressivo de crianças e adolescentes, com o fornecimento de

informações adequadas à sua compreensão e à de suas famílias; • Rigor quanto às políticas de compartilhamento de dados pessoais de crianças e adolescentes com terceiros, garantindo-se que aqueles que recebem esses dados respeitarão o melhor interesse desses indivíduos; •

Políticas de privacidade que garantam a retenção dos dados pessoais de crianças e adolescentes estritamente apenas pelo tempo necessário para o fornecimento do produto ou serviço ou garantia do melhor interesse, vedando-se o tratamento de dados pessoais coletados durante a infância ou adolescência para fins comerciais na vida adulta dos titulares; •

Garantir que o rastreamento da geolocalização de crianças e adolescentes seja desligado por padrão e que os titulares sejam ostensivamente informados caso estejam sendo rastreados, o que só deve ocorrer em seu melhor interesse; • Implementar ferramentas que facilitem o exercício dos direitos do titular por crianças, adolescentes e suas famílias; •

Disponibilizar ferramentas de acompanhamento e mediação parental de maneira equilibrada com a autonomia da criança ou do adolescente e respeitosa ao seu desenvolvimento progressivo; • Implementar mecanismos de garantia etária e controle de acesso razoáveis e proporcionais aos riscos oferecidos pelo produto ou serviço aos direitos de crianças e adolescentes. ","708762":"A garantia etária é um termo guarda-chuva que inclui soluções de verificação etária e estimativa de idade. A palavra garantia remete a diferentes níveis de certeza que soluções estabelecem ao propor estabelecer uma idade de certo usuário de plataforma digital ou estimar sua faixa etária. A verificação etária é um processo que depende de identificadores rígidos e/ou outras fontes verificadas de identificação, que proporcionam alto grau de certeza na determinação exata da idade de um usuário. A estimativa de idade é um processo que estabelece que um usuário: tem uma certa idade, está dentro de uma faixa etária ou está acima ou abaixo de uma certa idade. No documento 5Rights - How do They Know It's a Child, alguns métodos mapeados, oferecidos de forma sistematizada em quadro anexo são: Autodeclaração (Estimativa). Utilizada em plataformas como TikTok e Instagram, onde os usuários inserem suas datas de nascimento. Embora medidas técnicas sejam adotadas para desencorajar declarações falsas (como bloqueio de acesso), esse método é facilmente burlável e pode responsabilizar indevidamente crianças e adolescentes. A percepção de risco é baixa, e a eficácia é limitada. Uso de identificadores duros (Verificação Etária ou Identificação). Uso de documentos como RG, CPF ou cartão de crédito, cruzados com bases de dados certificadas. É eficaz para identificar maiores de 18 anos, mas menos útil para determinar faixas etárias específicas, especialmente para menores de 18 anos. Um ex.: é o YouTube na Europa, que exige RG ou cartão de crédito para acessar conteúdo 18+. Biometria (identificação/verificação etária), a ex.: de análises de métricas e dados corporais e biológicos. O método do reconhecimento facial, em especial, tem sido identificado como ineficiente para crianças e adolescentes, não sendo apropriado para distinguir pessoas entre idades próximas. A sensibilidade dos dados tratados e os notórios casos de impacto a direitos fundamentais fazem questionar tratar-se de método adequado. Qualquer uso deve ser atrelado a padrões altos de prestação de contas, garantia de auditorias independentes e fortes requisitos de transparência. A má utilização de dados pode ensejar em usos absolutamente ilegítimos, a exemplo de análise emocional da criança e do adolescente. O método, entretanto, é usado para operações de segurança no combate ao abuso e exploração sexual, a ex.: de softwares que rastreiam faces de crianças em exibição em sites

de pornografia a fim de identificar caso de possível abuso e exploração sexual. Teste de capacidade (estimativa), Inclui quizzes ou testes de linguagem e matemática. Deve ser usado com cautela, pois capacidade e idade não são sinônimos, e o método é facilmente fraudável. É recomendado como complemento a outras estratégias, mas não pode determinar a idade exata. Autenticação entre contas (single sign on): Permite que um novo serviço acesse dados do usuário de outra plataforma via API. Depende da qualidade de autenticação da plataforma original. No caso de uso deste método, a transferência de dados deve ater-se à minimização e vinculação estrita à legitimidade de verificação etária, coibindo práticas que criam perfis de monitoramento compartilhados de crianças e adolescentes entre diferentes redes. Provedor de garantia de idade terceirizado: Em que pese ser solução que depende de padrões de segurança para garantia da integridade do terceiro autenticador, políticas de tokens de idade e de validação etária por provedores de certificados podem apoiar uma minimização na medida em que não é necessário transmitir outras informações além da confirmação de query de idade. Controles de dispositivo/sistema operacional (estimação/verificação): Permite que sistemas operacionais definam a experiência adequada para crianças e adolescentes, com base na estimativa etária. Pode haver conflitos em ambientes onde o uso de dispositivos é compartilhado. Seu uso deve ser modulado para garantir uma abordagem de supervisão parental à luz da noção de parentalidade positiva e respeito à autonomia progressiva, evitando que a implementação de filtros e controles impactam direitos à informação, privacidade e outros aspectos da criança e do","708764":"O Comentário Geral n° 25 reconhece os impactos negativos dos sistemas de recomendação algorítmica sobre os direitos de crianças e adolescentes. No parágrafo 62, alerta que esses sistemas podem inferir o estado emocional das crianças, sendo necessário que os Estados garantam que não sejam usados para influenciar seu comportamento ou limitar suas oportunidades e desenvolvimento. A interpretação da ANPD sobre perfilamento comportamental deve reafirmar as disposições da Convenção sobre os Direitos da Criança, com base nos parágrafos 42, 53 e 62 do Comentário Geral n° 25, que estabelece parâmetros claros para a formação de perfis e práticas de tratamento de dados. Interesse Prioritário e Justificado: O perfilamento de crianças e adolescentes deve ser conduzido com foco na garantia do melhor interesse desse público. Qualquer atividade de perfilamento deve ser rigorosamente avaliada para assegurar que não prejudique, mas promova seu bem-estar e direitos fundamentais em sua maior extensão possível. Proibição de Perfilamento para Publicidade: Todas as práticas de tratamento de dados que visem ao perfilamento comportamental para direcionamento de publicidade são ilegais desde a coleta, devido à hipervulnerabilidade das crianças. Isso inclui a análise emocional, neuromarketing e uso de dados para criar perfis destinados ao direcionamento de comunicação mercadológica. A proibição abrange tanto perfis individuais quanto grupais e protege a privacidade de crianças e adolescentes quanto à atributos inferidos de sua análise comportamental. Desativação Padrão de Perfilamento Comportamental: O perfilamento comportamental para direcionamento de publicidade deve ser desligado por padrão, especialmente quando não há verificação confiável da idade do usuário, de forma a não colocar a criança ou adolescente que acessa ou burla sistema de garantia etária de plataforma em risco de exploração comercial. Nenhuma coleta de dados comportamentais, rastreamento ou monitoramento deve ocorrer automaticamente ou de forma oculta, posto que isto coloca

mais em riscos os direitos e melhor interesse de crianças e adolescentes e fomenta cultura de monitoramento e rastreamento. Configurações padrões mais protetivas para adultos são medidas de design a serem exigidas em casos concretos de evidências notórias de falhas de mecanismos de verificação etária. Caso o controlador não seja capaz de implementar medidas que impeçam a exploração comercial dos dados de crianças e adolescentes neste fim, deve deixar de realizar a atividade. Promoção do Empoderamento e Autonomia: O processo de perfilamento deve ser orientado por princípios que promovam o empoderamento, direito à informação, autonomia e liberdade das crianças e adolescentes. Plataformas digitais devem criar ambientes apropriados à idade, respeitando a capacidade e estágio de desenvolvimento do usuário. Direito de Reset: Crianças e adolescentes devem ter o direito de redefinir, controlar ou apagar seus perfis e históricos digitais a qualquer momento, com comunicação facilitada e acessível para esse exercício. Esse "direito de reset" assegura a proteção da privacidade e o direito ao esquecimento. Proibição do Uso de Dados a Longo Prazo: Dados coletados durante a infância ou adolescência não podem ser utilizados posteriormente para perfilamento comercial. A proteção desses dados deve se estender ao longo da vida, respeitando o contexto em que foram inicialmente coletados. Sistemas de Recomendação Transparente: Sistemas de recomendação de conteúdo não devem priorizar conteúdos pagos ou com motivação comercial em detrimento do direito à informação das crianças e adolescentes (CG25, §62). Reparação de Danos: Deve ser garantida a devida reparação à criança ou adolescente que sofreu perfilamento que afetou negativamente sua esfera de proteção de direitos. Restrições à Análise Emocional: Sistemas de recomendação de conteúdo, mesmo que orgânicos, não devem realizar direcionamento baseado em análise emocional, evitando a exploração de vulnerabilidades e o reforço de padrões negativos repetitivos, conhecidos como "efeito toca de coelho".","708768":"Parentalidade Positiva (Lei nº 14.826/2024) e Autonomia Progressiva: a Lei mencionada enfatiza a importância da parentalidade positiva e da consideração da autonomia progressiva no desenvolvimento de crianças e adolescentes. Além disso, a lei promove respeito, acolhimento e não violência na educação, garantindo um ambiente seguro a crianças e adolescentes. Esses usuários devem adquirir mais controle sobre seus dados à medida que ficam mais velhos, sempre com orientação e supervisão dos responsáveis, por meio de configurações de privacidade adaptáveis. A personalização das plataformas digitais por faixa etária é essencial para ampliar o controle dos responsáveis sobre o tratamento de dados pessoais. Adaptar conteúdo e interações de acordo com a idade dos usuários assegura que as informações e funcionalidades ofertadas sejam adequadas e seguras. De acordo com o Design Apropriado para a Idade: Código de Práticas para Serviços Online , do ICO, isso significa aplicar padrões que proporcionem um nível adequado de proteção aos dados das crianças e adolescentes, adaptando as salvaguardas conforme a faixa etária dos usuários, tornando-se uma prática flexível e ajustada às especificidades de cada serviço online A privacidade é um direito fundamental para crianças e adolescentes no ambiente digital. As plataformas digitais devem implementar políticas transparentes e eficazes que protejam os dados desses usuários, utilizando métodos como anonimização e minimização de dados para evitar exploração comercial e manipulação comportamental. O Instituto Alana enfatiza, por exemplo, a importância de educar e capacitar os pais e responsáveis sobre o uso seguro da tecnologia.

Mecanismos para o exercício dos direitos dos titulares, como acesso, correção e exclusão de dados, devem ser simplificados. A LGPD exige que o consentimento parental seja específico e destacado, reforçando a necessidade de ferramentas que facilitem esse processo. As plataformas digitais devem alertar sobre os riscos do compartilhamento irresponsável de dados, por meio de avisos, bem como campanhas educativas para os responsáveis. ","708772":"Com o aumento do uso de plataformas online por crianças e adolescentes, que são hipervulneráveis e não têm plena consciência dos riscos envolvidos, é essencial que essas plataformas adotem boas práticas que garantam o melhor interesse da criança e do adolescente, especialmente no que diz respeito à transparência no tratamento de seus dados. Uma das principais diretrizes para garantir essa transparência é a clareza na comunicação. As organizações devem utilizar uma linguagem simples e acessível, evitando jargões técnicos que possam confundir as crianças e seus responsáveis. Além disso, é fundamental adotar múltiplas linguagens além da escrita, como gráficos, vídeos e elementos interativos, para facilitar a compreensão de como os dados são coletados e utilizados. Isso é crucial para que crianças e adolescentes compreendam seus direitos e as implicações do compartilhamento de suas informações pessoais.. O acesso às informações também é crucial. As políticas de privacidade devem ser facilmente acessíveis e redigidas de forma que as crianças possam entender, com seções específicas voltadas para o público infantil. Ferramentas interativas podem ajudar esses usuários a explorar suas informações e direitos de maneira lúdica, aumentando a compreensão e o engajamento com as questões de privacidade. Além disso, é fundamental que as plataformas ofereçam opções de configuração que permitam que esses usuários gerenciem suas preferências de privacidade de maneira adequada à sua faixa etária. Outro aspecto essencial é o consentimento e a autorização. A obtenção do consentimento dos responsáveis legais deve ser feita de maneira clara e informada, garantindo que os pais compreendam o que está sendo consentido. Também é importante que as plataformas ofereçam opções de configuração que permitam que crianças e adolescentes gerenciem suas preferências de privacidade. A educação e a conscientização sobre privacidade digital são indispensáveis. Programas educativos que ensinam crianças e adolescentes sobre segurança online e proteção de dados. Campanhas de sensibilização voltadas para responsáveis também são importantes, pois ajudam a criar um ambiente familiar que valoriza a proteção de dados. Por fim, é imprescindível evitar a publicidade direcionada a crianças, seja ela simples ou por meio de IA. As organizações devem garantir que informações sobre direitos e privacidade não sejam misturadas com conteúdos publicitários, especialmente em plataformas que não são apropriadas para o público infantil. O cumprimento de regulamentações que proíbem essa prática é essencial para proteger esses usuários de influências ilícitas. Exemplos de boas práticas podem ser observados tanto em âmbito nacional quanto internacional: a ANPD fornece orientações sobre o tratamento de dados pessoais, incluindo orientações específicas para crianças e adolescentes, e o ICO recomenda que as plataformas adotem uma abordagem centrada na criança, com informações claras sobre como os dados são usados e a importância do consentimento. ","708775":"Por fim, de maneira complementar às demais considerações apresentadas ao longo das respostas a essa tomada de subsídios, o Instituto Alana apresenta algumas linhas de ação que considera importantes para que a ANPD possa cumprir plena e efetivamente com o papel que lhe cabe na proteção dos direitos de crianças e adolescentes:

Realização de tomadas de subsídios e “sandboxes” regulatórios para a regulação de temas complexos e recorrentes do ponto de vista da proteção de crianças e adolescentes: determinados temas relacionados à proteção de dados pessoais de crianças e adolescentes desafiam a proteção integral desses indivíduos na medida em que contrapõem e tensionam diferentes direitos fundamentais garantidos a eles. É o que se verifica, por exemplo, nas discussões relativas à verificação etária e à criptografia, que, de maneira geral, apresentam uma tensão (ao menos aparente) entre os direitos de crianças e adolescentes à privacidade e à segurança. Como antes se expôs, a garantia do melhor interesse presta-se, também, a oferecer parâmetros para que, em casos como esses, sejam adotadas soluções que atendam à proteção e promoção dos direitos dessas pessoas na maior extensão possível, à luz de suas circunstâncias concretas, da escuta de suas vozes e dos insumos fornecidos por especialistas. Assim, considerando que essas discussões afetam uma grande quantidade de controladores e titulares de dados pessoais, a ANPD, orientando-se pela garantia do melhor interesse, pode fazer uso dos instrumentos regulatórios à sua disposição, como tomadas de subsídios e sandboxes, para buscar determinar de que forma esses debates podem ser solucionados na realidade brasileira, de modo a concretizar o melhor interesse das crianças e adolescentes residentes em território nacional. Esses instrumentos, evidentemente, devem ser complementados por iniciativas que garantam a participação de crianças e adolescentes nesses processos, como dispõe o C.G. nº 14. Articulação com o Sistema de Garantia de Direitos da Criança e do Adolescente: a articulação com outros órgãos integrantes do SGCA é imprescindível para que a ANPD possa ampliar o alcance de suas ações e a sua capacidade fiscalizatória. Parcerias com o Ministério da Educação, por exemplo, podem ser firmadas para disseminar informações sobre a proteção de dados pessoais a crianças e adolescentes de maneira mais efetiva. Ministérios Públicos, Defensorias e órgãos do Sistema Nacional de Proteção ao Consumidor podem contribuir com as investigações conduzidas pela ANPD e colaborar com a investigação de ilícitos. Na mesma toada, é particularmente relevante a articulação com o Conanda, que não apenas detém competência para articular as políticas de proteção à criança e ao adolescente em território nacional, como ainda publicou, em maio, a sua Resolução n° 245, que prevê a criação de uma política nacional para a proteção de crianças e adolescentes nos ambientes digitais. É essencial que a ANPD atue em parceria com o Conanda e oriente sua atuação pelas disposições da referida Resolução, inclusive no que diz respeito à interpretação a ser conferida à LGPD e às bases legais aplicáveis ao tratamento de dados pessoais de pessoas com menos de 18 anos. Articulação com outras Autoridades de Proteção de Dados em nível internacional: a colaboração direta com outras Autoridades de Proteção de Dados pode fornecer subsídios importantes para a atuação da ANPD. Investigações conduzidas em outras jurisdições podem servir de ponto de partida para a atuação fiscalizatória da ANPD e aumentar a sua capacidade de monitorar efetivamente a atuação de empresas com atuação transnacional. Além disso, o diálogo com outras Autoridades pode servir para evidenciar políticas discriminatórias de empresas contra países do Sul Global, cuja existência já foi evidenciada em estudos conduzidos sobre o tema. Ainda, podem ser fornecidos insumos relevantes para a avaliação concreta do melhor interesse de crianças e adolescentes, especialmente em se tratando da colaboração com autoridades de outros países latino-americanos.

Contribuinte: GUILHERME VIANA

REFERÊNCIA: TOMADA DE SUBSÍDIOS - TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

ENTIDADE DESTINATÁRIA: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (“ANPD”)

ENTIDADE CONTRIBUINTE: CÂMARA BRASILEIRA DA ECONOMIA DIGITAL (“CAMARA-E.NET”)

A Câmara Brasileira da Economia Digital (camara-e.net) gostaria de parabenizar a ANPD pela iniciativa de abordar o tema sobre o tratamento de dados de crianças e adolescentes. Nos parágrafos que seguem, a camara-e.net se dedicará a discorrer sobre suas contribuições à Tomada de Subsídios.

I - Princípio do melhor interesse

De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança,[1] no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU[2] e no Comentário Geral n° 25, de 2021, do Comitê dos Direitos da Criança.[3] Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz.

[1] FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). Convenção sobre os Direitos da Criança. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em 12 jun 2024.

[2] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em 12 jun 2024.

[3] 8 UNITED NATIONS. General comment No. 25 (2021) on children's rights in relation to the digital environment. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em 12 jun 2024.

Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, questiona-se:

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Seria imprescindível que a Autoridade evidenciasse que o melhor interesse não pode ser concebido de forma abstrata e apriorística, sendo necessária uma análise concreta para definir qual é o melhor interesse da criança e do adolescente em determinada circunstância. Como se sabe, o melhor interesse exige necessariamente um olhar dinâmico, voltado para o caso concreto e para as características do indivíduo ou do grupo de indivíduos afetados. Nesse sentido, cabe referenciar o Comentário Geral nº 14 do Comitê dos Direitos da Criança da Organização das Nações Unidas (ONU)[1]: "[...] o conceito de melhor interesse da criança é flexível e adaptável. Deve ser ajustado e definido de forma individual, com base na situação concreta da criança ou crianças afetadas, tendo em vista o contexto e as necessidades pessoais. No que diz respeito às decisões particulares, deve ser analisado e determinado o interesse superior da criança em função das circunstâncias específicas de cada criança em concreto".

Ainda no Comentário Geral nº 14, o Comitê dos Direitos da Criança da ONU ressalta que a flexibilidade do conceito de melhor interesse permite que ele seja responsivo à situação de cada menor e que haja progresso no conhecimento sobre o desenvolvimento dos menores. Em outro ponto, a flexibilidade, a dinamicidade e o olhar voltado ao caso concreto permitem que se possa endereçar a interação do melhor interesse com os diversos direitos que podem estar implicados nas situações concretas que envolvem um menor e/ou um grupo de menores. Nessa toada, o Comitê dos Direitos da Criança da ONU ressalta a interação do conceito com múltiplos direitos, são eles: direito à não-discriminação; direito à vida, sobrevivência e desenvolvimento; e direito de ser ouvido.

Assim, a análise do melhor interesse deve considerar as diversas dimensões que envolvem a proteção dos interesses da criança e do adolescente. Desta forma, é necessário levar em conta os interesses que podem ser afetados caso a Autoridade opte por uma perspectiva restritiva do melhor interesse. Esses interesses vão além da proteção de dados do menor, incluindo segurança, acesso à informação, direito a brincar e se conectar, entre outros. Portanto, é essencial compreender que avaliar qual é o melhor interesse da

[1] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: <https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf>. Acesso em: 07 de out. de 2022.

criança e do adolescente não se restringe a verificar se o direito à proteção de dados pessoais está sendo respeitado, mas implica também avaliar o impacto ao gozo de outros direitos e considerar o desenvolvimento integral da criança e do adolescente.

Este posicionamento está em conformidade com as orientações do Conselho da Europa[2], que destaca a necessidade de proteção igualitária de direitos como: acesso ao ambiente digital, liberdade de expressão e informação, educação e participação; e da Organização para a Cooperação e Desenvolvimento Econômico ("OCDE")[3], que destaca que os atores que desempenham um papel ativo na definição de políticas e práticas ou prestação de serviços para crianças e adolescentes no ambiente digital devem considerar suas diferentes necessidades em vista da idade e da maturidade, com medidas proporcionais aos riscos, baseadas em evidências, eficazes, equilibradas e formuladas com uma visão de maximizar as oportunidades e benefícios para as crianças e adolescentes no ambiente digital além de promover a liberdade de expressão das crianças e dos adolescentes e não prejudicar outros direitos humanos e liberdades fundamentais.

Ainda, é preciso que a Autoridade evidencie que eventuais interpretações do melhor interesse devem considerar a condição peculiar da criança e do adolescente como pessoa em desenvolvimento. Como é sabido, não só o Estatuto da Criança e do Adolescente ("ECA") diferencia crianças (pessoas com até doze anos de idade incompletos) e adolescentes (pessoas entre doze e dezoito anos de idade), como estabelece que suas normas deverão ser interpretadas considerando esta condição peculiar. Em consonância, a doutrina[4] traz a condição peculiar de pessoa em desenvolvimento como verdadeiro princípio do direito da criança e do adolescente, alertando para a necessidade de considerar, nas demandas relativas ao público infanto-juvenil, que se está tratando de uma fase da

[2] Council of Europe. Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Recommendation CM/Rec(2018)7 of the Committee of Ministers. 2018. Disponível em: <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.

[3] OECD, Recommendation of the Council on Children in the Digital Environment, OECD/LEGAL/0389. Disponível em: <https://legalinstruments.oecd.org/public/doc/272/272.en.pdf>.

[4] SEABRA, Gustavo Cives. Manual de Direito da Criança e do Adolescente. Belo Horizonte: CEI, 2020.

vida que envolve modificações constantes em termos físicos, cognitivos, psicológicos e sociais e o desenvolvimento progressivo de capacidades e habilidades[5].

Um tema específico que a Câmara-e.net entende que merece atenção no que tange ao atendimento do melhor interesse da criança e do adolescente é a necessidade de equacionar o princípio da necessidade com a garantia de outros princípios previstos na legislação na aplicação do melhor interesse no caso concreto. Existem situações nas quais a coleta de dados adicionais é necessária para a observância de outros princípios como o é o caso da implementação de mecanismos de detecção de idade. Portanto, é essencial que a ANPD reconheça que o cumprimento do princípio da necessidade não significa tratar o mínimo de dados, mas sim tratar aqueles dados necessários para o cumprimento da finalidade em observância de outros princípios da legislação e do melhor interesse da criança e do adolescente. A tensão que pode existir entre mecanismos de segurança e o direito à proteção de dados é algo que pode ser apreendido a partir da análise de casos concretos, que permitem discutir a ponderação adequada entre distintos valores em oposição[6]. Coletar determinados dados pessoais pode, em certos casos, atender melhor ao interesse da criança e do adolescente, como na eficácia de barrar o acesso a conteúdos ou plataformas impróprios para a sua idade. Portanto, é crucial garantir que os controladores não sejam penalizados indevidamente pelo balanceamento do princípio da necessidade com outros princípios e obrigações legais, quando justificada.

Diante de todo o exposto, a Câmara-e.net gostaria de sugerir à ANPD que sejam evitadas perspectivas apriorísticas e genéricas sobre o melhor interesse de crianças e adolescentes no que diz respeito ao tratamento de seus dados pessoais, e reconhecer que controladores precisam de flexibilidade e autonomia para a aplicação do melhor interesse no caso concreto. A presente associação entende que, para avaliar o melhor interesse de crianças e adolescentes, é preciso um olhar para o caso concreto, que considere as circunstâncias específicas do tratamento de dados pessoais em questão, como: (a) características gerais dos titulares de dados, (b) dados tratados; (c) finalidade do tratamento; e (d) possíveis benefícios e danos decorrentes do tratamento de dados. Da mesma forma,

[5] HARTUNG, Pedro Affonso Duarte. Levando os Direitos das Crianças a Sério: A Absoluta Prioridade dos Direitos Fundamentais e Melhor Interesse da Criança. Tese (Doutorado – Programa de Pós-Graduação em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, 2019. Disponível em: < https://www.teses.usp.br/teses/disponiveis/2/2134/tde-04092020-174138/pt-br.php>.

[6] Meta. (2022). Privacy Within Meta's Integrity Systems. Disponível em: <https://about.fb.com/wp-content/uploads/2022/07/Privacy-Within-Metas-Integrity-Systems.pdf>

é preciso dar ao controlador a oportunidade de promover ajustes (por ex.: adotando certas salvaguardas, promovendo maior transparência, etc.) para que o tratamento não afete o melhor interesse de crianças e adolescentes.

Em complemento, a Câmara-e.net entende que a Autoridade deve evidenciar que a análise do atendimento ao melhor interesse da criança e do adolescente deve ser pautada pela multidimensionalidade, pois não envolve apenas a proteção dos dados do menor, mas também outros direitos. Além disso, a ANPD deve reconhecer que o melhor interesse deve considerar a condição peculiar da criança e do adolescente como pessoas em desenvolvimento. Por fim, a Associação entende que seria relevante que a Autoridade reconhecesse que, em determinadas circunstâncias, para que haja o respeito ao melhor interesse da criança e do adolescente, será necessária uma interpretação flexível do princípio da necessidade.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

A Câmara-e.net entende que seria relevante que a presente Autoridade esclarecesse que o uso da base legal do legítimo interesse para o tratamento de dados pessoais de crianças e adolescentes não é, *prima facie*, contrário ao seu melhor interesse. Nesse sentido, é importante destacar que, apesar do entendimento firmado no Enunciado nº 1/2022, o Guia Orientativo sobre a hipótese legal do legítimo interesse trouxe uma perspectiva preocupante sobre o tratamento de dados pessoais de crianças e adolescentes. Exemplo de afirmativa presente no Guia Orientativo que gerou apreensão foi a de que o uso do legítimo interesse seria mais apropriado em situações específicas como quando há uma relação direta do controlador com os titulares e quando o tratamento visa a proteção de direitos e interesses dos titulares ou a prestação de serviços a ele benéficos[7].

O Estudo Preliminar que embasou o Enunciado nº 1/2022 da ANPD concluiu que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base em todas as bases legais previstas na LGPD, desde que observado e prevalente o seu melhor interesse, a ser avaliado no caso concreto. Para chegar a esta conclusão, diversos argumentos foram considerados: (i) a flexibilidade propiciada pela possibilidade do uso de bases legais distintas, desde que o tratamento respeite o melhor interesse da criança e do adolescente; (ii) a possibilidade de estender a aplicação do melhor interesse da criança e do adolescente para todas as

[7] Parágrafo 22, páginas 6 e 7.

bases legais; (iii) a ausência de proibições jurídicas abstratas em relação a certas hipóteses legais e a necessidade de analisar as situações de forma concreta; e (iv) o tratamento não diferenciado entre as hipóteses legais, mantendo-se a ausência de hierarquia entre elas, como previsto pela LGPD.

Assim, a ANPD não deve, *a priori*, restringir o uso de qualquer base legal, inclusive a do legítimo interesse, para o tratamento de dados pessoais de crianças e adolescentes a situações específicas. Para definir a presença do melhor interesse de crianças e adolescentes, é preciso que a Autoridade olhe para o caso concreto e considere as circunstâncias específicas do tratamento de dados pessoais em questão, como: (a) características gerais dos titulares de dados, (b) quais dados são tratados; (c) qual a finalidade do tratamento; e (d) possíveis benefícios e danos decorrentes do tratamento de dados. Além disso, a ANPD deve equilibrar o legítimo interesse com os demais princípios da LGPD.

Quanto a situações que demandam maior atenção, a Câmara-e.net considera que é preciso cautela para não pressupor que o uso de dados pessoais de crianças e adolescentes para direcionamento de publicidade é negativo. No exemplo 3 do Guia do Legítimo Interesse, a Autoridade trata sobre o uso de dados de crianças e adolescentes para publicidade e traz exemplo em que a publicidade pode afetar negativamente os direitos e liberdades fundamentais dos menores. Ocorre que a publicidade online (inclusive para menores de idade) é uma atividade lícita e regulamentada, portanto, é importante que a ANPD reconheça a licitude e possíveis benefícios da atividade no escopo de sua atuação com relação à proteção de dados pessoais de menores.

Nesse contexto, é relevante que se considere a diferença entre publicidade personalizada (utilização de dados específicos do usuário, como idade e interesses, para direcionar anúncios relevantes ao perfil individual) e publicidade não personalizada (baseia-se em dados genéricos do dispositivo, como localização obtida pelo IP e idioma do aplicativo, para direcionar os anúncios). O uso de publicidade personalizada pode inclusive auxiliar no respeito à condição peculiar da criança e do adolescente como pessoa em desenvolvimento, assegurando uma experiência segura e adequada, de acordo com sua faixa etária. Deste modo, avaliar se o direcionamento de publicidade a crianças e adolescentes respeita seu melhor interesse requer uma avaliação do caso concreto, levando em conta a legislação existente. Como destacado anteriormente, a publicidade online para menores é uma atividade lícita e

regulamentada: o Código de Defesa do Consumidor (“CDC”), em seu artigo 37, veda a publicidade enganosa ou abusiva, estabelecendo que seria abusiva aquela publicidade que se aproveita da deficiência de julgamento e experiência da criança. Em complemento, o Código Brasileiro de Autorregulamentação Publicitária do Conselho Nacional de Autorregulamentação Publicitária (“CONAR”) conta com dispositivo voltado especialmente a estabelecer parâmetros éticos que devem ser considerados em anúncios voltados às crianças e aos adolescentes (artigo 37).

Outra situação que exige cautela da Autoridade para evitar pressuposições envolve a elaboração de perfis comportamentais para fins de direcionamento de conteúdo. Isso porque a elaboração de perfis comportamentais pode ser uma prática valiosa para atender ao melhor interesse da criança, visto que pode ser utilizado para direcionar conteúdos adequados à idade dos usuários (e vedar que conteúdos inadequados sejam exibidos), proporcionando uma abordagem adaptada para atender às características únicas de crianças e adolescentes Assim, é preciso desconstruir eventuais pré-concepções de que a elaboração de perfis comportamentais é utilizada para fins prejudiciais, e reconhecer que quando aplicada de forma adequada, oferece uma abordagem valiosa para garantir o direcionamento não só de conteúdo adequado, mas também interessante e relevante para crianças e adolescentes, garantindo sua melhor experiência de forma eficaz.

II - Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

O §1º do artigo 14 da LGPD estabelece que o tratamento de dados pessoais de crianças deve ser realizado com base no consentimento específico e em destaque (quando essa for a hipótese legal eleita pelo controlador), dado por pelo menos um dos pais ou pelo responsável legal. Primeiramente, é importante destacar que a exigência do consentimento específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal, se aplica apenas às crianças, não se estendendo aos adolescentes. Neste contexto, vale lembrar que o Estatuto da Criança e do Adolescente (ECA) diferencia, em seu artigo 2º, a criança (pessoa de até

12 anos incompletos) do adolescente (pessoas entre 12 e 18 anos) e estabelece, em seu artigo 6º, o dever de interpretar suas normas considerando a condição peculiar de desenvolvimento desses sujeitos.

Necessário esclarecer, ainda, que o consentimento não é a única base legal para o tratamento de dados pessoais de crianças e adolescentes e que não há prevalência de tal base legal em relação às demais hipóteses de tratamento. De modo convergente a este entendimento, esta Autoridade editou o Enunciado nº 1 de 2023, por meio do qual firmou o entendimento de que o tratamento de dados pessoais de crianças e adolescentes pode ser feito com base nas hipóteses legais previstas tanto no artigo 7º quanto no artigo 11º da LGPD.

Para trazer maior segurança jurídica nos casos em que a base legal do consentimento será usada para o tratamento de dados pessoais de crianças e adolescentes, é necessário que a Autoridade esclareça o que entende por consentimento "específico e em destaque". Em relação ao consentimento "específico", a Câmara-e.net entende que deve haver flexibilidade na interpretação sobre seu nível de granularidade, desde que o usuário seja informado com um grau razoável de transparência sobre o fluxo de dados, por meio de informações claras, precisas e facilmente acessíveis, capazes de proporcionar clareza ao titular para uma decisão mais informada. Essa perspectiva se justifica em prol de uma transparência eficaz e também para evitar os efeitos negativos da fadiga do consentimento. Quanto ao termo "em destaque", a ANPD deve garantir uma flexibilidade conceitual que considere as diferenças técnicas de cada serviço ou produto, evitando um modelo rígido e padronizado que não leve em conta as diversas naturezas e propósitos. Isso permitirá que os regulados se adaptem aos seus contextos específicos de atuação, com diferentes interfaces.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

Primeiramente, é importante salientar a tensão inerente entre a efetividade dos mecanismos de verificação de consentimento parental e o princípio da necessidade de dados. Mecanismos de verificação mais precisos muitas vezes exigem uma coleta maior de dados, o que pode gerar insegurança para o controlador, haja vista potenciais interpretações restritivas do princípio da necessidade. A ANPD deve, portanto, considerar esse princípio de forma ponderada, reconhecendo que, em alguns casos, é necessário uma maior coleta

de dados para confirmar que o consentimento foi realmente dado por um dos responsáveis e que não se trata de uma estratégia para contornar a regra do consentimento parental.

Em outro ponto, é preciso que se considere que medidas excessivamente onerosas para obter consentimento, bem como o uso excessivo desta base legal podem dificultar que pais e responsáveis concedam o consentimento de forma efetiva. Assim, é preciso tomar cuidado com a 'fadiga do consentimento'[8], que na prática pode levar a que pais e responsáveis, especialmente aqueles menos familiarizados com a legislação, consintam excessivamente, gerando um efeito contrário ao pretendido. Isso destaca a necessidade de explorar outras bases legais, conforme já indicado pelo Enunciado nº 01/2023 e pelo Guia de Legítimo Interesse, e enfatiza a importância de que as medidas para obter um consentimento parental válido sejam proporcionais e práticas.

Sobre os mecanismos de verificação de consentimento parental em si, é importante salientar que o European Data Protection Board ("EDPB")[9] advoga pela proporcionalidade e destaca que o que é considerado razoável para verificar se o consentimento foi de fato fornecido pelos pais ou responsáveis legais dependerá dos riscos ligados ao tratamento, bem como das tecnologias disponíveis. O EDPB pontua que, em casos de baixo risco, a verificação via e-mail seria suficiente, enquanto em casos de alto risco, poderia ser apropriado solicitar mais provas. No mesmo sentido, o Information Commissioner's Office[10] entende que a análise da adequabilidade dos esforços razoáveis dependerá dos riscos ensejados pelo tratamento e da tecnologia disponível. A Data Protection Commission[11] também endossa a posição do EDPB e realiza apontamentos relevantes: (i) em vista do princípio da minimização, é preciso cautela para não realizar uma coleta excessiva de dados ao realizar o procedimento de verificação do consentimento; (ii) em última análise, cabe às organizações (como controladoras) decidir quais métodos de verificação são mais apropriados e proporcionais; e (iii) não há um padrão de referência quanto ao que constitui "esforços razoáveis", tendo em vista a diversidade de estruturas existentes entre os controladores (de modo que aquilo que pode ser considerado um esforço razoável para uma organização pode não ser razoável para outra).

[8] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[9] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[10] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/

[11] https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

Ao dispor sobre a Children's Online Privacy Protection Rule ("COPPA")[12], a Federal Trade Commission ("FTC")[13] também salienta que cabe à organização determinar qual mecanismo utilizará para obter o consentimento parental, listando uma série de mecanismos que considera aceitáveis. São eles: (i) assinar um formulário de consentimento e enviá-lo de volta; (ii) usar um cartão de crédito, cartão de débito ou outro sistema de pagamento online que forneça notificação de cada transação separada ao titular da conta; (iii) ligar para um número gratuito atendido por pessoal treinado; (iv) conectar-se a pessoal treinado por meio de videoconferência; (v) fornecer uma cópia de um documento de identidade; (vi) responder a uma série de perguntas de desafio baseadas em conhecimento que seriam difíceis de responder para alguém que não seja o pai ou responsável; e (vii) verificar uma foto de uma carteira de motorista ou outro documento de identidade com foto enviado pelo pai ou responsável e depois comparar essa foto com uma segunda foto enviada pelo pai ou responsável, usando tecnologia de reconhecimento facial.

Portanto, a Câmara-e.net acredita que cabe a cada organização decidir, com base nos riscos e nas tecnologias disponíveis, o melhor método para verificar o consentimento. Não há um padrão fixo para esforços razoáveis, pois eles variam entre organizações. Ainda, é importante notar que não existe uma solução única ou infalível; diferentes métodos têm seus prós e contras e devem ser avaliados conforme os riscos envolvidos. Para definir parâmetros que garantam o consentimento dos pais ou responsáveis, a ANPD deve considerar a tecnologia disponível, recursos, nível de risco e a natureza dos serviços e produtos. A autoridade deve estabelecer diretrizes flexíveis e práticas, garantindo métodos proporcionais e respeitadores da privacidade.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

O Estatuto da Criança e do Adolescente faz diferenciação clara, em seu artigo 2º, entre a criança (pessoa de até 12 anos incompletos) e o adolescente (pessoas entre 12 a 18 anos), e estabelece, em seu artigo 6º, o dever de interpretação de suas normas considerando a condição peculiar de desenvolvimento desses sujeitos. A abordagem diferenciada para crianças e adolescentes exige considerar

[12] A COPPA é trazida como um exemplo, mas é importante considerar que o consentimento exigido em tal legislação é mais amplo que o consentimento exigido pela LGPD, que se restringe ao consentimento para fins de tratamento de dados pessoais da criança.

[13] https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business

os diferentes estágios de desenvolvimento e autonomia desses titulares, gerando a desnecessidade de representação ou assistência pelos pais ou responsáveis legais no caso dos adolescentes, em respeito ao princípio da condição peculiar de pessoa em desenvolvimento e, em última análise, ao princípio do melhor interesse da criança e do adolescente.

Neste contexto, a Lei Geral de Proteção de Dados Pessoais, em seu artigo 14, dispõe especificamente sobre o tratamento de dados pessoais de crianças e adolescentes, que deve ser feito visando o melhor interesse do menor e respeitando a legislação pertinente. Observa-se que, ao não mencionar a necessidade de consentimento por pelo menos um dos pais ou pelo responsável legal no §1º do artigo 14, a LGPD pretende reconhecer a validade do consentimento manifestado pelo próprio adolescente para tratamento de seus dados, atribuindo-lhe maior liberdade para exercer sua personalidade de forma autônoma, o que deve levar, naturalmente, a uma redução gradual da interferência parental. Nesse sentido, a Câmara-e.net entende que, tendo em vista a condição peculiar de pessoa em desenvolvimento, enquanto às crianças devem ser oferecidos mecanismos de controle parental, ou seja, mecanismos que permitam uma maior participação e definição dos pais e responsáveis, e aos adolescentes devem ser reservados mecanismos de supervisão parental, ou seja, mecanismos mais próximos ao monitoramento, que respeitem e promovam sua autonomia e capacidade, de acordo com os seus respectivos graus de desenvolvimento, requerendo, a depender da idade, maior ou menor autonomia.

O regime de incapacidades do Código Civil Brasileiro não é o melhor parâmetro para o direito à autonomia progressiva, positivado na legislação brasileira, por tratar as crianças e adolescentes como seres passivos que precisam de controle de um adulto e não como indivíduos em desenvolvimento com capacidade de tomar decisões[14]. Este entendimento não é harmônico com os Comentários Gerais nº 12/2009 e 25/2016 do Comitê da ONU sobre Direitos da Criança e com as recomendações da Comissão Interamericana de Direitos Humanos, que estimulam que os países adaptem suas legislações para reconhecer e efetivar a autonomia progressiva das crianças e adolescentes.

[14]TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 287-322; e TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e de adolescentes. Revista do advogado, n. 144, nov. 2019, p. 54-59

O Código Civil Brasileiro não foi criado para o contexto digital, necessitando adaptações para as interações online modernas. É crucial flexibilizar a capacidade civil e a assistência para adolescentes em "atos corriqueiros" online, como criar conteúdo e interagir em plataformas[15]. Presume-se que os pais estão cientes e concordam com essas atividades, uma vez que as plataformas têm proteções e termos conhecidos. A lei brasileira não exige autorização explícita dos pais para todas as atividades dos adolescentes, mas espera que orientem e monitorem o uso da internet de forma abrangente e não invasiva, permitindo a participação dos jovens em atividades digitais rotineiras sob supervisão indireta.

Além disso, tal entendimento é corroborado pela leitura do Relatório da Comissão Especial destinada a Proferir Parecer ao Projeto de Lei 4.060/2012, que originou a LGPD. O relatório destaca que a exigência mais rigorosa de consentimento se aplica ao tratamento de dados de crianças[16]. Portanto, a Câmara-e.net entende que a interpretação que deve prevalecer é a de que os adolescentes podem consentir com o tratamento de seus dados pessoais, respeitando o ECA e os instrumentos internacionais que privilegiam o princípio da condição peculiar de pessoa em desenvolvimento (e que, ao fim e ao cabo, fomentam o melhor interesse desses menores). Tal abordagem diferenciada considera os diferentes estágios de desenvolvimento, com certa flexibilidade para respeitar a autonomia dos adolescentes, além de possibilitar que os pais orientem e monitorem o uso da internet pelos adolescentes de forma abrangente, mas não invasiva, permitindo que os jovens participem das atividades digitais rotineiras, (como por exemplo: interações sociais com colegas/amigos) sob a supervisão geral e indireta dos responsáveis, sem a necessidade de representação/assistência.

[15] Leal, Sheila do Rocio Cercal Santos. Contratos eletrônicos: validade jurídica dos contratos via Internet; Schreiber, Anderson. "Releitura das Incapacidades". In: Manual de Direito Civil Contemporâneo; Tepedino, Gustavo. "Esboço de uma classificação funcional dos atos jurídicos". Instituto Brasileiro de Direito Civil)

[16] COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO PROJETO DE LEI Nº4060, DE 2012. Tratamento e Proteção de Dados Pessoais. Projeto de Lei nº 4.060, de 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/ prop_mostrarintegra?codteor=1663305&filename=

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações “estritamente necessárias à atividade”.

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar “as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança”.

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de design, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:
1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?
Em relação aos princípios, é importante considerar que o ordenamento jurídico já os estabelece. Nesse sentido, no artigo 6º, a Lei Geral de Proteção de Dados Pessoais lista uma série de princípios que devem ser considerados para salvaguardar o direito à proteção de dados. Complementarmente, o artigo 14 estabelece que o princípio do melhor interesse deve ser um balizador no tratamento de dados pessoais de crianças e adolescentes. De igual modo, o direito internacional, a Constituição Federal e o Estatuto da Criança e do Adolescente trazem uma série de princípios aplicáveis a crianças e adolescentes, incluindo o princípio da condição peculiar de pessoa em desenvolvimento. Especificamente no que tange a este princípio, a Câmara-e.net gostaria de destacar a importância de considerá-lo no tratamento de dados de crianças e adolescentes. Isso porque, é preciso que haja equilíbrio entre o desejo de proteger as crianças e os adolescentes no ambiente digital com a necessidade de respeitar o desenvolvimento de capacidades e o alcance paulatino de discernimento. Além disso, é preciso evitar perspectivas excessivas que podem afetar o gozo de diversos direitos, como: liberdade, dignidade como pessoa em processo de desenvolvimento, convivência comunitária, educação, cultura, lazer, etc. Nesse sentido, ao estabelecer orientação sobre como respeitar e proteger os direitos das crianças e dos adolescentes no ambiente digital, para além dos direitos à privacidade,

proteção e segurança, o Conselho da Europa[17] destaca outros direitos que merecem igualmente proteção, são eles: acesso ao ambiente digital, liberdade de expressão e informação, educação e participação.

No mesmo sentido, a Organização para a Cooperação e Desenvolvimento Econômico ("OCDE")[18] entende que atores desempenham um papel ativo na definição de políticas e práticas ou prestação de serviços para crianças e adolescentes no ambiente digital devem considerar suas diferentes necessidades em vista da idade e da maturidade. No mesmo documento, a OCDE destaca que as medidas adotadas por tais atores devem: (i) ser proporcionais aos riscos, baseadas em evidências, eficazes, equilibradas e formuladas com uma visão de maximizar as oportunidades e benefícios para as crianças e adolescentes no ambiente digital; e (ii) promover a liberdade de expressão das crianças e dos adolescentes e não prejudicar outros direitos humanos e liberdades fundamentais.

Assim, entende-se que a condição peculiar de pessoa em desenvolvimento deve ser considerada não só como um princípio, mas também como um parâmetro que guie não só a atuação das organizações como também da própria ANPD. O Age Appropriate Design Code[19] do ICO, por exemplo, trabalha com cinco estágios de desenvolvimento, são eles: pré-alfabetizados e alfabetizados (de zero a cinco anos de idade); anos básicos do ensino fundamental (de seis a nove anos de idade); anos de transição (de dez a doze anos de idade); início da adolescência (de treze a quinze anos de idade); e aproximando-se da idade adulta (de doze a dezessete anos). Além disso, o escritório do Reino Unido fornece um anexo[20] visando trazer clareza sobre os principais aspectos a serem considerados em cada fase.

Outro elemento que pode ser considerado como um parâmetro não só pelas organizações mas pela própria ANPD é a proporcionalidade, a fim de equilibrar o desejo de proteger crianças e adolescentes online com a necessidade de salvaguardar seus

[17] Council of Europe. Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Recommendation CM/Rec(2018)7 of the Committee of Ministers. 2018. Disponível em: <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.

[18] OECD, Recommendation of the Council on Children in the Digital Environment, OECD/LEGAL/0389. Disponível em: <https://legalinstruments.oecd.org/public/doc/272/272.en.pdf>.

[19] Information Commissioner's Office. 3. Age appropriate application. Disponível em: < https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/>.

[20] Information Commissioner's Office. Annex B: Age and developmental stages. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>.

diversos direitos e liberdades, dentre eles o acesso ao ambiente digital, a liberdade de expressão, o acesso à informação e à educação. Uma abordagem baseada em risco, adaptável a diferentes produtos e serviços, que pondere a disponibilidade tecnológica, natureza e propósito é mais um parâmetro que deve ser considerado e que pode ser um grande aliado em uma abordagem guiada pela proporcionalidade. Essa abordagem é um reflexo da própria LGPD, mas também pode ser encontrada em diversos documentos elaborados por autoridades internacionais sobre a temática da proteção de crianças e adolescentes online, dentre elas: ICO[21], Ministério do Interior e das Relações do Reino da Holanda[22], Commission Nationale Informatique & Libertés ("CNIL")[23] e DPC[24].

Além disso, a Camara-e.net reafirma a necessidade de flexibilização do princípio da necessidade com os demais princípios da LGPD, como o princípio do melhor interesse. Tendo em vista que, uma abordagem restritiva ao princípio da necessidade pode impedir a implementação pelo controlador de técnicas eficazes que promovam maior segurança online aos menores. É preciso ter em mente que o tratamento de dados de menores não é contrário ao princípio do melhor interesse, por vezes é necessário o tratamento para apurar se de fato se trata de um dos responsáveis ou se não se trata de uma estratégia que contorne a regra do consentimento parental, e até para adequar o conteúdo a menores de idade.

Aproveita-se esta oportunidade para destacar medidas já adotadas pela indústria como: a limitação do uso de certas plataformas para maiores de 13 anos; a criação de perfis no modo privado por padrão; as limitações impostas à comunicação no casos de contas de crianças e adolescentes; restrições quanto ao uso de certas funcionalidades; disponibilização de informações sobre privacidade e proteção de dados para responsáveis e crianças e adolescentes; dentre outras.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

[21]https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[22] https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf

[23] https://www.cnil.fr/en/digital-rights-children

[24]https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

Como aspecto preliminar, a Câmara-e.net gostaria de destacar que o termo "verificação de idade" abrange uma gama restrita de mecanismos que visam certificar a idade de um indivíduo. Nesse sentido, conforme documento elaborado pelo Future of Privacy Forum[25], a expressão "age assurance" é utilizada para englobar uma variedade mais ampla de mecanismos de certificação de idade: declaração, estimativa e verificação. A declaração incluiria mecanismos nos quais o usuário indica sua data de nascimento, ou nos quais o responsável declara a idade da criança ou adolescente. Já a estimativa abrangeria métodos que vão desde a estimativa da idade com base em imagens faciais até métodos que utilizam outros meios (voz, histórico de navegação, etc.). Por fim, a verificação englobaria mecanismos como aqueles que avaliam um escaneamento de documento em relação a uma foto ou vídeo, utilizando reconhecimento facial e aqueles que se utilizam de identidades digitais. No mesmo sentido, o Office of the Privacy Commissioner of Canada[26], em consulta que está sendo realizada sobre proteção de dados e “age assurance”, adota a terminologia sugerida pelo FPF.

Em relação à temática de certificação de idade, é preciso que essa Autoridade considere que não há uma solução única e/ou perfeita. Nesse sentido, a DPC[27] destaca que: (i) a área tecnológica de mecanismos e ferramentas de certificação de idade ainda está em desenvolvimento; e (ii) não existe uma solução única para a questão da certificação de idade, de modo que mecanismos apropriados provavelmente variarão, dependendo, por exemplo, de fatores como o serviço sendo oferecido e a sensibilidade dos dados pessoais sendo tratados. A CNIL[28] salienta que todas as soluções atualmente propostas podem ser, em alguma medida, burladas. Além disso, ao analisar várias soluções existentes para certificação de idade, a autoridade francesa pontuou que nenhuma delas atenderia satisfatoriamente os seguintes requisitos: verificação suficientemente confiável, cobertura completa da população e respeito à proteção dos dados e privacidade dos indivíduos, bem como sua segurança.

Como visto, a verificação da idade dos usuários é um desafio técnico que pode variar significativamente conforme a natureza do serviço. Assim, as orientações da ANPD devem reconhecer que não existe um método único de verificação que seja melhor que

[25] https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf

[26] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-age/expl_gd_age/

[27] https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

[28] https://www.cnil.fr/en/digital-rights-children

outros, pois a escolha do mecanismo adequado depende do contexto específico, incluindo a finalidade e a natureza do tratamento dos dados, bem como o modelo de negócios envolvido. Ainda, é crucial considerar que os sistemas de verificação de idade não são infalíveis e que cada método pode apresentar suas próprias limitações e vantagens; A possibilidade de crianças burlarem esses mecanismos, como ao usar o celular dos pais, exemplifica a falibilidade dessas medidas. Nesse sentido, é fundamental que a autoridade enxergue esses esforços com base em melhores esforços; ou seja, mecanismos para que se tente identificar possíveis fraudes e corrigi-las.

A Electronic Frontier Foundation ("EFF")[29], em 2023, levantou preocupações importantes sobre o equilíbrio dos riscos associados aos mecanismos de verificação de idade. A EFF argumenta que tais sistemas funcionam como formas de vigilância, o que leva a organização a se opor a leis que obrigam a implementação desses mecanismos. Esse debate destaca a complexidade de encontrar um equilíbrio adequado entre a proteção dos dados e a privacidade dos usuários e as preocupações com a vigilância excessiva. Nesse sentido, a avaliação da razoabilidade e a proporcionalidade são essenciais, especialmente considerando que pequenas empresas podem enfrentar custos significativos na implementação dessas ferramentas, enquanto grandes empresas de tecnologia podem ter recursos mais abundantes.

A ANPD tem oportunidade de liderar o debate e dispor sobre os mecanismos de verificação de idade, a partir de orientações que assegurem a consistência com as preocupações acima aventadas. Evitando, assim, que outras autoridades façam sem a devida consideração à proteção de dados, gerando insegurança jurídica para os agentes de tratamento de dados, como por exemplo o Projeto de Lei nº 2628 de 2022 e a Resolução do CONANDA, que estabelecem mecanismos de verificação de idade que desconsideram particularidades contextuais e desafios técnicos, a partir de uma abordagem não condizente com interpretações da ANPD sobre a LGPD.

Dessa forma, para além das contribuições acima e a fim de subsidiar a presente Autoridade nessa tarefa, a Câmara-e.net lista alguns de mecanismos de verificação que são utilizados por seus associados: autodeclaração, inserção do e-mail do responsável,

[29] https://www.eff.org/pt-br/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online

fornecimento de informações de cartão de crédito, etc. Um outro aspecto a ser considerado pela Autoridade, são soluções que possam ser aproveitadas pelo setor privado como um todo, em colaboração e coordenação de atores que atuam em camadas diferentes do ecossistema digital.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

Inicialmente, é preciso esclarecer o recorte do artigo 14, §4º da LGPD, que dispõe que os controladores não deverão condicionar a participação de crianças em jogos, aplicações de internet e outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. O parágrafo faz remissão clara às disposições do parágrafo 1º, sobre tratamento de dados pessoais de crianças, e não de adolescentes, qualquer interpretação extensiva na tentativa de equiparar crianças e adolescentes poderia gerar violação ao princípio da condição peculiar de pessoa em desenvolvimento, presente nas mais diversas normas protetivas, como na Constituição Federal, no Estatuto da Criança e do Adolescente na Convenção sobre os Direitos da Criança, promulgada pelo Decreto nº 99.710/1990 e com a Doutrina.

Como destacado pela Câmara-e.net em outros momentos desta contribuição, é importante considerar o princípio do melhor interesse e a condição peculiar da pessoa em desenvolvimento no tratamento de dados de crianças e adolescentes. É preciso evitar perspectivas excessivas que podem afetar o gozo de diversos direitos, como: liberdade, dignidade como pessoa em processo de desenvolvimento, convivência comunitária, educação, cultura, lazer, etc., para que haja equilíbrio entre o desejo de proteger as crianças e os adolescentes no ambiente digital com a necessidade de respeitar o desenvolvimento de capacidades e o alcance paulatino de discernimento. Qualquer restrição automática ou pré-definida para a coleta de dados pessoais de crianças e adolescentes para além das já explícitas na legislação, pode resultar em maior insegurança para os menores e agentes de tratamento. Além disso, a LGPD não estabelece restrições específicas ao tratamento de dados de crianças e adolescentes, inclusive dados pessoais sensíveis, desde que o agente de tratamento justifique com base legal adequada, implemente medidas necessárias para cumprimento das obrigações estabelecidas pela LGPD e que este tratamento seja alinhado com o melhor interesse dos menores.

Em relação à formação de perfis comportamentais, embora exista uma tendência de enxergar a prática com preocupação, estes não devem ser associados automaticamente a práticas prejudiciais. O uso destas tecnologias representa diversos benefícios, principalmente quanto ao tratamento de dados de crianças e adolescentes. Por vezes, é necessário formar perfis comportamentais para cumprimento de obrigações legais, regulatórias e até mesmo para indicar conteúdos adequados à idade do usuário e restringir o conteúdo inadequado. A formação de perfis comportamentais também pode ser usado no combate de ilícitos, para melhorar a precisão da estimativa de idade, além de permitir personalização de serviços para oferecer experiências relevantes e seguras para crianças e adolescentes, dentre outras várias situações nas quais as técnicas de elaboração de perfis comportamentais são utilizadas, justamente, no melhor interesse da criança e do adolescente.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

Aproveita-se o questionamento para reiterar que nem sempre o consentimento será a melhor forma de salvaguardar o melhor interesse de crianças e adolescentes. Esse foi o entendimento esposado pela ANPD no estudo que fundamentou o Enunciado CD/ANPD nº 01/2023. Embora o consentimento possa ser uma ferramenta importante na proteção de dados de crianças e adolescentes, em alguns casos seu uso não será a solução mais adequada. A necessidade de equilibrar a proteção e a autonomia na proteção de crianças e adolescentes no ambiente digital também fundamenta essa perspectiva.

Nesse sentido, destaca-se que as medidas de proteção de privacidade para menores devem ser adaptáveis aos níveis de maturidade e autonomia, em consonância com o princípio da condição peculiar de pessoa em desenvolvimento. As configurações de privacidade não devem ser rígidas, mas sim flexíveis, permitindo ajustes que correspondam à idade e ao estágio de desenvolvimento do usuário. Essa abordagem reconhece que diferentes idades e níveis de compreensão exigem diferentes níveis de proteção e interação, respeitando a autonomia progressiva e o melhor interesse da criança e do adolescente, conforme a legislação brasileira e internacional exigem. Nesse sentido, a Câmara-e.net entende que, tendo em vista a condição peculiar de pessoa em desenvolvimento, enquanto às crianças devem ser oferecidos mecanismos de controle parental, ou seja, mecanismos que permitam uma maior participação e definição dos pais e responsáveis, e aos adolescentes devem ser reservados mecanismos de supervisão parental, ou seja, mecanismos mais próximos ao monitoramento, que respeitem e promovam sua autonomia e capacidade, de acordo com os seus respectivos graus de desenvolvimento, requerendo, a depender da idade, maior ou menor autonomia.".

Em outro ponto, é preciso que se considere a diversidade de agentes que atuam no ecossistema digital, diversidade essa que encontra-se refletida nas medidas adotadas por esses atores, são exemplos:

- Redes sociais: mecanismos de sincronização familiar, que vinculam a conta dos pais às dos filhos; ajustes do tempo de uso de tela pelos responsáveis; ativação de restrições como: impedimento para iniciar lives, aplicação de filtros a comentários publicados, restrição de quem pode enviar mensagens aos adolescentes; disponibilização de ferramentas que promovem o diálogo entre os pais e os adolescentes; transparência voltada aos pais e responsáveis; mecanismos de limitação de anúncios; acesso as interações com terceiros; possibilidade de edição do perfil; impossibilidade de participação em programas de recompensa, recarga e gratificação, sem assistência; limitação do conteúdo visualizado; possibilidade de denunciar contas de terceiros;
- Plataformas de compartilhamento de vídeos: atualizar informações e configurações da conta; excluir a conta; gerenciar os controles de atividades;
- Plataformas de streaming: escolher os conteúdos que serão disponibilizados; criar um perfil que terá apenas conteúdo selecionado para crianças e que não terá acesso as configurações da conta; criação de perfis com classificação indicativa; gerenciamento do perfil;
- Plataformas de e-commerce: controle das compras feitas;
- Jogos: definir permissões para contar de crianças e adolescentes que afetam atividades específicas (jogos multijogador, convites para entrar em jogos de outros jogadores, possibilidade de comunicação, compras); limitação de compras; recomendações de idade que consideram o conteúdo; possibilidade de gerenciamento do conteúdo acessível; e
- Lojas de aplicativos: aplicativos e conteúdos de vídeo com classificação indicativa, ferramenta de controle parental que permite selecionar, com base nas faixas etárias, quais aplicativos serão visíveis na loja; organizador pode usar recursos como: “restrições”, “tempo de uso” e “pedir para comprar”; possibilidade de restringir o uso de certas ferramentas e o uso de certos aplicativos; possibilidade de aprovação, pelos pais, do download de aplicativos; e realização de verificação de idade.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

A transparência direcionada aos pais e responsáveis ajuda a garantir uma supervisão eficaz sobre o uso de plataformas por crianças e adolescentes. Guias específicos, com uma linguagem clara e acessível, são importantes para que os pais compreendam as ferramentas e mecanismos disponíveis para o cumprimento de seu dever de supervisão.

Embora a Política de Privacidade (PP) deva conter todas as informações necessárias sobre o tratamento de dados, não é necessário que ela seja exibida continuamente, o que poderia causar fadiga aos usuários e seus responsáveis. Em vez disso, é mais eficiente relembrar as informações específicas sobre o tratamento em momentos pertinentes e diretamente relacionados às ações do serviço.

As informações fornecidas aos usuários e seus responsáveis precisam ser relevantes e compreensíveis. A quantidade de informações não garante transparência, especialmente se essas informações forem complexas e menos propensas a serem lidas e compreendidas. Além da PP, outros meios de comunicação, como artigos em centrais de transparência, se disponíveis, ou notícias divulgadas pelos agentes de tratamento, podem complementar a transparência. Esses meios adicionais podem ajudar a assegurar que os dados sejam tratados para finalidades legítimas e informadas ao titular, especialmente durante a utilização dos produtos e serviços, por meio de notificações e outros recursos específicos.

A transparência deve ser adaptada às necessidades e às características dos usuários. Isso pode ser alcançado através de portais e outros meios que utilizem elementos visuais, interativos e de linguagem facilitada para tornar a compreensão das informações mais acessível para adolescentes. A adoção de mecanismos que transmitam a informação de forma facilitada (como vídeos lúdicos ou gamificação) pode ser uma alternativa. Além disso, é importante fornecer suporte e informações apropriadas aos pais e responsáveis legais sobre as práticas de tratamento de dados e recursos de supervisão parental.

Entretanto, entendemos que não há necessidade de a Política de Privacidade conter uma seção específica dedicada ao tratamento de dados de menores. Em vez disso, uma abordagem positiva é adotar uma Política que utilize uma linguagem clara e acessível, considerando as necessidades específicas deste público e mais compreensíveis tanto para os menores quanto para seus responsáveis. Deste modo, a Política pode oferecer uma proteção robusta e adequada sem a necessidade de uma seção separada.

É necessário, ainda, equilibrar a transparência com a proteção dos segredos comerciais e industriais. Informações excessivas sobre ferramentas de tratamento de dados podem facilitar a ação de agentes mal-intencionados que busquem contornar mecanismos de segurança, colocando em risco a proteção dos usuários. Portanto, deve-se estabelecer uma transparência adequada que priorize a segurança e os melhores interesses dos titulares dos dados.

Por fim, manter uma colaboração contínua com pais, responsáveis legais e adolescentes ajuda a aprimorar os recursos de transparência disponíveis. Essa parceria é importante para melhorar a compreensão e a gestão das questões de privacidade e segurança, ajustando as práticas para atender às necessidades e preocupações dos usuários.
6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?
A Câmara-e.net gostaria de chamar a atenção desta Autoridade para a crescente importância e complexidade das discussões sobre a proteção de crianças e adolescentes no ambiente digital. Em meio a debates em diversos fóruns e iniciativas de diferentes entidades, há um potencial significativo de conflitos relacionados às competências da ANPD e à integridade da Lei Geral de Proteção de Dados. Assim, para além dos aspectos trazidos ao longo desta tomada de subsídios, a Câmara-e.net encoraja respeitosamente a ANPD a adotar medidas e emitir posicionamentos que fortaleçam não só sua autoridade como órgão competente para regulamentar o tratamento de dados pessoais de crianças e adolescentes, mas também para evitar conflitos com a própria LGPD e com os entendimentos já consolidados pela própria Autoridade sobre a temática.

Response to consultation
Making Subsidies: Processing of Personal Data of Children & Adolescents

16 July 2024

About Yoti

Yoti is a digital identity company that makes it safer for people to prove who they are. Founded in April 2014, we started by creating a secure Digital ID app which gives people a safer and instant way to prove their identity, with no need to show identity documents or share an excessive amount of personal data. Yoti now provides verification solutions across the globe, spanning identity verification, age verification, age estimation, eSigning and authentication. We're a team of over 400 people, working together to shape the future of digital identity.

We're committed to making the digital world safer for everyone. Our seven ethical principles guide us in everything we do and we're held accountable by our independent Guardian Council, whose minutes we publish. With an award-winning social purpose strategy, we're always looking for new ways to explore what (digital) identity means globally. The journey isn't one we're making alone, but with the help of policy advisers, think tanks, researchers, humanitarian bodies and everyday people.

What we are doing and why:

- Transforming the way individuals can prove their age and identity
- Increasing security and privacy of personal data
- Helping to create age-appropriate experiences and safer communities online
- Creating the most reliable and comprehensive identity verification solutions
- Shaking up the way we sign documents

Technology as a force for good - Yoti was founded on seven business principles which guide our actions. Yoti is also a founding UK B Corp meaning we aim to balance profit with purpose.

Security credentials - We commission regular external audits of our business and have been certified to meet some of the world's most stringent security standards, such as ISO 27001 and SOC2 Type II. We are also certified by the UK Government under the UKDIATF. (Digital Identity & Attributes Trust Framework).

A transparent, open and honest approach - Yoti publishes regular white papers to build trust and understanding of our technology.

Yoti has conducted over 600 million age checks; hence we bring the benefit of that experience to our response; as per the chart below. We already offer age assurance checks at a variety of ages 18+, 25+, 13-17 and under 18 and we support parental consent.

Consultation

1. In addition to the aspects covered in Statement CD/ANPD nº 01/2022 and in the Guidance on the legal hypothesis of legitimate interest, which issues related to the principle of best interest require specific guidance or regulation by the ANPD?

1. **Definition and Scope of Best Interest**:
    - Clear definitions of what constitutes the "best interest" in various contexts, especially concerning children and other vulnerable groups.
    - Criteria or guidelines for assessing the best interest in data processing activities.
2. **Age Verification and Consent**:
    - Methods and technologies for verifying the age of data subjects, particularly children; ideally linking these to the best practise work of the global age assurance standards -

        IEEE 2089.1 Standard for Online Age Verification was published in May 2024, the result of over two years of deliberation by a working group of industry experts from around the world.

ISO/IEC 27566 (CD)

ISO/IEC 27566 Information security, cybersecurity and privacy protection — Age assurance systems — Framework Part 1: Framework has reached the Committee Draft stage in its development, which means there is a stable document which has been agreed by the relevant global working group (SC27/WG5).

- Guidelines on obtaining and managing consent from parents or legal guardians for processing children's data.
- Clarification on situations where consent might not be necessary and the role of legitimate interest in those cases.

3. **Data Minimization and Purpose Limitation**:
   - Best practices for ensuring data minimization and purpose limitation in the context of children's data.
   - Specific examples or scenarios where data minimization should be prioritized.
4. **Transparency and Communication**:
   - Requirements for transparency and clear communication with children and their guardians about data processing activities.
   - Development of child-friendly privacy notices (using plain language) and communication strategies.
5. **Rights of Data Subjects**:
   - Procedures for exercising data subject rights, particularly for children.
   - Guidelines on handling requests from children or their guardians to access, correct, or delete data.
6. **Data Security and Protection Measures**:
   - Enhanced security measures for protecting children's data.
   - Recommendations for regular security assessments and audits specific to data involving children.
7. **Impact Assessments and Risk Management**:
   - Guidelines for conducting Data Protection Impact Assessments (DPIAs) with a focus on children's data.
   - Risk management frameworks that include specific considerations for the best interest of children.
8. **Educational and Awareness Programs**:
   - Initiatives for educating children, parents, and guardians about data protection rights and best practices.

- Development of educational materials and resources tailored for different age groups.

9. **Enforcement and Penalties**:
   - Clear consequences and penalties for non-compliance with best interest principles in data processing.
   - Mechanisms for reporting and addressing violations involving children's data.
10. **Collaboration with Other Authorities**:
    - Guidelines on collaboration with other regulatory bodies, child protection agencies, and educational institutions to ensure a holistic approach to data protection for children.

By addressing these issues, the ANPD can provide comprehensive guidance and regulation to ensure that the principle of best interest is effectively applied and upheld in the context of data protection, especially for vulnerable groups such as children.

We would signal to the ANPD the work of the ICO in terms of its guidance in the Age Appropriate Design Code; the international regulators working group on age assurance, the work of the EU Consent Project and its deliverables in terms of childs rights, led by Professor Sonia Livingstone which are publicly available.

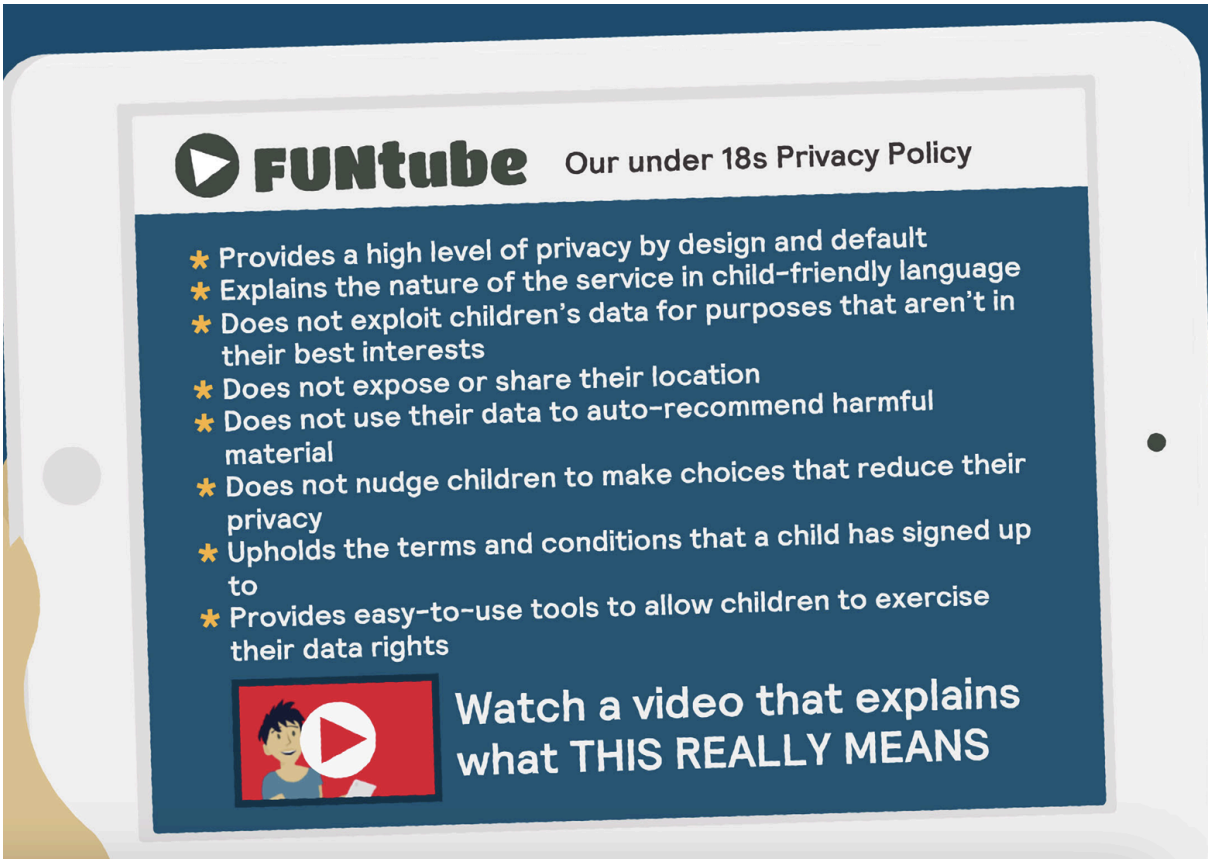
2. Are there specific situations or contexts in the processing of personal data of children and adolescents that require greater attention and detail regarding the principle of best interests? If so, indicate which situations or contexts were identified and the main issues to be addressed.

The non profit 5rights produced a publication 'Demystifying the Age Appropriate Design Code[1]', see the slides below which highlight key elements required by platforms to act in the best interest of the child.

Context
30% of people online are minors and minors are not solely to be found on sites designed for children. Sites aimed at adults may also attract minors - for instance adult content, dating, gambling. Immersive/AR/VR sites may offer blended social and adult or gaming and adult offerings, for instance with gambling or crypto currency provision. In all of these settings the personal data of minors may be being processed, if they are treated as though they are adults and not recognised as minors. This may include location data as well as sensitive age, gender or health data.

[1] https://5rightsfoundation.com/uploads/demystifying-the-age-appropriate-design-code.pdf

The context may also lead to a child being offered to set up a contract, under age, to engage with age inappropriate content, witness age inappropriate conduct or contact.



Targeted advertising and marketing directed at children and adolescents.
A clear issue is preventing the profiling of minors for advertisment purposes, ensuring that marketing content is appropriate and not manipulative, and relying on a valid legal basis for data collection. Limitations are clearly necessary in terms of behavioral advertising targeting minors.

IoT and Smart Devices and immersive environments
The Use of smart toys, wearables, and other Internet of Things (IoT) devices by children brings the challenges of ensuring device security and data encryption, providing clear information on data collection and sharing practices, and obtaining parental consent for data use.
Manufacturers and platforms should conduct regular security assessments and offer easy-to-use privacy controls.
Data leakage will be infinitely higher in immersive environments; divulging sensitive age, gender, motor or cognitive delay or acuity.

II - Consent

1. What criteria or parameters must be observed to obtain “specific and prominent” consent from parents or legal guardians?

From our experience, obtaining "specific and prominent" consent from parents or legal guardians for processing the personal data of children involves adhering to a number of parameters to ensure that the consent is informed, voluntary, and clearly communicated. Key elements to observe:

1. **Plain Language**: Use clear, simple, and age-appropriate language to explain what data will be collected, how it will be used, and who it will be shared with. This must avoid tech jargon or ‘legalese’
2. **Transparent, Comprehensive Information**: Parents need clear detail about the data processing activities, the types of data collected, the purposes for data collection, and the data retention period, the specific purposes for which consent is being sought.
3. **Easy to read** - consent requests need to be displayed clearly
4. **Specific separate Consent** for different data processing activities, eg. consent for collecting data should be separate from consent for sharing data with third parties.
5. **Informed & opt-in** opt-in mechanisms ensure active and affirmative, informed consent is given
6. **More info -** additional educational materials or FAQs can help parents or guardians understand the implications of their consent.
7. **Voluntary -** avoiding any form of coercion or undue pressure.
8. **Revocation/Withdrawal Options**: Clearly explain that consent can be easily revoked at at any time & show the method
9. **Documentation and Record-Keeping** - Keeping detailed records of the consent obtained, including the date, the method of obtaining consent, and the specific information provided. Maintain audit trails to demonstrate compliance with consent requirements.
10. **User-Friendly Design** which is **Intuitive Interface**: an intuitive consent interface is user-friendly and minimizes the steps required to give or withdraw consent.
11. **Clear Actions**: Use clear action buttons (e.g., "I Agree" / "I Do Not Agree").
12. **Ongoing Communication**: Keep parents or guardians informed of any changes in data processing practices and obtain renewed consent if necessary; reviewing and updating consent forms to ensure continued compliance.

Verification of Parent/ Guardian Status:

- **Age assurance**: Offer a range of age verification or age estimation mechanisms to ensure that consent is being sought from an age appropriate individual (i.e., an adult who is old enough to be the parent or legal guardian; typically this is above the age of 25).
- This may be from a government issued identity document or this may be via checks to sources such as credit card or credit reference agencies. For inclusion, it may also be via an age estimation approach, such as **facial age estimation.**

[Here below, is included data, on the public record from the joint application by Yoti, ESRB, Superawesome to the FTC[2], with the response letter in footnote[3]; we are able to resubmit following the now complete NIST Benchmark of Facial age estimation.

The Commission is aware that Yoti submitted a facial age estimation model to the National Institute of Standards and Technology ("NIST") in September 2023,[4] and Yoti has stated that it anticipates that a report reflecting NIST's evaluation of the model is forthcoming. The Commission expects that this report will materially assist the Commission, and the public, in better understanding age verification technologies and the ESRB group's application. Therefore, rather than staying or extending the deadline for the Commission to make a decision on the application, the Commission is declining the application without prejudice to the applicants refiling in the future. The public would have an opportunity to comment on a refiled application. In declining the application at this time, the Commission is taking no position on the merits of the ESRB group's application.]

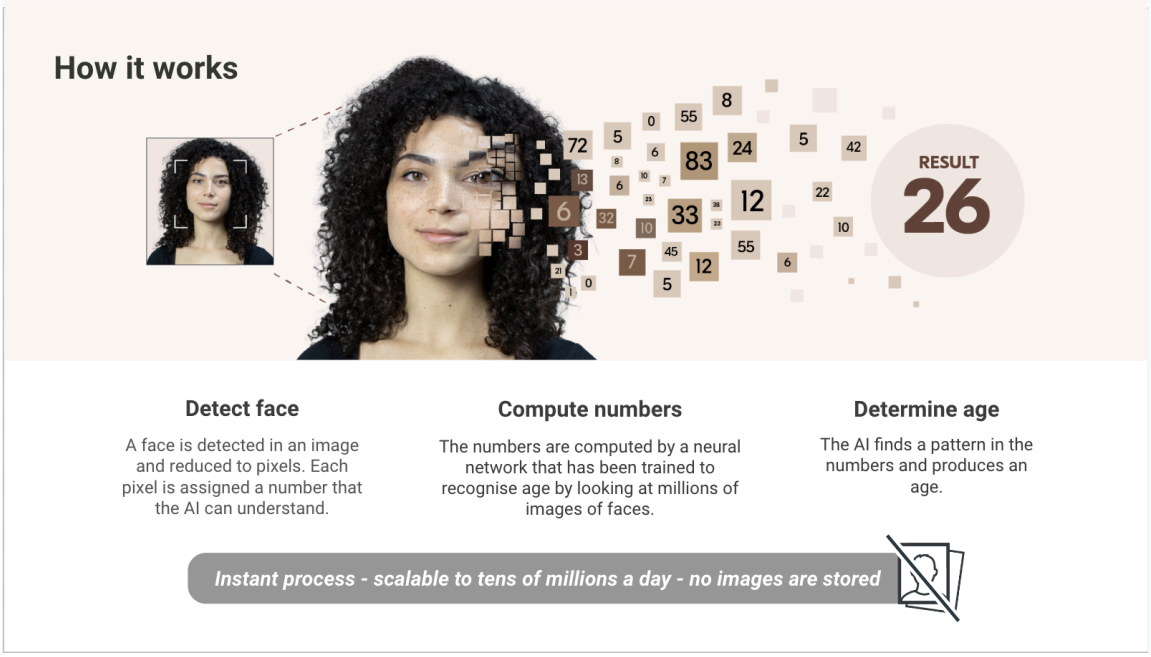
The following diagram from the *Yoti White Paper* illustrates the facial age estimation process:[5]

[2] /https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf

[3] https://www.ftc.gov/system/files/ftc_gov/pdf/ESRB%20group%20decision%20letter%203.28.24_0.pdf

[4] https://pages.nist.gov/frvt/html/frvt_pad.html

[5] *Yoti White Paper*, *id*. at 20.



How Facial Age Estimation Technology Works

Facial age estimation uses computer vision and machine learning technology to estimate a person's age based on analysis of patterns in an image of their face. The system takes a facial image, converts it into numbers, and compares those numbers to patterns in its training dataset that are associated with known ages. By contrast, facial *recognition* technology, which seeks to identify a specific person based on a photo, looks for unique geometric measures of the face, such as the distance and relationship among facial features, and tries to match these to an existing unique set of measurements already recorded in a database along with unique identifying information.

In Yoti's case, the company trains its neural network model by feeding it millions of images of diverse human faces with their actual month and year of birth.[6] The system converts the pixels of these images into mathematical functions that represent patterns. Over time, the system has learned to correlate those patterns with the known age.

When performing a new age estimation, the system extracts the portions of the image containing a face, and only those portions of the image are analyzed for matching patterns. To

[6] Yoti collected its training data in accordance with the EU GDPR via the Yoti app. The Yoti app is a secure digital ID application that allows consumers to store their identification documents in one securely encrypted place, and to share that information (or share only the relevant attributes, such as age) with a business. The app has been downloaded 13 million times. For more information on how Yoti collects and handles model training data, *see* Yoti, *Facial Age Estimation: White Paper* at 27 (Mar. 2023) ("Data used to build the model ('training data')"), https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf ("Yoti White Paper").

match patterns, each node in Yoti's neural network performs a mathematical function on the pixel data and passes the result on to nodes in the next layer, until a number finally emerges on the other side. The only inputs are pixels of the face in the image, and the only outputs are numbers. Based on a review of the number patterns, the system creates an age estimation.

Although an individual's age may be considered an attribute of their identity, establishing the identity of an individual is not necessary to gain age assurance. Because the only data used to train the model are face images and the person's age in months and years, the model cannot work out anything other than the person's estimated age.

When using Privacy-Protective Facial Age Estimation, the user takes a photo of themselves (a selfie) assisted by an auto face capture module that guides the positioning of their face in frame. The system then checks whether there is a live human face in the frame and requires the image to be captured in the moment.[7] The upload of still images is not accepted, and photos that do not meet the required level of quality to create an age estimate are rejected. These factors minimize the risk of circumvention and of children taking images of unaware adults.[8]

The captured image is securely transmitted from the user's device to the Yoti backend server for age estimation processing using TLS 1.2 encryption.

The processing takes on average less than one second. For the use case of parent verification, the operator receives only a yes/no result on whether the individual in the image meets a designated age threshold. If the image does not meet the age threshold, the individual may be permitted to restart the verification process (as configured by the operator). Images are immediately, permanently deleted, and not used by Yoti for training purposes.

Yoti and SuperAwesome have implemented the Privacy-Protective Facial Age Estimation method for legally required parental consent in territories outside the U.S. and have—since 2022—delivered more than 4.8 million age estimations using this method for this purpose.[9]

- *Facial Age Estimation is accurate* – in the Applicants' implementation the facial age estimation system correctly estimates that someone is an adult 99.97% of the time.[10]

---

[7] This proprietary anti-spoofing technology has been tested and approved by the National Voluntary Laboratory Accreditation Program of the United States' National Institute of Standards and Technology (NIST). For more information, *see* National Voluntary Laboratory Accreditation Program (NVLAP), https://www.nist.gov/nvlap.

[8] For more information about how Yoti's anti-spoofing technology works, *see* Yoti, *Yoti MyFace Liveness: White Paper* (Mar. 2023), https://www.yoti.com/wp-content/uploads/Yoti-MyFace-Liveness-White-Paper-March-2023.pdf.

[9] Analytics data from KWS and Yoti, since 2021, across multiple customer implementations worldwide. For more information about Kids Web Services, including examples of current live customer implementations, *see* https://dev.superawesome.com/.

[10] The proportion of those estimated to be over the configured threshold of 25 who are in fact adults (18 or older).

- *Facial Age Estimation is effective* – on average 35% of users in the EU and U.K. who attempt to prove they are adults are rejected for being under the threshold age (they can choose another method if they disagree). *Facial Age Estimation is private* – it requires no collection of identity or payment card information, and no images are stored. *See* Section II.C, Parents' Privacy.
- *Facial Age Estimation is inclusive* – everyone has a face, but not everyone has a payment card, passport, driver's license or social security number (SSN).
- *Facial Age Estimation is equally, or more, reliable than existing methods* – when combined with a liveness test, face scan is very difficult to spoof.
- *Facial Age Estimation is preferred by users* – when given a choice of three methods, generally over 70% of users choose facial age estimation.
- *Facial Age Estimation is easier to use* – 91%+ of users who start the face scan flow complete it, as compared to 65% for payment cards, or 66% for SSN.

(for appendices see /https://www.ftc.gov/system/files/ftc_gov/pdf/Application-for-a-new-VPC-method-ESRB-SuperAwesome-Yoti-06-02-2023.pdf)

SuperAwesome's Kids Web Services ("KWS") currently deploys Facial Age Estimation in its parental consent tool as a verification method that developers can choose to make available to parents outside the U.S. alongside other methods, such as payment card or identity documents scan. Developers integrate KWS' parent verification (PV) module with their existing parental permissions flow, typically adding it at the end to verify that the person providing the permissions is an adult.

Examples of legally required parental consent flows powered by KWS, which use Facial Age Estimation, can be seen live in the account creation flows (outside the U.S.) of SuperAwesome KWS customers, including Epic Games.

For use as a PC (parental consent) method, Privacy-Protective Facial Age Estimation can be deployed as follows:

1. Child visits an online service and is presented with a neutral age gate.
2. Operator collects a parent's email address from the child.
3. Operator sends direct notice to parent
4. Parent provides relevant permissions for the child.
5. Operator informs parent of the requirement to verify they're an adult; offers parent a choice of verification methods.
    a. Parent selects Privacy-Protective Facial Age Estimation.
    b. Parent is given notice of how facial age estimation works and provides consent for the collection of a face scan for the purpose of PC.
    c. Parent provides consent to access the camera on their device.

d. Parent presents face to the camera, the system performs a liveness test and takes a selfie.
e. Age estimation takes place and collected image is deleted.
f. System provides results of age estimation to operator, confirming whether the parent is over the configured age threshold.

6. If Facial Age Estimation concludes the person is not an adult, then one of the following will occur (depending on the operator's configuration):
    a. If the person is estimated as being 18-25, or there is some other uncertainty about whether the person is an adult, the person is returned to the beginning of step 5, where they can choose an alternative verification method that uses additional personal information, such as a payment card, driver's license or SSN.
    b. If the person is estimated as being under the age threshold, the operator will inform the person that PC is denied and direct them to contact the operator's customer support if they disagree with the result or believe there was a technical error.

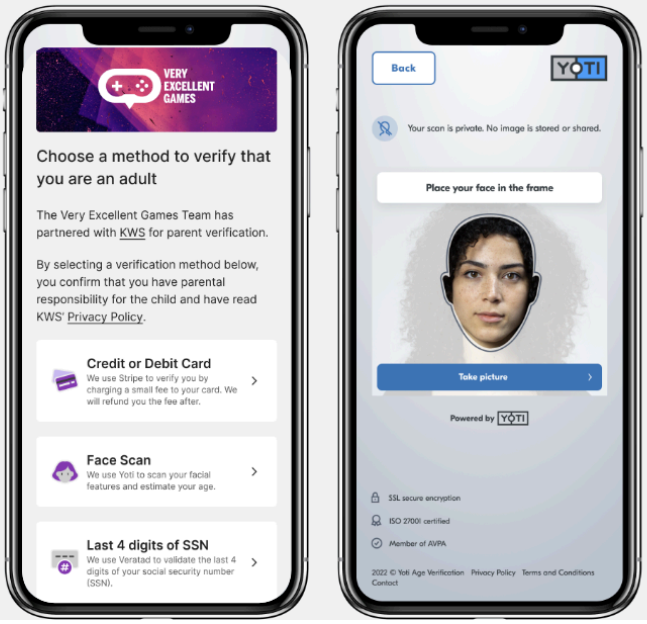
Seamless verified parental consent with age estimation checks

Yoti and KWS have implemented Yoti's Facial Age Estimation method for legally required parental consent in territories outside the U.S. and have—since 2022—delivered more than 5 million age estimations using this method.

1. **User detected to need Verified Parental Consent**
   User enters an 'under age of consent' date of birth at the age gate and enters parent email address.

2. **Parent required to prove age to ensure they are an adult**
   Parents sent an email and required to complete age verification.

3. **Parent selects age estimation and completes the process.**
   Age is estimated and parent moves on to consent options.
   .



2. Considering good practices, available technologies and the principles of the LGPD, in particular the principles of purpose, necessity and suitability, as well as the legal requirement to adopt "all reasonable efforts", what measures and mechanisms do controllers should they adopt, especially in the digital environment, to enable and verify that consent was provided by the child's parents or guardians?

The method described above, 'Facial Age Estimation' is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. In addition, the method promotes children's privacy, does not present any substantial risk to parents' privacy, and addresses issues of potential bias and discrimination as well as inclusion. Facial Age Estimation preserves privacy by not requiring the parent to produce additional identity documentation or information. Facial Age Estimation is not used to determine that the individual is who they claim to be, but to determine that the individual is the *age* they claim to be.

All the currently approved US VPC methods establish that the person is an adult; none of them definitively authenticates the parent-child relationship.[11] The COPPA Rule, nonetheless, permits these methods in line with the Rule's qualification that new VPC methods be held to the standard of "reasonably available technology," not a requirement of perfect, still-to-be developed, solutions.

Moreover, children cannot easily circumvent Facial Age Estimation, which requires the live participation of an adult who is old enough to be the child's parent to submit to the process. A child's 14-year-old sibling or 18-year-old babysitter, for example, would not be able to pass the Facial Age Estimation process. This makes it more likely that the person going through the age estimation flow is the child's parent.
Facial Age Estimation also addresses privacy-related issues such as inclusion as well as bias and discrimination.[12] Parents who do not have a social security number or a payment card can use the facial age estimation process.

III - Internet games and applications

1. What principles, parameters and safeguards, including design measures, must be observed when processing personal data of children and adolescents by digital platforms, in order to ensure respect for

[11] *See* Yoti Response to the Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule (Responses to Q.1a and Q.7) (Mar. 22, 2020), https://www.regulations.gov/comment/FTC-2019-0054-113202.

[12] The FTC recently set out various concerns that biometric information technologies, such as those that process facial images, "can lead or contribute to harmful or unlawful discrimination." FTC, *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act* [hereinafter, *Biometric Information Policy Statement*] 4-5 (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. The FTC has long stressed the importance of addressing unlawful bias and discrimination as well as other harms arising from data-intensive technologies. *See e.g.*, FTC, *Combatting Online Harms Through Innovation: A Report to Congress* (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf;
FTC, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. Just last month, the agency, along with officials from the Department of Justice (DOJ), the Consumer Financial Protection Bureau (CFPB), and the Equal Employment Opportunity Commission (EEOC) released a joint statement announcing the agencies' resolve to monitor automated systems for bias and discrimination and "vigorously use our collective authorities to protect individuals' rights regardless of whether legal violations occur through traditional means or advanced technologies." S*ee Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems* 3 (Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

their best interests, promote and ensure high levels of privacy and protection of personal data and mitigate the risks arising from the use of these platforms?

We would advocate the following measures to be observed:

1. **Best Interest of the Child**:
    - Ensure that the processing of personal data always considers the best interests of the child, prioritizing their well-being, safety, and development.
2. **Transparency**:
    - Provide clear, understandable, and age-appropriate information about data processing practices, including what data is collected, how it is used, and with whom it is shared.
3. **Purpose Limitation**:
    - Collect and process personal data only for specific, explicit, and legitimate purposes relevant to the child's use of the platform.
4. **Data Minimization**:
    - Limit the collection of personal data to what is necessary for the intended purpose, avoiding excessive or unnecessary data collection.
5. **Security**:
    - Implement robust security measures to protect personal data from unauthorized access, loss, or misuse.
6. **Consent**:
    - Obtain verifiable parental / guardian consent before collecting or processing the personal data of children, ensuring the consent process is clear and straightforward.

Parameters and Safeguards

1. **Age assurance**:
    - Implement a range of reliable, independently audited age assurance mechanisms, meeting international standards - eg PAS1296:2018, ISO, IEEE
    - Offering choice to the consumer of age assurance options
    - Ensuring that parental consent is obtained from the appropriate party (parent or guardian) for children under the age of consent.
    - In each instance, a data minimised age attribute can be shared.
2. **Parental Controls and Oversight**:
    - Provide tools for parents or guardians to monitor and control their child's activities on the platform, including data collection and sharing preferences.

3. **Data Subject Rights**:
    - Ensure that children and their parents or guardians can easily exercise their data protection rights, such as access, correction, deletion, and objection to data processing.
4. **Anonymization and Pseudonymization**:
    - Where possible tokenise, anonymize or pseudonymize children's and adults' data to protect their identity and privacy.
5. **Data Retention Policies**:
    - Establish clear data retention policies, ensuring that personal data is not kept longer than necessary and is securely deleted when no longer needed.
6. **Third-Party Data Sharing**:
    - Limit the sharing of personal data with third parties and ensure that any third-party service providers comply with the same data protection standards.
7. **Behavioral Advertising Restrictions**:
    - Avoid using children's data for targeted advertising or profiling purposes

Design Measures

1. **Privacy by Design and Default**:
    - Embed privacy and data protection features into the design of digital platforms from the outset, ensuring that privacy settings are set to high by default.
2. **User-Friendly Interface**:
    - Design interfaces that are easy to navigate and understand, enabling children and parents to manage privacy settings and understand data practices effectively.
3. **Educational Content**:
    - Provide educational resources and materials to help children and parents understand online privacy, data protection, and safe internet practices.
4. **Regular Audits and Assessments**:
    - Conduct regular data protection impact assessments (DPIAs) to identify and mitigate risks related to the processing of children's data.
5. **Incident Response Plan**:
    - Develop and implement a comprehensive incident response plan to address data breaches promptly, including notifying affected parties and regulatory authorities as required.

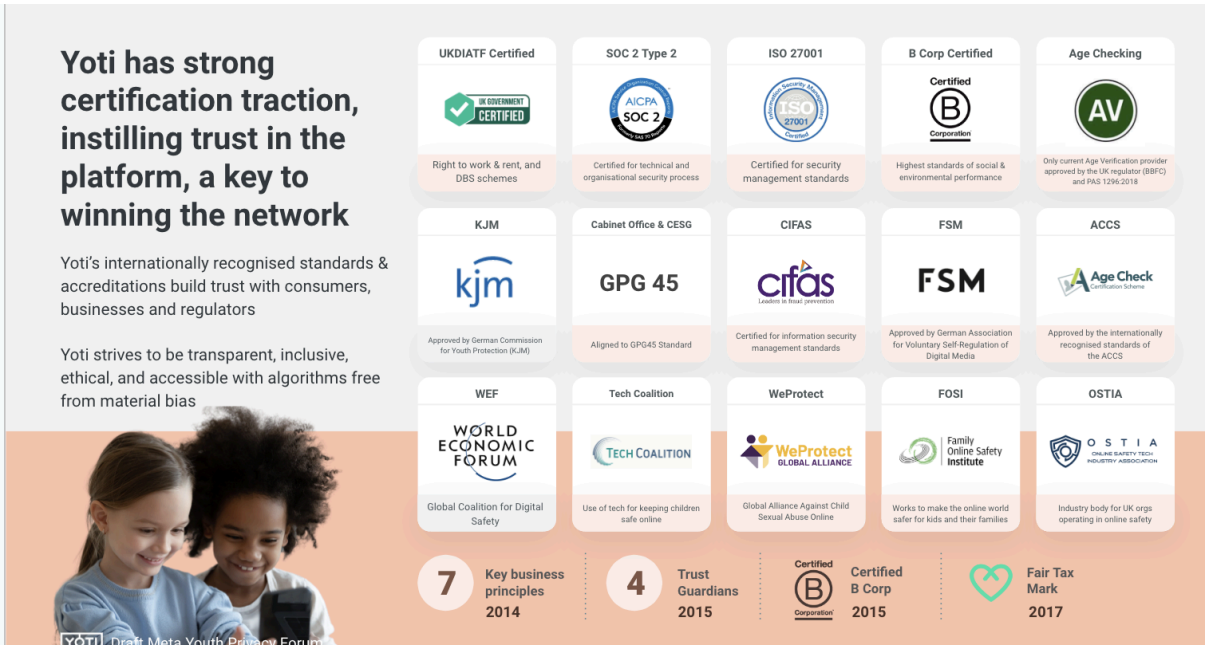
Monitoring and Compliance

- **Regular Monitoring**:

- Continuously monitor data processing activities to ensure compliance with data protection principles and promptly address any issues.

- **Training and Awareness**:
  - Provide regular training for employees on data protection principles, specifically focusing on the processing of children's data.
- **Engagement with Stakeholders**:
  - Engage with child protection organizations, regulators, and other stakeholders to stay updated on best practices and regulatory changes.

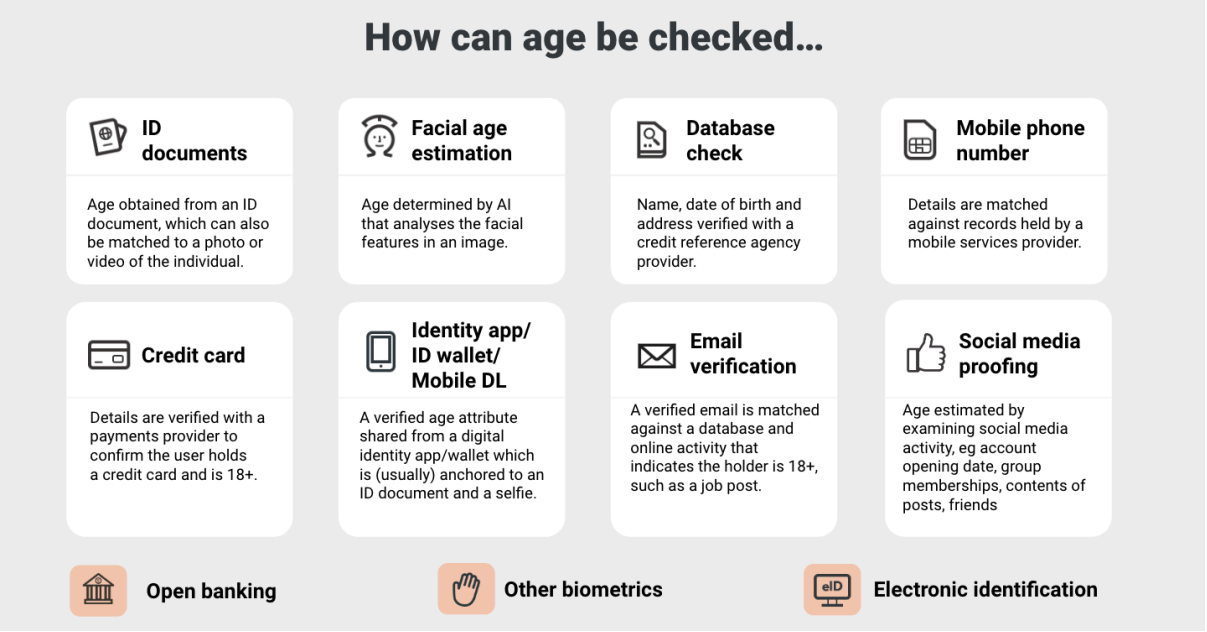
    We are happy to provide further detail on the organisations that we engage with as below:



2. Considering that the processing of personal data must be limited to that strictly necessary for the purpose for which it is intended, what are the good practices and techniques available and appropriate for verifying the age of users of digital platforms?

We would refer to the standards developed for age assurance - PAS 1296:2018[13], IEEE 2089.1 and ISO/27566[14] (CD) to detail good practise in terms of tokenised, data minimised age assurance, meeting privacy requirements.

Given the word limit, we provide here a chart here of techniques available; we are happy to provide detailed followup information on each approach, if that is of interest.



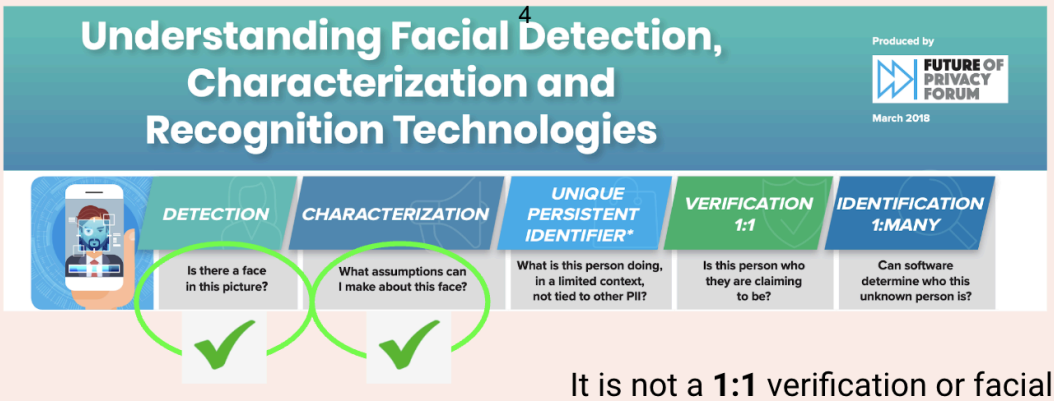
In terms of facial age estimation, it is key to understand that data is instantly deleted and that there is no unique recognition:.

[13] https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice?version=standard

[14] **https://www.iso27001security.com/html/27566.html**

AI Facial Age Estimation

Detects a face & then analyses it

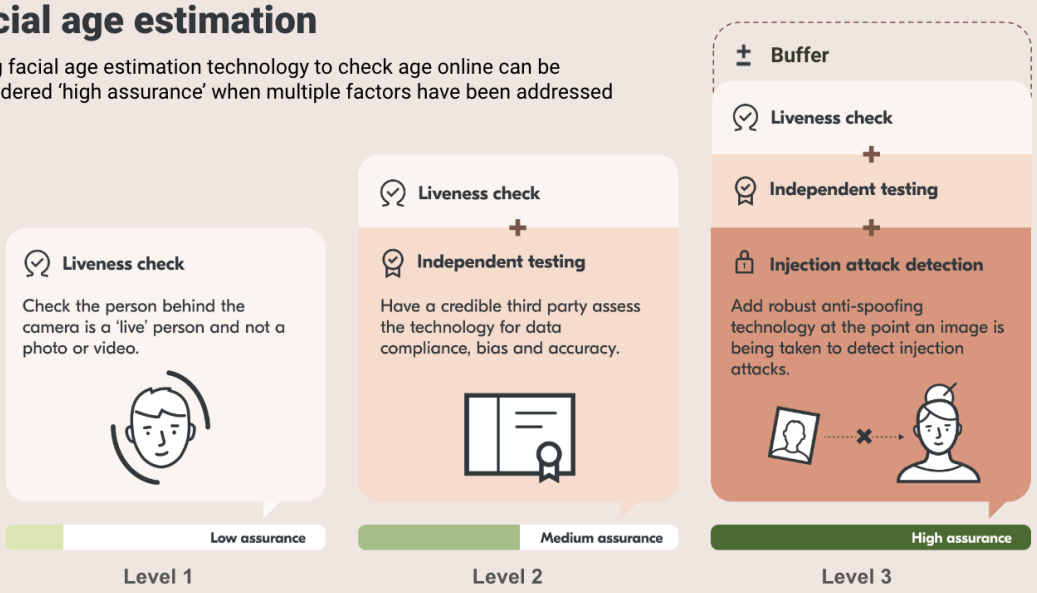


It is not a **1:1** verification or facial recognition or a **1: MANY** facial recognition

YOTI

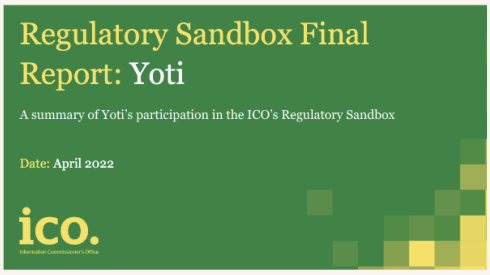
Facial age estimation

Using facial age estimation technology to check age online can be considered 'high assurance' when multiple factors have been addressed



Sandboxing with regulators is a useful tool.

ICO sandbox 2022 ahead of the Age Appropriate Design Code (AADC)

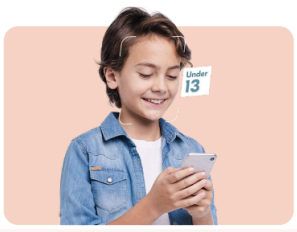


- Extended the data set from 6-70 to support the age bands in the AADC
- Co created explainer materials with young people, following Unicef guidelines

- *Yoti's age estimation tool has demonstrated that it is possible to*
- *use biometrics to make a decision about an individual or treat them differently* ***without using that biometric data for the purpose of uniquely identifying that person.***
- *Yoti's age estimation tool will* ***not result in the processing of special category data.****'*

Attitude research with users is key:[15]

Attitudes to Facial Age Estimation - Playverto Research findings

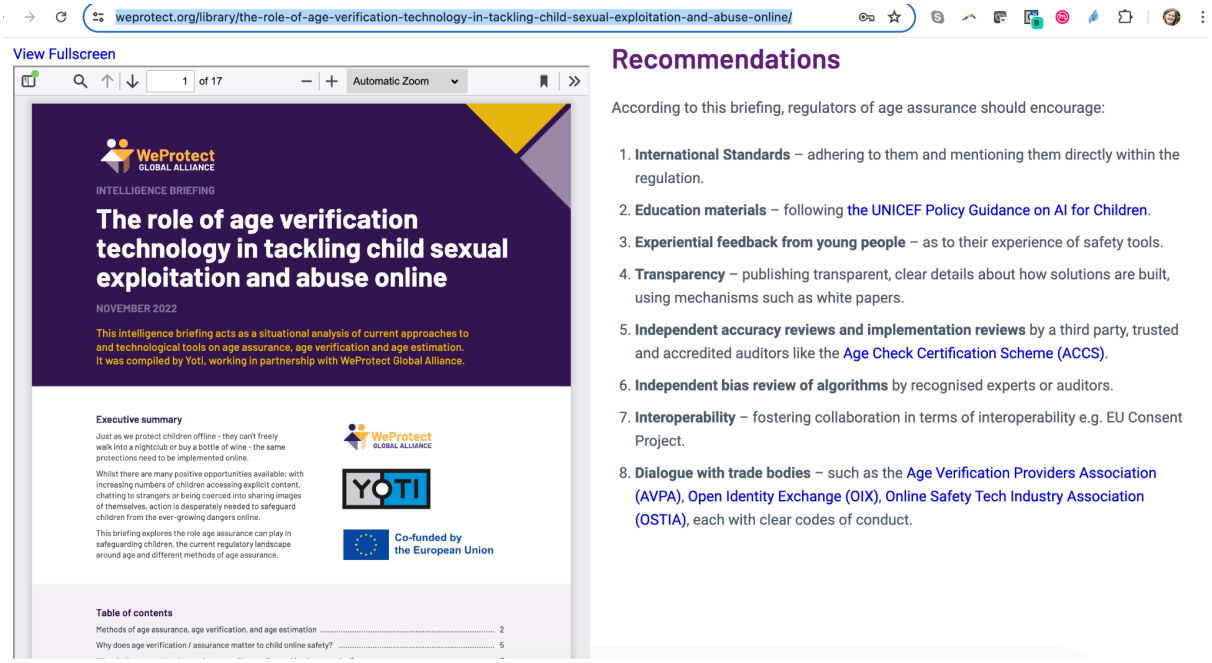


Results from children

- **50% were curious about how the technology estimates their age**
- **84.6% of children said they understand why websites check age**
- **67.5% understood what the selfie was for & how it would be used**
- **88.3% found the instructions to use easy to understand**
- **62% of children said they were either likely or very likely to use it again**

15 https://www.yoti.com/blog/play-verto-research-young-peoples-attitudes-towards-facial-age-estimation/

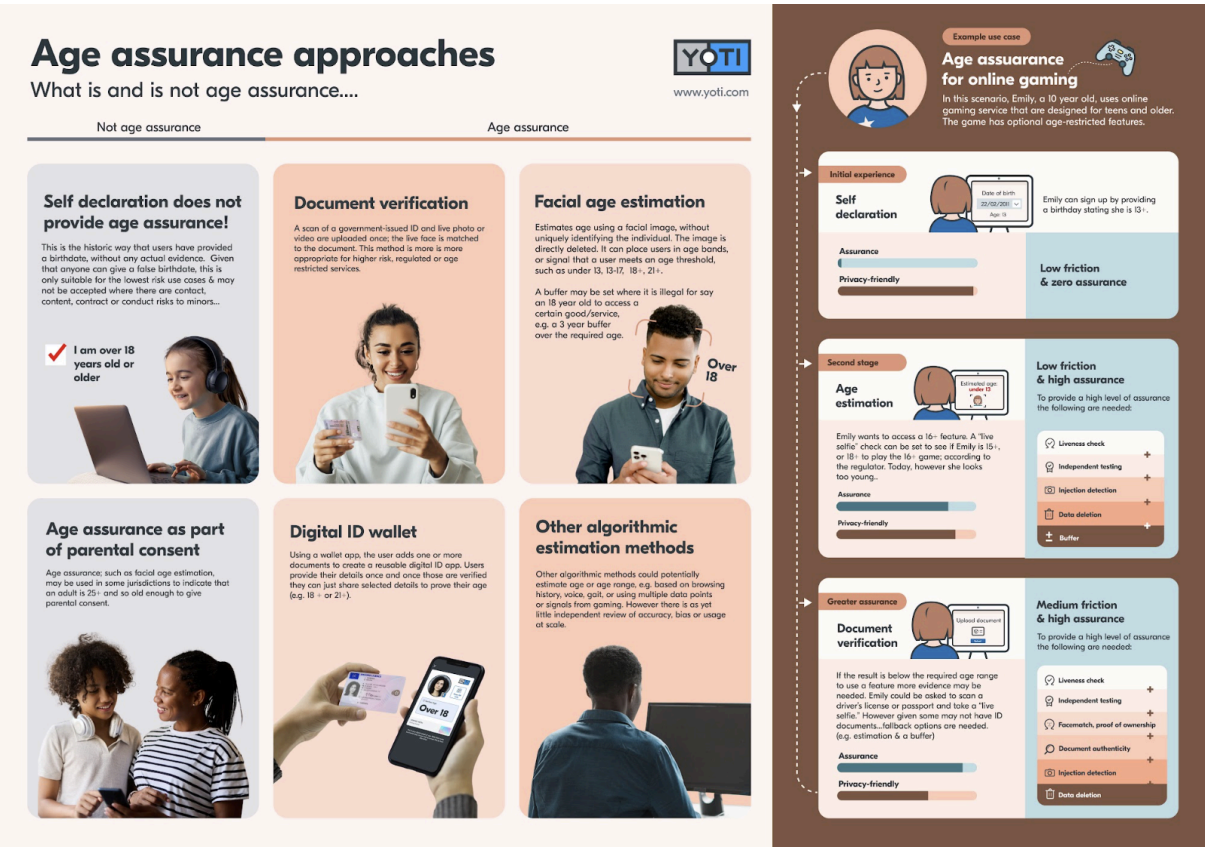
Working with respected global organisations, expert in child safety, see [joint explainer document published by WeProtect Global Alliance & Yoti]
16



Providing educational materials on the range of options available:

16

https://www.weprotect.org/library/the-role-of-age-verification-technology-in-tackling-child-sexual-exploitation-and-abuse-online/

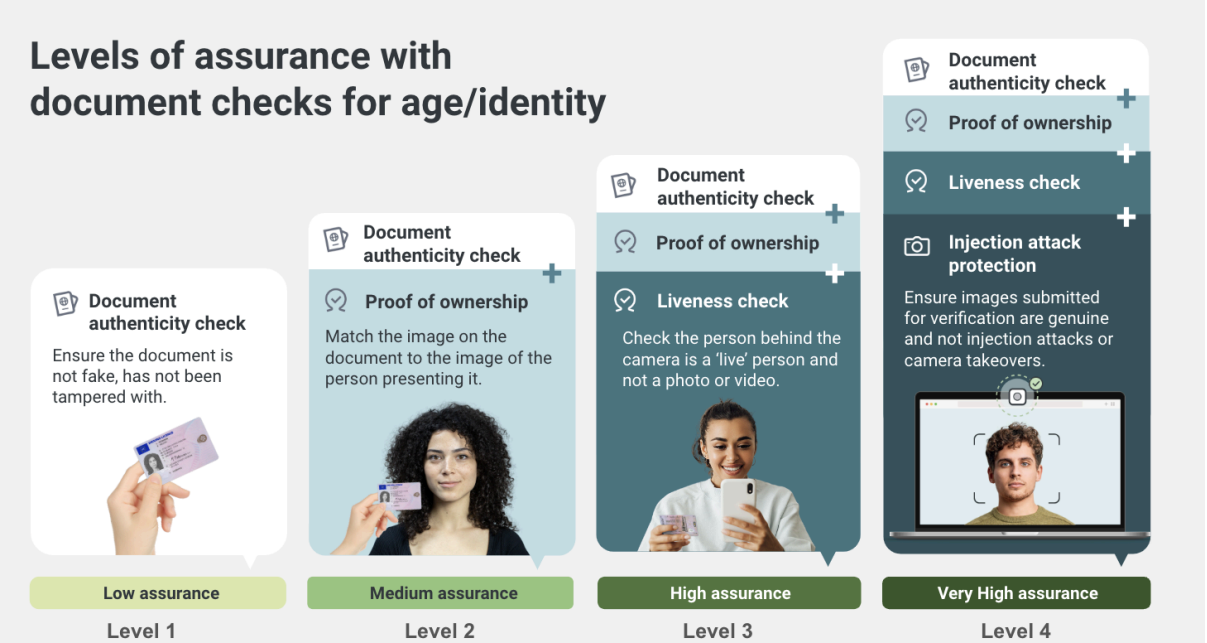


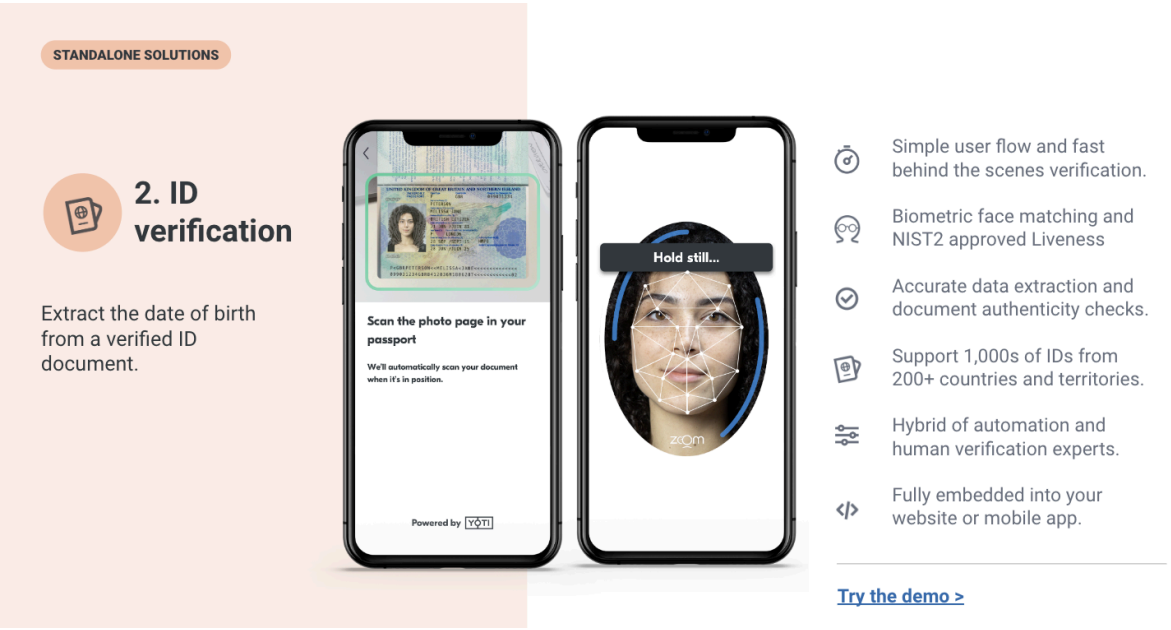
We have supported the minimum standards for age assurance[17] proposed by Baroness Kidron[18]

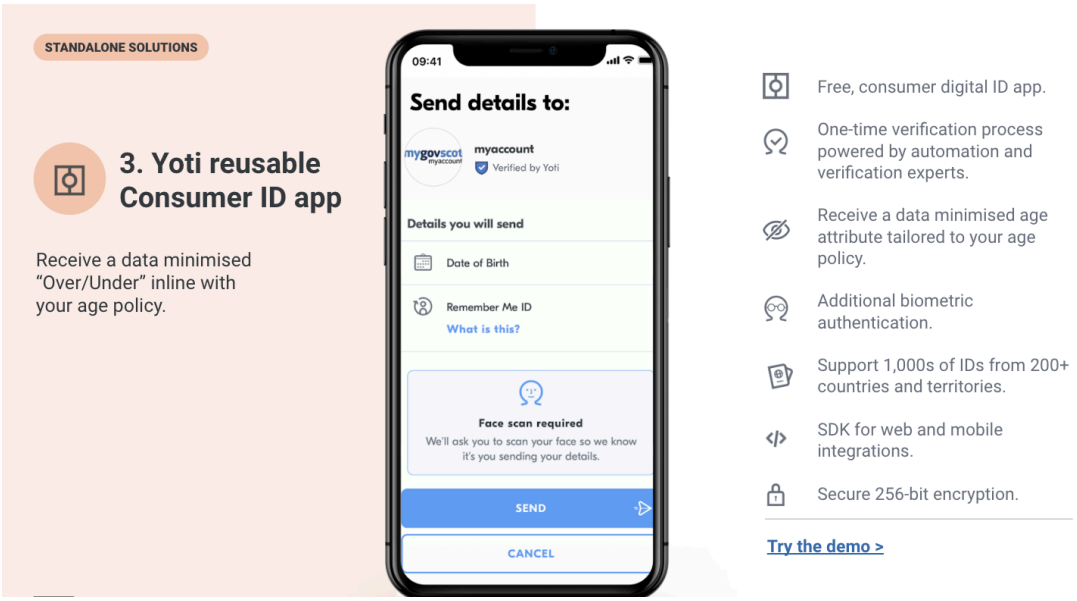
We undertake regular regulatory roundtables with interested stakeholders, from regulators, civil society, international organisations and academia.

We provide granular briefings and demonstrations to explain which approaches meet which levels of assurance.

[17] https://5rightsfoundation.com/in-action/letter-on-age-assurance-minimum-standards-bill.html
[18] https://lordslibrary.parliament.uk/age-assurance-minimum-standards-bill-hl/


Levels of assurance with document checks for age/identity
Document authenticity check
Ensure the document is not fake, has not been tampered with.
Low assurance
Level 1
Document authenticity check
Proof of ownership
Match the image on the document to the image of the person presenting it.
Medium assurance
Level 2
Document authenticity check
Proof of ownership
Liveness check
Check the person behind the camera is a 'live' person and not a photo or video.
High assurance
Level 3
Document authenticity check
Proof of ownership
Liveness check
Injection attack protection
Ensure images submitted for verification are genuine and not injection attacks or camera takeovers.
Very High assurance
Level 4


STANDALONE SOLUTIONS
2. ID verification
Extract the date of birth from a verified ID document.
Scan the photo page in your passport
We'll automatically scan your document when it's in position.
Powered by YOTI
Hold still...
Simple user flow and fast behind the scenes verification.
Biometric face matching and NIST2 approved Liveness
Accurate data extraction and document authenticity checks.
Support 1,000s of IDs from 200+ countries and territories.
Hybrid of automation and human verification experts.
Fully embedded into your website or mobile app.
Try the demo >



3. What specific limitations must be observed when collecting personal data from children and adolescents via digital platforms, considering the provisions of art. 14, § 4, of the LGPD and, among other aspects, the nature of the data collected and the purpose of the processing, such as the formation of behavioral profiles?

In each instance, only data minimised age attributes should be shared.
Age assurance approaches should meet clear data privacy and security requirements,, meeting recognised standards, eg PAS 1296:2018..

5. What good practices related to transparency and providing information in a simple, clear and accessible way can be observed by digital platforms regarding the processing of personal data of children and adolescents?

We are happy to provide the ICO Age Appropriate Design Code Audit[19] and ICO Sandbox Exit report from Yoti, link to our privacy notice for children and young adults.

19 https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/4019830/age-appropriate-design-code-yoti-app-audit-report-executive-summary-v1_0.pdf

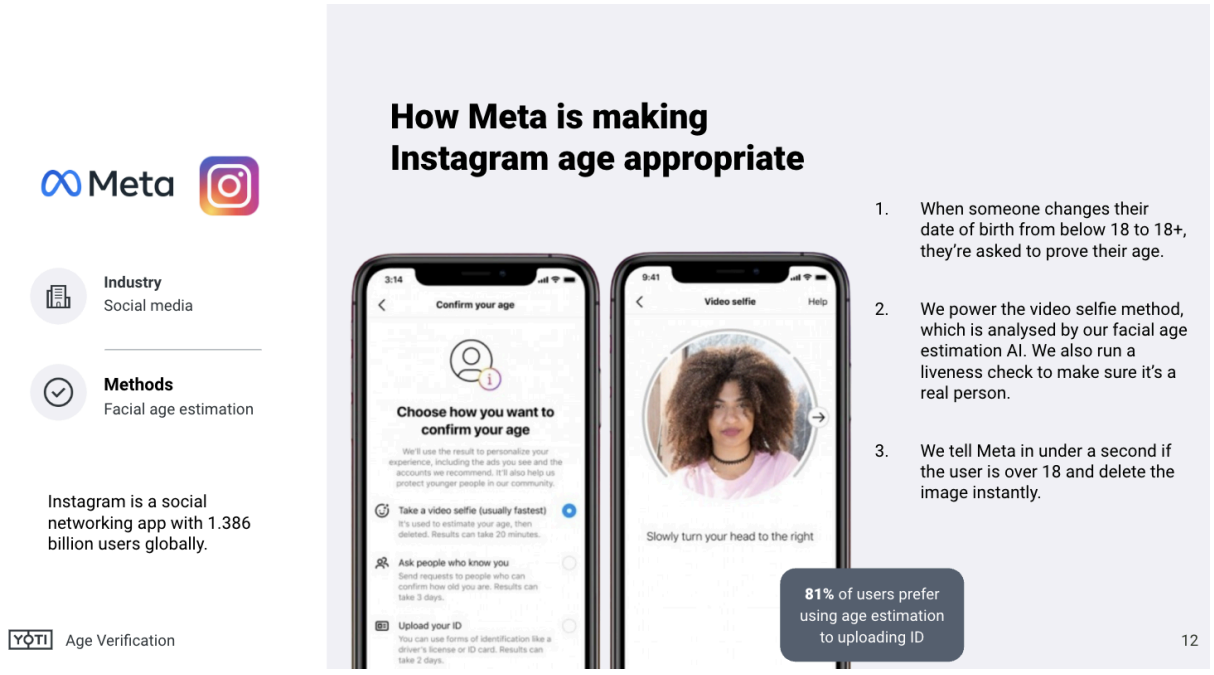
The 5Rights Foundation document Age Appropriate Presentation of Published Terms[20], provides useful suggestions on this topic.

> Simply deploying plain English and consulting with young people would be straightforward steps to improve the clarity of terms and statements. Examples of improved privacy statements which were developed in this way to meet the AADC include that of *'King'*, with its cartoon based privacy saga (*'Privacy Saga'*, available at https://tcs.king.com/privacy-saga/level1.html, as detailed in this blog ('King's Award-Winning *'Privacy Saga Makes Terms of Service Playful'*, available at https://newsroom.activisionblizzard.com/p/king-privacy-saga-awards).

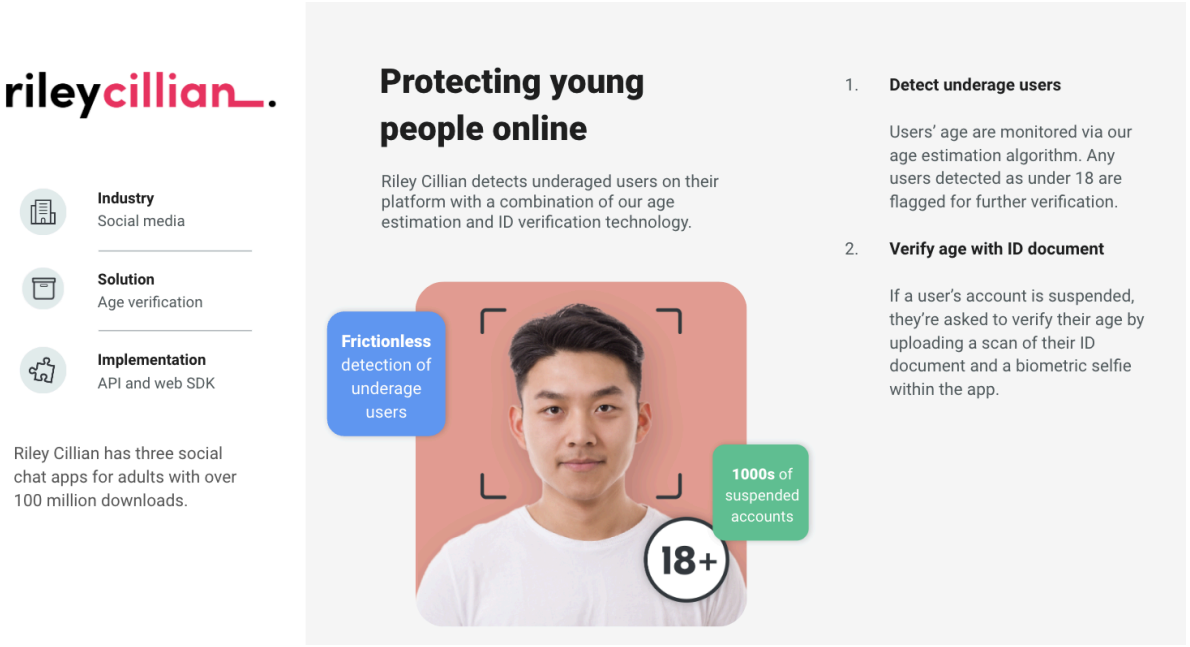
6. Are there other issues related to the processing of personal data of children and adolescents that deserve clarification or additional regulation?

It is useful to see some case studies:

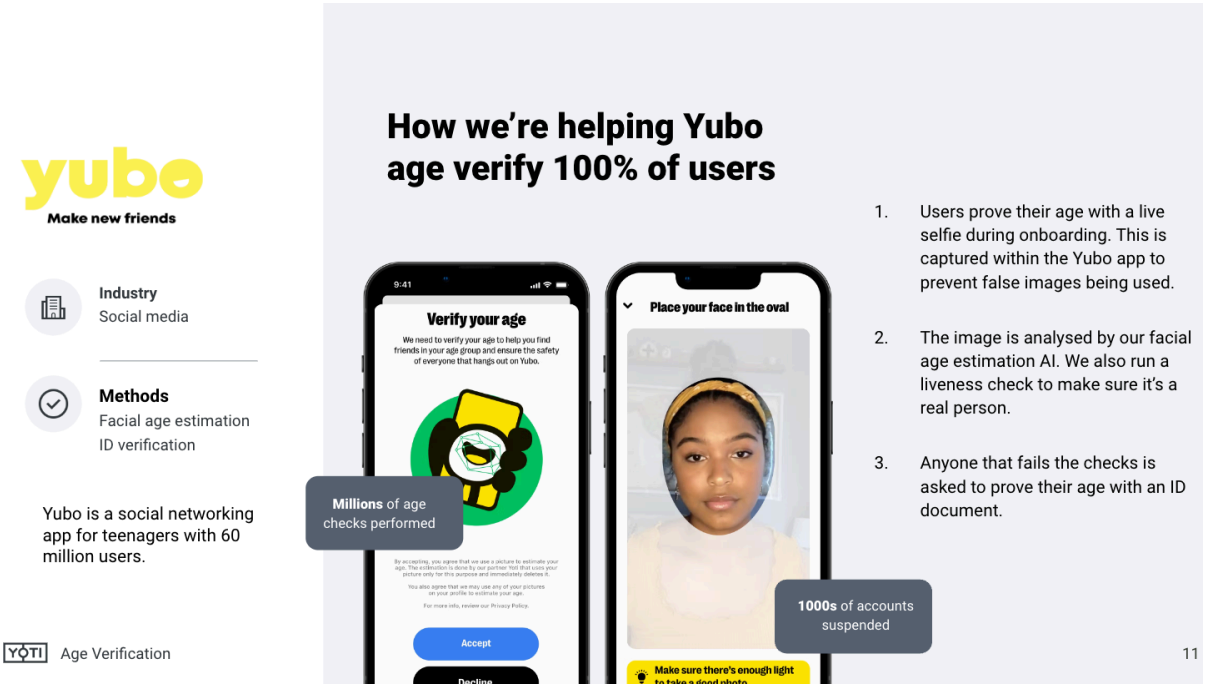
It is useful to see that age assurance can be used to enable an under 18 year old, to share a data minimised under 18 attribute.

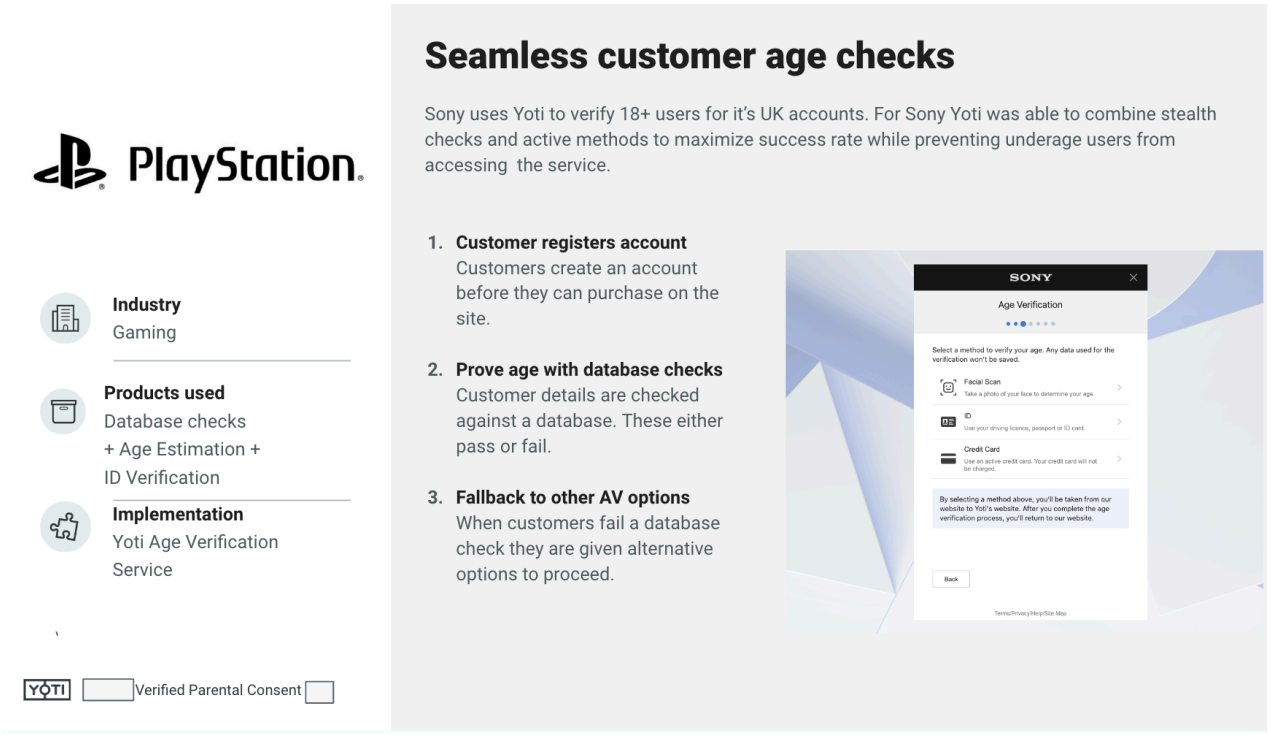


20



With Yubo, users are age assessed into 13-17 or 18 plus areas.





We are happy to answer any further questions.

Julie Dawson
Chief Regulatory & Policy Officer, Yoti

Appendix 1:

Option for parental consent using facial age estimation; example below from the partnership between KWS and Yoti

KWS
KIDS WEB SERVICES

Industry
Gaming

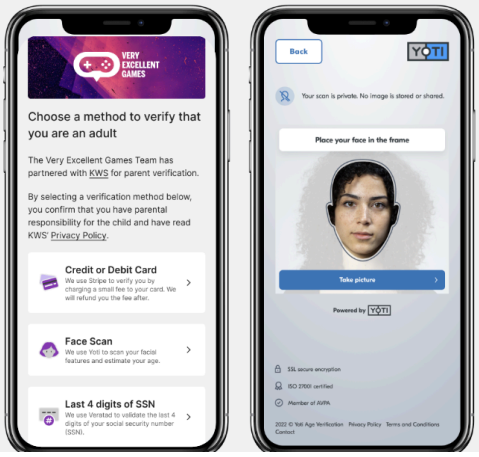
Products used
Age Estimation

Implementation
Yoti Age Verification Service

Seamless verified parental consent with age estimation checks

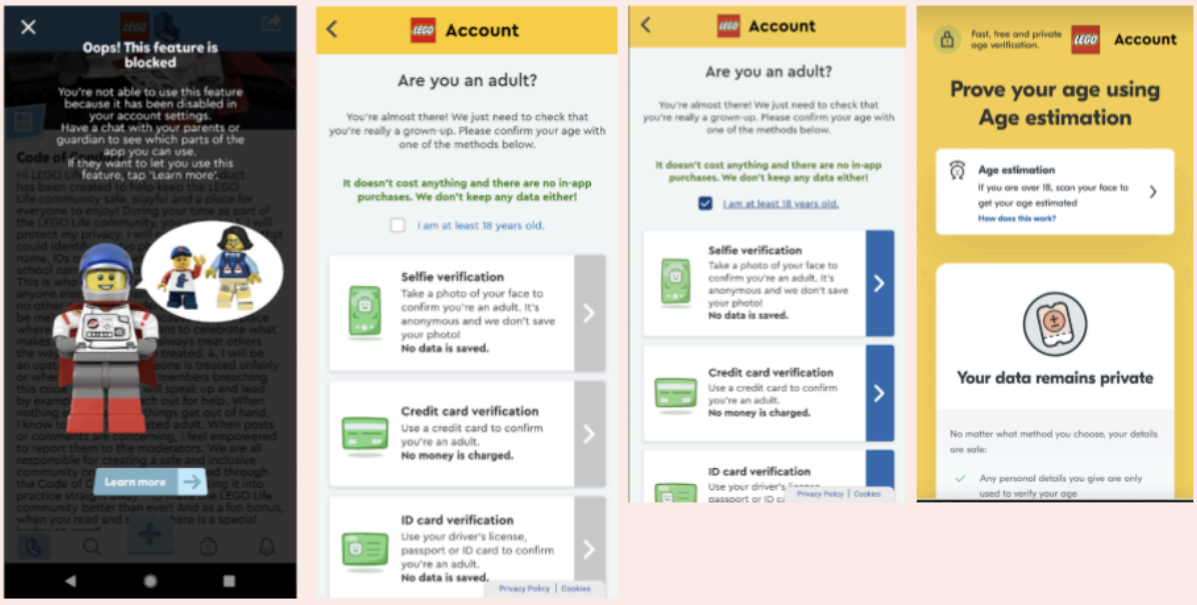
Yoti and KWS have implemented Yoti's Facial Age Estimation method for legally required parental consent in territories outside the U.S. and have—since 2022—delivered more than 5 million age estimations using this method.

1. **User detected to need Verified Parental Consent**
   User enters an 'under age of consent' date of birth at the age gate and enters parent email address.
2. **Parent required to prove age to ensure they are an adult**
   Parents sent an email and required to complete age verification.
3. **Parent selects age estimation and completes the process.**
   Age is estimated and parent moves on to consent options.

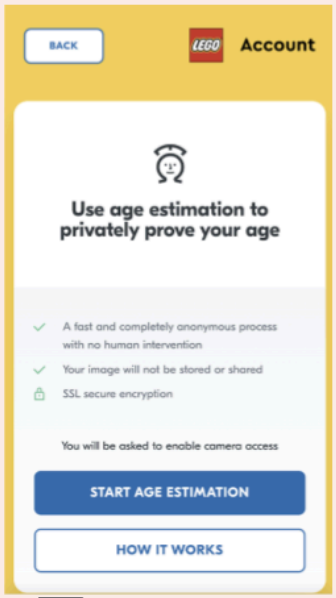


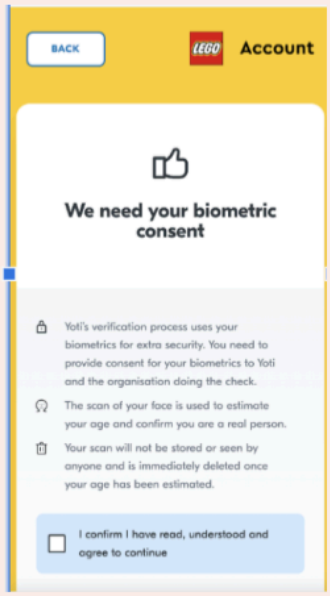
Parental Consent example flows using screen shots from live services e.g. Lego, Yubo

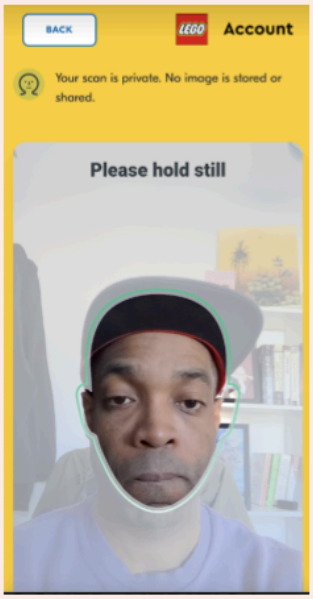
Age Verification for a digital world



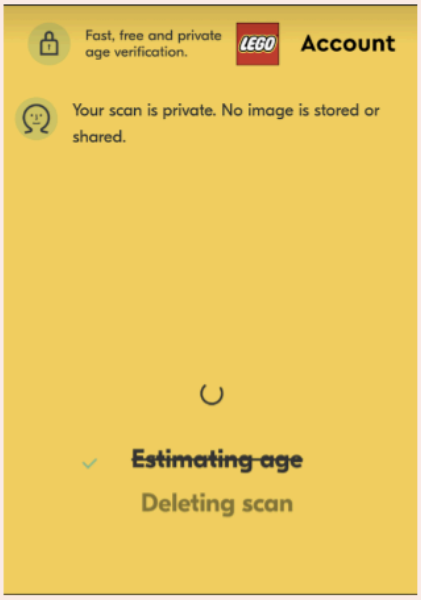
Age Verification for a digital world

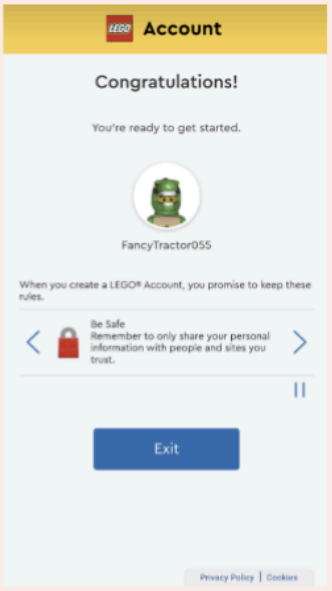


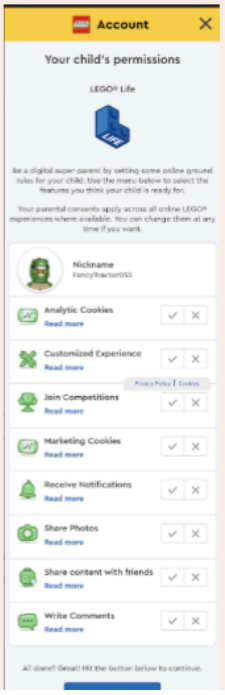




Age Verification for a digital world







Age Verification for a digital world

Key points re parental consent, using facial age estimation in the flow

- Facial age estimation can assess the age of the young person and the adult
- It is clear when young people are trying to game parental consent & this is successfully stopping that. Parents then want a range of options to verify that they are adults.
- Success rates of the age estimation circa 70-90%
- Inclusive method - does not rely on credit card or ID document ownership.
- Image deleted, independently audited
- Data minimisation - only an age range can be shared e.g. 18+ or 25+ or 30+
- Bias across gender and skintone are published transparently
- Crucially th etrainin data for the AI facial age esitmation is collected in accordance with GDPR, as described in the Yoti white paper, which is regularly updated

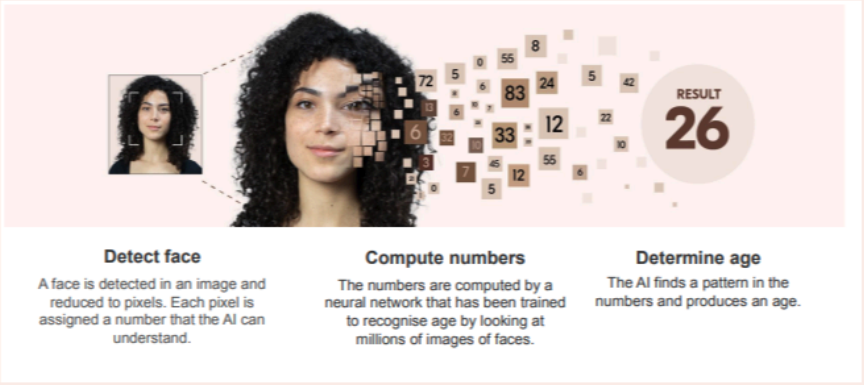
Mean Absolute Error by year

Age	Gender								All
	Female				Male				
	Skin Tone (Fitzpatrick Scale)								
	Type I & II	Type III & IV	Type V & VI	All	Type I & II	Type III & IV	Type V & VI	All	
	MAE	MAE	MAE	Average MAE	MAE	MAE	MAE	Average MAE	Average MAE
6	1.13	1.73	1.55	1.47	1.47	2.06	1.68	1.74	1.60
7	1.40	1.41	1.32	1.38	1.05	1.33	1.85	1.41	1.39
8	1.58	1.14	1.58	1.44	1.51	1.75	1.21	1.49	1.46
9	1.43	1.32	1.40	1.38	1.62	1.10	1.25	1.33	1.35
10	1.16	1.11	1.63	1.30	0.99	1.00	1.00	1.00	1.15
11	0.79	1.16	2.12	1.36	0.87	0.84	1.06	0.92	1.14
12	1.71	1.76	1.50	1.65	1.26	1.30	1.09	1.22	1.44
13	2.20	2.85	2.65	2.57	1.83	1.81	2.16	1.93	2.25
14	1.62	2.14	2.69	2.15	1.46	1.84	2.23	1.84	2.00
15	1.20	1.56	1.97	1.58	1.06	1.34	1.71	1.37	1.47
16	0.93	1.14	1.34	1.13	0.82	1.17	1.20	1.07	1.10
17	1.08	0.91	0.88	0.96	0.92	1.12	0.91	0.98	0.97
18	1.44	1.18	0.88	1.17	1.15	1.42	1.26	1.28	1.22

Age Verification for a digital world

15

How age estimation works



Detect face
A face is detected in an image and reduced to pixels. Each pixel is assigned a number that the AI can understand.

Compute numbers
The numbers are computed by a neural network that has been trained to recognise age by looking at millions of images of faces.

Determine age
The AI finds a pattern in the numbers and produces an age.

yubo

Industry
Social media

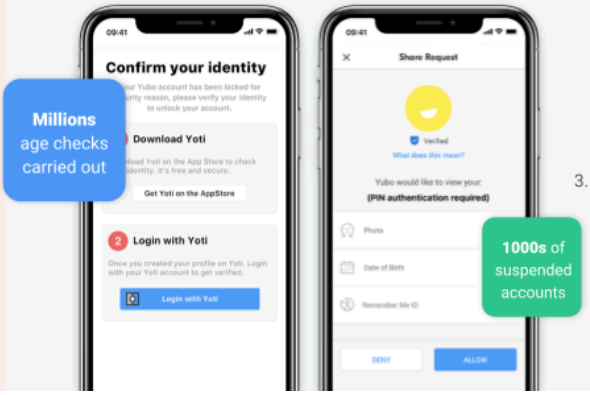
Solution
Age verification

Implementation
API and Digital ID

Yubo is a live streaming app for teenagers with over 50 million users globally.

Protecting young people online

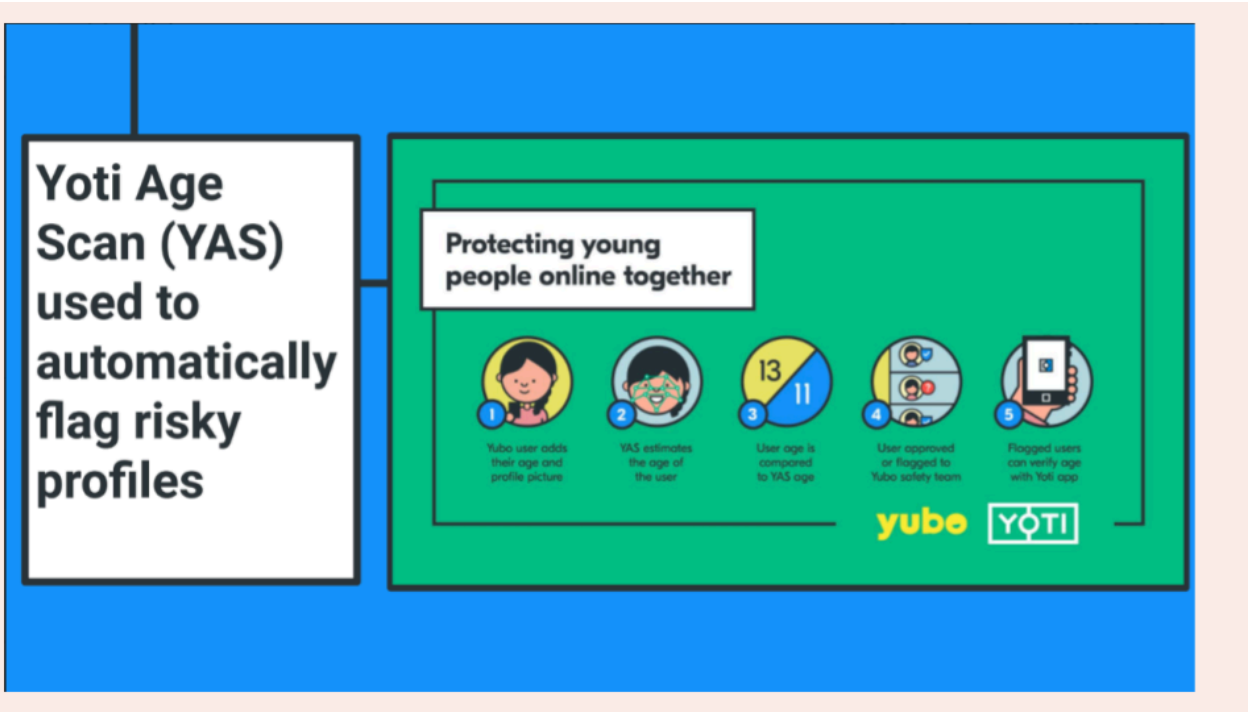
Yubo uses our age estimation technology and digital ID app to age gate it's different communities for 13-17 year olds and 18+.

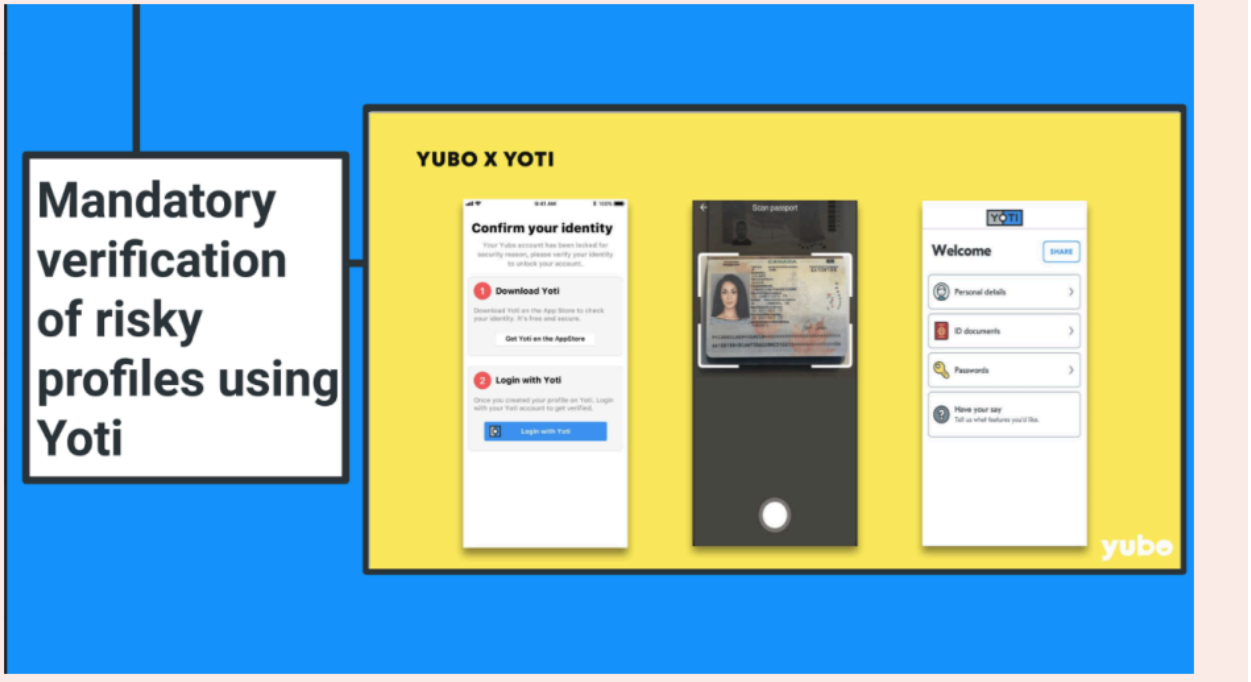


1. **Detect underage users** Yubo analyses users' age with our age estimation algorithm. Potential underage accounts are flagged to Yubo's moderation team.

2. **Prove age with Yoti** If a user's account is suspended, they're asked to verify their identity via Yoti. This involves downloading the free Yoti app and uploading an ID document and biometric selfie, and sharing their verified age with Yubo.

3. **Elective age verification** Users can also choose to voluntarily verify their picture and date of birth via the Yoti app to gain a verified tick on their profile.


Yoti Age Scan (YAS) used to automatically flag risky profiles
Protecting young people online together
13
11
Yubo user adds their age and profile picture
YAS estimates the age of the user
User age is compared to YAS age
User approved or flagged to Yubo safety team
Flagged users can verify age with Yoti app
yubo
YOTI


Mandatory verification of risky profiles using Yoti
YUBO X YOTI
Confirm your identity
Download Yoti
Login with Yoti
Welcome
Personal details
ID documents
Passwords
yubo

Appendix 2: LEGO application for Parental Consent Method to the Federal Trade Commission (FTC), Project No. P23540

August 21, 2023

VIA ELECTRONIC FILING

Mrs. April Tabor Secretary Federal Trade Commission Office of the Secretary 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B) Washington, DC 20580

RE: Application for Parental Consent Method, Project No. P23540

Dear Secretary Tabor:

The LEGO Group respectfully submits these written comments to the public consultation issued by the Federal Trade Commission (FTC) on the application of the 'ESRB group' (including Yoti and SuperAwesome) for approval of a parental consent method. Given the current pace of development in technology and the changing relationship of children and parents to the internet, it is appropriate to review new technical methods to obtain verified parental consent (VPC) and we support the continuous efforts of the FTC to review and potentially approve new mechanisms. We consider that the ESRB group's proposal offers a new, proportionate, accurate, and privacy-preserving VPC solution that improves the ability of children to access appropriate online services, allowing them to play, grow, and thrive online. For that reason, we support the application.

At the LEGO Group, the rights, safety, and wellbeing of the millions of children we engage with every day around the world are of paramount importance. Safety and privacy sit firmly alongside our six core values - imagination, creativity, fun, quality, learning, and caring - and are fundamental components of every interaction we have. This is as true online as it is with our bricks in the physical world. It is our long-standing record of physical and digital safety and the quality of our play experiences and materials that have over the years solidified a deep trust with consumers and a strong global reputation.

When we look to the future, we see digital play as being of increasing importance to enable children's agency, education, and the development of 21st-century skills like creativity, problem-solving, and critical thinking. Accordingly, it is critical that both regulation and technology facilitate children's access to safe, privacy-preserving digital play. We believe methods of VPC that reduce the amount of personal information processed, achieve a high level of accuracy and assurance, minimize barriers to adoption, and ultimately make it easier for parents to give genuine permission for children to participate in safe online environments are the gold standard.

Unfortunately, very few available solutions have met this standard. After meaningful investments to implement a more functional VPC process, including improving how we communicate with parents and caregivers on the importance of VPC as well as limiting the disruption in the user experience, we have been able to improve security and reduce the number of parents that do not complete the process. However, we still see that the lack of user familiarity and lack of willingness to go through VPC is a serious barrier to entry that limits age and content-appropriate play experiences from reaching children and, as a result, pushes children, parents, and caregivers towards lower-barrier play experiences that are not necessarily designed for the child's age. Accordingly, we believe that there is an urgent need

to find less disruptive, more cost-effective, and scalable solutions that do not interrupt the engagement experience or deter viable access.

We consider that the ESRB group's proposed method does indeed offer a robust VPC solution that meets the requirements laid out in 16 CFR 312.5(b)(1). In our assessment of VPC solutions, we have concluded facial age estimation to be a robust method which, given technical means available, is proficient at ensuring consent is provided by a child's parent or guardian. This is evidenced by (1) the method's high levels of accuracy (including marginal false positive rates of 0.03%), (2) a clear record of effectively distinguishing between users who are 25+ and those that are younger, and (3) the difficulty for children to manipulate the system (i.e. by implementing anti-spoofing measures to ensure there is a live human face in the frame). We consider that this method works particularly well in ecosystems where any user estimated to be under 25 is rerouted to use other VPC methods, allowing the 'buffer' age to remain high and further reducing the chance of manipulation or false positives.

We believe the overall efficacy of facial age estimation is particularly acute when compared with other popular solutions, including those currently approved under 312.5(b)(1). It offers a relatively quick, understandable, and low-friction process when compared to making a phone or video call, signing, and scanning a form or even facial recognition with government ID. This ease of use is an important feature; the Future of Privacy Forum has noted how burdensome and time-consuming consent methods can lead to significant rates of user drop-off, creating a risk that children and parents will turn to experiences with lower obstacles that are not necessarily designed for the children's age. This finding is consistent with our own experience. The LEGO Group is a strong advocate of protections for children, but we acknowledge the persistent risk that the most appropriate and value-adding spaces in the digital environment become undesirable to children because the barriers to access are too high.

From the LEGO Group's perspective, the privacy and security benefits for users offered by this solution (as built by Yoti) are particularly important. Trust in the online world is low, largely due to expectations that firms will collect and harvest personal information for their own benefit. As we understand it, the training data for the model is restricted to facial images associated with a person's age - therefore the method when applied is limited to estimating age rather than identifying individuals. Further, as the only data captured from a user is their facial images and not any identifying documents, the personal information needed to establish consent for those that pass verification is minimal. The information that is collected is securely transmitted using robust encryption standards and, upon reaching the provider's backend server, is rapidly and permanently deleted after processing. We were encouraged to see the UK Information Commissioner's Office note that Yoti's specific solution did not involve the processing of sensitive personal data (i.e., health information) and their wider conclusion that facial age analysis has the 'potential to be more privacy-friendly if data minimization and purpose limitation are applied rigorously' - which we understand they are. If other facial age estimation systems were to offer the same level of privacy protection, we consider that these solutions would offer our users a higher degree of trust than VPC methods such as document verification or facial recognition.

The LEGO Group believes that play is for everyone, no matter where you come from, what you look like, or how you identify. It is critical for us to know that any process we implement, technical or otherwise, does not discriminate on the basis of race or gender. The risk of bias in facial recognition and similar technologies is well documented and underscores the need for algorithmic models to be deployed responsibly. It is therefore encouraging to see that facial age estimation systems can achieve high levels of fairness if trained on diverse data sets that are representative of people across the world. Notably, we believe that this method can result in more equitable outcomes than VPC based on credit cards or government identification which may exclude children with parents or caregivers that are under- or

un-banked, as well as undocumented. Children should not be left out of the digital ecosystem and their right to play, learn, and develop online because of such technical barriers.

The LEGO Group's mission is to inspire and develop the builders of tomorrow, enabling, and empowering children through playful experiences to learn, develop, and maximize their creative potential. From our perspective, it is therefore essential that parents are given the means to allow their children to access the digital environment safely and confidently. We believe the approval of new but proven methods of privacy-preserving VPC will play a key role in helping children thrive and build online.

Thank you for the opportunity to share some of our thoughts and experiences in this space. We welcome the opportunity to engage more closely in the future and welcome any questions you or the agency may have regarding our comments. Please contact me at if you have any questions or would like additional information.

Respectfully,

Carolina Giuga Sr. Director, Government & Public Affairs The LEGO Group

[6] See discussion of Yoti's improvements in age and skin tone recognition.

[7] The Future of Privacy Forum estimates that 8.4million households in the United States does not have any account at a bank or other financial institution.

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before the

National Data Protection Authority

Brasília, Brazil

In the Matter of: Making Subsidies: Processing of Personal Data of Children and Adolescents	)	Process No. 00261.004146/2024-39

July 17, 2024

CONTENTS

Comments of ITIF 1
Introduction and Summary 2
Internet Games and Applications 2
Conclusion 4

INTRODUCTION AND SUMMARY

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Brazilian National Data Protection Authority's (ANPD) request for public comment concerning "Making Subsidies: Processing of Personal Data of Children and Adolescents."[1] ITIF is a nonprofit, non-partisan public policy think tank based in Washington, D.C., committed to articulating and advancing pro-productivity, pro-innovation, and pro-technology public policy agendas around the world that spur growth, prosperity, and progress.

Age verification, parental controls, and transparency have become hot button issues within the global debate surrounding children's online safety and privacy. Improved systems for age verification would keep more children away from inappropriate content, but the different methods of verifying users' ages online pose varying risks to user privacy and could restrict some adult users from age-gated digital platforms. Greater parental control over children's online behavior would allow for a more individualized approach to children's protection, but this requires parents to be informed and involved in their children's online safety and privacy. Finally, greater transparency surrounding digital platforms' safeguards for children and the potential risks children may face online will not solve these issues, but it would better inform parents and policymakers, leading to better decision-making at every level.

INTERNET GAMES AND APPLICATIONS

2. Considering that the processing of personal data must be limited to that strictly necessary for the purpose for which it is intended, what are the good practices and techniques available and appropriate for verifying the age of users of digital platforms?

There are multiple different ways digital platforms can verify users' ages, and each of these methods comes with different strengths and weaknesses. Some are more accurate but more invasive, whereas others are less invasive but also less accurate.

First, many digital platforms already require users to either check a box indicating they are over a certain age or input their date of birth to confirm they are over a certain age. This form of self-verification is the least invasive, because it only requires users to disclose, at most, one piece of personal information: their date of birth. Because many people share the same birthday, this piece of information cannot uniquely identify an

[1] "Making Subsidies: Processing of Personal Data of Children and Adolescents," National Data Protection Authority, June 18, 2024, https://www.gov.br/participamaisbrasil/tscriancaeadolescente.

individual. However, this method is also the least reliable, as underage users can and often do lie about their age in order to gain access to certain digital platforms.[2]

On the other end of the spectrum when it comes to accuracy and invasiveness is the ID check. This form of age verification is common in physical spaces, where customers must provide a valid government-issued ID in order to prove they are above the minimum age required to enter an age-gated space or purchase an age-gated product. It is also highly accurate, as government-issued IDs are more difficult to falsify than checking a box or entering one's date of birth. However, because most in-person ID checks do not involve making a copy of each customer's ID, these encounters pose lower privacy risks than online ID checks, where a digital platform may store the information from users' IDs. Additionally, as many as three million Brazilians do not have necessary identity documents, complicating the process of online ID checks for those individuals.[3]

Digital forms of government-issued identification could solve some of the privacy concerns associated with ID checks for age verification, as well as make the process more efficient. Currently, online ID checks typically require users to upload a photo of their physical ID as well as sometimes additional steps to prove the ID belongs to them, such as uploading a current image of their face to compare to the photograph on the ID. If designed right, digital IDs would streamline this process and allow users to only share necessary information. For example, individuals trying to access an age-restricted digital platform could verify that they are over a certain age without providing their exact date of birth, let alone all the other information a physical ID would reveal. Brazil's digital ID system has 153 million registered users, and while these IDs currently allow users to prove their identity to access government services, the system could potentially allow for easier and more privacy-protective age verification in the future.[4]

Finally, in between self-verification and ID checks, there is a third potential method of age verification using artificial intelligence (AI) to estimate users' ages from an image of their face. Combined with privacy protections requiring online services to delete users' images after the age estimation process is complete, this would minimize the amount of personal information users have to give up in order to verify their age. Of course, age estimation technology is not perfectly accurate and likely never will be, but it is constantly improving.

4. What mechanisms and good practices can be adopted to increase the control of parents and guardians over the processing of personal data of children and adolescents in the digital environment?

In order to increase parental control, and as an alternative to age verification, device operating systems could create a "trustworthy child flag" for user accounts that signals to apps and websites that a user is underage and apps and websites that serve age-restricted content could check for this signal from their users and block underage users from this content. Rather than using ID checks to determine whether to activate this child flag option, this would be an opt-in process built in to existing parental controls on devices. Parents could activate

[2] Yonder Consulting, "Children's Online User Ages Quantitative Research Study" (Ofcom, October 2022), https://www.ofcom.org.uk/__data/assets/pdf_file/0015/245004/children-user-ages-chart-pack.pdf.

[3] Juliana Andrade, "CNJ records 100,000 services during Civil Registry Week," *Agência Brasil*, https://agenciabrasil.ebc.com.br/justica/noticia/2023-05/cnj-contabiliza-100-mil-atendimentos-na-semana-de-registro-civil.

[4] "Gov.br Digital ID," Global Digital Public Infrastructure Repository, accessed July 10, 2024, https://www.dpi.global/globaldpi/gbr_digital_id.

or disable the child flag option depending on their own values and the maturity of their children. Additionally, devices could default to certain parental controls recommended for children.[5]

Because this approach does not require anyone to disclose or verify their identity, it does not create privacy risks by forcing users to share their government IDs or allowing online services to link their online activity to their offline identities. It is also a low-impact approach, allowing adults to continue using the Internet as they do today. Similarly, the vast majority of websites and apps that are meant for the general public would not have to take any action. Third, it would be entirely voluntary for users. Parents who want to control what their children see on the Internet could choose to use this feature and other parents could choose not to.

5. What good practices related to transparency and the provision of information in a simple, clear, and accessible manner can be observed by digital platforms when processing personal data of children and adolescents?

Requiring digital platforms to provide certain information would enable children and parents to make better-informed safety and privacy decisions. With the necessary information at their fingertips, parents could more effectively tailor their child's online safety and privacy protections to their parenting style and the child's developmental needs, allowing for an individualized approach to children's online safety and privacy instead of a one-size-fits-all mandate. Information that would be useful to children and their parents includes information about a digital platform's safety and privacy safeguards, potential risks facing children on the platform, personalized recommendation systems the platform uses, and advertising on the platform that targets children.

CONCLUSION

A combination of privacy-protective age verification systems utilizing digital forms of identification and AI, parental controls that are readily available and easy to use, and greater transparency from digital platforms would increase children's safety and privacy, encourage innovation in improved safety and privacy controls, and better inform policymakers and parents on next steps to protect children.

Thank you for your consideration.

Ashley Johnson
Senior Policy Manager

[5] Ash Johnson, "How to Address Children's Online Safety in the United States" (ITIF, June 2024), https://itif.org/publications/2024/06/03/how-to-address-childrens-online-safety-in-united-states/.

São Paulo, 16 de julho de 2024.

À
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)
Coordenação-Geral de Normatização
A/C: Rodrigo Santana dos Santos
normatizacao@anpd.gov.br

Ref.: Tomada de Subsídios ANPD – Tratamento de dados pessoais de crianças e adolescentes

Prezados/as,

A **ASSOCIAÇÃO BRASILEIRA DE INTERNET – ABRANET,** pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Rua MMDC, nº 450 cj. 304, São Paulo/SP, é uma entidade de classe sem fins lucrativos, fundada em 1996, para representar empresas pioneiras e inovadoras em serviços nativos da Internet, especialmente pequenos provedores de acesso à Internet, provedores de conteúdo, plataformas, fintechs, paytechs e data centers. De abrangência nacional, conta com mais de 400 (quatrocentas) associadas, tendo atuado como uma das principais fontes técnicas do setor junto ao Poder Público, sociedade civil e mercado, em apoio à proteção de dados, empreendedorismo, inovação, concorrência, simplicidade e democratização do acesso a produtos e serviços digitais. Trata-se, portanto, de uma das principais entidades envolvendo agentes de tratamento atuantes na internet no Brasil. Diante disso, enquanto representantes de uma ampla gama de controladores e operadores, a ABRANET possui profundo interesse em contribuir com uma regulação adequada sobre o tratamento de dados pessoais de crianças e adolescentes.

Alguns exemplos ilustram a ampla atuação da ABRANET na atuação junto à ANPD, como: (i) participação na construção da LGPD; (ii) apoio à criação da Autoridade Nacional de Proteção de Dados; (iii) envio de contribuições para as consultas públicas sobre incidentes de segurança com dados pessoais, legítimo interesse, regulamento para atuação do Encarregado, sandbox regulatório de inteligência artificial e proteção de dados pessoais e sobre anonimização e pseudonimização, (iv) envio de contribuições para as Tomadas de Subsídios sobre direitos dos titulares e sobre tratamento de dados pessoais de alto risco e em larga escala.

No âmbito da presente Tomada de Subsídios, as principais considerações levantadas pela ABRANET são:

a) A relevância de a **ANPD balizar o uso do princípio do legítimo interesse por meio de exemplos sobre sua aplicação em casos concretos**, na toada já prevista nos guias orientativos da Autoridade. Antecipar situações e descrever os motivos pelos quais se entende que em uma determinada situação a aplicação do princípio é adequada e em outra, não, é de suma importância para definir, por exemplo, **em quais cenários o princípio deve ser sopesado com outros previstos na LGPD**;

b) A necessidade de esclarecimento sobre a **forma de obtenção do consentimento ser variável a depender da faixa etária do titular dos dados pessoais**, levando em conta, principalmente, a crescente autonomia de crianças e adolescentes. Nesse sentido, a ABRANET entende que uma interpretação restritiva que considera o consentimento como a única opção viável pode resultar em limitações excessivas, mesmo quando o tratamento dos dados está em conformidade com o melhor interesse da criança;

c) O fato de a legislação brasileira já conferir aos adolescentes autonomia em cenários da vida civil consideravelmente complexos, devendo a ANPD, portanto, levar em conta que **adolescentes também poderiam ter a capacidade de fornecer consentimento para o tratamento de seus dados pessoais em alguns contextos**;

d) A importância de a ANPD fornecer exemplos ou parâmetros que orientem os agentes de tratamento sobre **medidas de segurança consideradas adequadas em seus respectivos setores de atuação**, sem violar os demais princípios da LGPD -- em particular no que diz respeito ao setor financeiro e de pagamentos.

e) A ausência de manifestação da Autoridade sobre **a retenção de dados pessoais de titulares após atingirem a maioridade**. A ABRANET entende que um direcionamento sobre o assunto é essencial para garantir segurança jurídica aos agentes de tratamento e, ao mesmo tempo, a conformidade com a LGPD, assegurando que os direitos dos indivíduos sejam plenamente respeitados à medida que transitam da infância e adolescência para a idade adulta.

A ABRANET agradece e parabeniza a Autoridade pela oportunidade de compartilhar suas considerações para a Tomada de Subsídios de forma construtiva para o aprimoramento

das políticas relacionadas à proteção de dados no Brasil. Abaixo seguem as contribuições específicas da Associação.

Sendo o que cumpria para o momento, a ABRANET coloca-se à disposição da ANPD para qualquer colaboração que esta venha a julgar necessária e apresenta seus protestos de elevada estima e consideração.

Atenciosamente,

ASSOCIAÇÃO BRASILEIRA DE INTERNET – ABRANET

Tomada de Subsídios ANPD – Tratamento de Dados Pessoais de Crianças e Adolescentes

Acesse os detalhes da TS aqui.

I - Princípio do melhor interesse

De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança[1], no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU[2] e no Comentário Geral n° 25, de 2021, do Comitê dos Direitos da Criança[3]. Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz.

Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, questiona-se:

Pergunta	Resposta ABRANET

[1] FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). Convenção sobre os Direitos da Criança. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em 12 jun 2024.

[2] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em 12 jun 2024.

[3] 8 UNITED NATIONS. General comment No. 25 (2021) on children's rights in relation to the digital environment. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em 12 jun 2024.

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?	É importante entender que, tendo em vista o grau de amplitude e abstração do princípio do melhor interesse - que, vale ressaltar, é natural e faz parte da própria ideia do princípio - o mais relevante é que a ANPD forneça **balizas sobre como, em casos concretos, esse princípio será avaliado,** tal como em guias orientativos. Evidente que não será possível prever exaustivamente todos os cenários existentes, e nem seria este o objetivo, mas adotar uma lógica como vem sendo feito em outros materiais de exemplificar situações, descrevendo os motivos pelos quais se entende que a situação A é considerada adequada e a situação B, inadequada, já seriam uma grande contribuição. Nesse mesmo sentido, seria importante que, ao levar em conta situações hipotéticas, a autoridade considerasse nuances concretas e esforços tecnicamente disponíveis, mantendo flexibilidade para diferentes contextos e modelos de negócio. A ABRANET reforça que o conceito de "melhor interesse" deve incluir tratamentos que protegem tanto o titular quanto terceiros, como na prevenção de fraudes e na proteção de identidade, mas também deve ser considerado em situações em que o tratamento não gera qualquer prejuízo para as crianças e os adolescentes. Em particular**, entende-se ser relevante conferir clareza sobre cenários em que este princípio deve ser sopesado com outros da LGPD.** Em particular, citamos o princípio da minimização, na medida em que ferramentas mais acuradas de verificação de idade, por exemplo, frequentemente implicam numa coleta mais expressiva de

	dados. Para que a ANPD possa direcionar o mercado, seria de extrema relevância que ela buscasse esclarecer em quais contextos esse tipo de conduta será adequada ou mesmo necessária, e em quais contextos será vista como excessiva. Por fim, a ABRANET reforça que é necessário que a ANPD, como autoridade competente, garanta a segurança jurídica ao orientar os agentes de tratamento sobre o "melhor interesse" na seara de proteção de dados pessoais antes que outras entidades menos preparadas o façam, como demonstrado pela Resolução Nº 245/2024 - CONANDA e o Projeto de Lei n° 2628 de 2022. A análise do "melhor interesse" deve considerar várias dimensões, tal como a segurança, acesso à informação e direitos ao lazer e conexão, entre outros aspectos e, principalmente, o respeito à autonomia progressiva, fornecendo orientações sobre como garantir que o "melhor interesse" seja adaptável ao desenvolvimento de cada indivíduo. Como referência internacional no tema, citamos o artigo "Age assurance for the Children's code" do Information Commissioner's Office do Reino Unido, que busca definir critérios e balizas específicas a serem considerados em mecanismos de verificação da idade [1]. [1] Disponível em: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.	Como dito, entende-se que os cenários em que o princípio do melhor interesse precisa ser sopesado com outros princípios da LGPD são aqueles que demandam maior esforço de esclarecimento do lado da autoridade. Na medida em que a cultura de proteção de dados pessoais no Brasil é ainda em alguma medida incipiente, não é trivial para os agentes de tratamento concretizar os parâmetros que serão utilizados pela ANPD para avaliar cenários concretos. Seria de particular relevância indicar balizas nas quais os agentes podem se apoiar para tomar decisões específicas em cenários variados, tendo em vista (i) as especificidades do tratamento de dados de crianças, de um lado, e de adolescentes, de outro, (ii) as particularidades de uso de dados pessoais de crianças e adolescentes para fins de direcionamento de conteúdo, tendo aqui particular atenção ao fato de que a personalização nestes casos não deve ser confundida com a publicidade direcionada, pois trata-se mais propriamente de personalização do próprio conteúdo a ser exibido, o que certamente tem finalidades inclusive protetivas de crianças e adolescentes. Especificamente, o perfilamento para fins de publicidade envolve a coleta e análise de dados para criar anúncios personalizados, enquanto o perfilamento para conteúdo utiliza dados para oferecer conteúdo relevante ao usuário, sem fins publicitários. Assim, enquanto a exposição constante à publicidade personalizada pode influenciar negativamente os jovens, o perfilamento de conteúdo pode fornecer informações educativas e construtivas. Além disso, o perfilamento

	pode prevenir fraudes, protegendo os jovens de atividades maliciosas e garantindo um ambiente digital mais seguro. Crianças e adolescentes, devido à sua menor experiência, são especialmente vulneráveis a golpes online. O uso de técnicas de perfilamento permite detectar comportamentos suspeitos em tempo real, alertando os jovens e seus responsáveis sobre possíveis ameaças, contribuindo para a segurança digital e educando-os sobre os riscos online. Em particular para a ABRANET, é importante que a ANPD se atente e dê diretrizes sobre a coleta de biometria para acesso a sistemas e aplicativos financeiros. Por fim, seria importante que, ao tratar das bases legais adequadas para o tratamento de dados de menores, a ANPD não afastasse, a priori, o uso de qualquer base legal, inclusive o legítimo interesse – reforçando o que foi estabelecido no Enunciado nº 1/2022, o Guia Orientativo sobre a hipótese legal do legítimo interesse.
II - Consentimento O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).	

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

Pergunta	Resposta ABRANET
1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?	É importante que, sempre que o consentimento parental for requerido, ele esteja adequado ao contexto de relação entre titular, responsável legal e agente de tratamento. Em outras palavras, é preciso ter em vista que há cenários muitos diversos, que podem demandar parâmetros bastante diferentes para que o consentimento seja ofertado. Para ficar em apenas um exemplo, se a relação com o agente de tratamento se dá de forma 100% offline, não seria razoável exigir que o consentimento "específico e em destaque" seja obtido num formato digital, e vice-versa. Cabe também observar que os adjetivos "específico e em destaque" diferem dos adjetivos "livre, informado e inequívoco" mencionados na LGPD. Assim, seria importante que a ANPD esclarecesse a que exatamente se refere a especificidade – ela diz respeito às finalidades

	do tratamento, diz respeito àquele titular em particular, diz respeito ao conjunto de dados? No que diz respeito ao destaque, o entendimento que parece mais natural é o de que a informação deve ser de alguma forma "segmentada" em relação a eventuais outras informações. Mas seria importante esclarecer se a premissa da autoridade será de que esse destaque deve conter elementos adicionais – por exemplo, pensando na perspectiva de design, se será necessário utilizar cores e fontes que garantam uma diferença visual. Por fim, é importante que este esclarecimento conceitual determine se o consentimento deve variar conforme diferentes faixas etárias, levando em conta a crescente autonomia de crianças e adolescentes.
2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de “todos os esforços razoáveis”, quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?	Embora o consentimento seja uma base legal importante para o tratamento de dados pessoais de crianças e adolescentes, seu uso deve ser ponderado conforme o contexto específico. Assim, a ABRANET aponta que uma interpretação restritiva que considera o consentimento como a única opção viável pode resultar em limitações excessivas, mesmo quando o tratamento dos dados está em conformidade com o melhor interesse da criança. A própria ANPD já reconheceu que há outras bases legais para além do consentimento que podem ser adequadas para sustentar tratamentos de dados pessoais de crianças e adolescentes. O Enunciado nº 1/2023 da Autoridade Nacional de Proteção de Dados (ANPD) esclarece que as hipóteses legais previstas no art. 7º da LGPD, incluindo o legítimo

	interesse, podem ser aplicadas para o tratamento de dados pessoais de crianças e adolescentes, desde que respeitando o princípio do melhor interesse da criança ou adolescente. Essa orientação é reforçada pelo Guia de Legítimo Interesse, que oferece diretrizes claras para os controladores sobre como interpretar e aplicar essa hipótese legal, precedida por uma análise criteriosa de balanceamento de interesses. Se e quando o consentimento for escolhido como base legal adequada para o tratamento de dados, é crucial garantir, como ressaltado por autoridades estrangeiras, que ele será obtido com o menor nível de intrusão possível à privacidade. Por exemplo, o Children's Online Privacy Protection Rule ("COPPA"), administrado pela FTC, estabelece que, embora a regra seja o consentimento dos pais e responsáveis, há exceções claras e objetivas. O European Data Protection Board (EDPB) enfatiza a necessidade de proporcionalidade na verificação do consentimento para tratamento de dados, variando conforme o risco envolvido e a tecnologia disponível, com verificações mais simples para riscos baixos e mais rigorosas para riscos altos. O Information Commissioner's Office e a Data Protection Commission concordam que a adequação dos esforços para verificar o consentimento depende dos riscos e da tecnologia, e que não existe um padrão único para o que constitui "esforços razoáveis", cabendo a cada organização decidir o método mais proporcional.

	A ANPD deve considerar os esforços razoáveis realizados pelos controladores para obter e verificar o consentimento parental, utilizando métodos acessíveis e proporcionais ao contexto do tratamento. Por exemplo, no caso do setor financeiro, em que já se adota a validação biométrica, seria possível considerar a prática da documentoscopia – a análise de documentos a fim de comprovar a identidade do titular. Esse é um dos métodos sugeridos no COPPA, i.e. verificar uma foto de uma carteira de motorista ou outra identificação com foto enviada pelo pai ou responsável e, em seguida, comparar essa foto com uma segunda foto enviada pelo pai ou responsável, utilizando tecnologia de reconhecimento facial. É essencial também que a autoridade tenha em mente que inexistem mecanismos infalíveis e que todo sistema pode, em alguma medida, ser burlado. A ABRANET destaca a importância de levar esse ponto em consideração ao delimitar a responsabilidade dos agentes de tratamento em casos de falha dos mecanismos. Por fim, exigências desproporcionais e onerosas para os agentes de tratamento podem comprometer a eficácia do processo e acabar sendo ignoradas pelos usuários, o que contradiz os objetivos de proteção de dados da LGPD. Especialmente neste momento em que a cultura de proteção de dados pessoais no Brasil ainda está em desenvolvimento, pode ser mais estratégico que a autoridade não adote parâmetros excessivamente onerosos, cuja chance de efetivo

	compliance serão reduzidas, o que não significa que tais parâmetros não poderão ser revistos no futuro.
3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?	O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) define "criança" como a pessoa até 12 anos e "adolescente" como aquela entre 12 e 18 anos. Já o Código Civil Brasileiro estabelece que menores de 16 anos são absolutamente incapazes de exercer pessoalmente os atos da vida civil, devendo ser representados. Aqueles com mais de 16 e menos de 18 anos são relativamente capazes, podendo praticar atos da vida civil desde que assistidos Não há, no entanto, clareza sobre o que exatamente estaria incluído na definição de "atos da vida civil", e essa ambiguidade pode impactar a aplicação do consentimento como base legal. É importante destacar que a legislação brasileira já confere aos adolescentes autonomia em cenários da vida civil consideravelmente complexos, como votar nas eleições nacionais, estaduais e municipais, casar-se sem a autorização de um representante legal e viajar pelo território nacional sem a companhia dos pais ou representantes legais, sendo necessário apenas a apresentação de um documento de identificação. Portanto, a ANPD deve levar em conta que adolescentes também poderiam ter a capacidade de fornecer consentimento para o tratamento de seus dados pessoais em alguns contextos - dado que já possuem autonomia para exercer certos direitos e realizar atos da vida civil. Para tal, a complexidade do ato deve ser levada em conta pela

	autoridade ao orientar os agentes de tratamento, por exemplo, a capacidade de realizar atos simples como comprar um ingresso de cinema para assistir um filme. Na mesma direção, é importante que não se considere que todo e qualquer ato online é impossível de ser levado a cabo por um adolescente e que, portanto, todos equivalem aos parâmetros para é diferente da capacidade de realizar atos mais complexos, como a compra de um imóvel. É importante não equiparar todos os atos online à complexidade de transações imobiliárias. A autonomia progressiva, reconhecida pelo ECA, sugere que a capacidade decisória de crianças e adolescentes deve ser respeitada e expandida à medida que amadurecem. Essa autonomia é crucial no setor financeiro para permitir que jovens assumam responsabilidades financeiras de forma segura e informada. Contudo, o Código Civil trata os indivíduos de 12 a 16 anos como incapazes homogêneos, o que pode obstaculizar o melhor interesse do jovem. Por exemplo, mesmo o GDPR, considerado bastante exigente, permite que os Estados Membros da União Europeia estipulem, por lei, uma idade inferior a 16 anos para o tratamento de dados pessoais de menores sem autorização do responsável legal, desde que essa idade não seja inferior a 13 anos. O guia da ICO determina que, aos 13 anos, as crianças no Reino Unido podem fornecer seu próprio consentimento para o processamento de dados, se o consentimento for a base legal para o processamento, no contexto de oferecer um serviço online diretamente a uma criança (Best interests of the child; Annex B).

	Na visão da ABRANET, em respeito à autonomia progressiva, o desenvolvimento desses titulares adolescentes deve ser respeitado, o que pode tornar desnecessária a representação ou assistência pelos pais ou responsáveis legais para determinados atos. A ANPD poderá detalhar e orientar essas hipóteses de dispensa do consentimento de um dos pais ou responsável legal, o que pode ser uma medida importante para garantir o desenvolvimento pleno da personalidade e a formação cidadã dos indivíduos. É essencial reconhecer outras fontes de apoio além do suporte parental, promovendo a autonomia e o desenvolvimento progressivo das crianças e adolescentes à medida que crescem e adquirem experiências. A ABRANET ressalta que, para que essa autonomia progressiva seja efetivamente considerada e utilizada, é necessário que os controladores de dados adotem medidas que assegurem a compreensão e a clareza do consentimento fornecido pelos adolescentes. Isso inclui a elaboração de políticas de privacidade e termos de uso compreensíveis para essa faixa etária. Por fim, a ABRANET considera essencial que a ANPD esclareça em quais situações o consentimento dos pais ou responsáveis é indispensável. Por exemplo, para que os menores possam exercer seus direitos, é necessário obter o consentimento dos pais ou responsáveis? Isto é, o menor pode exercer esse direito diretamente ou o pai/responsável deve fazê-lo? Esse esclarecimento é relevante para que os agentes de

	tratamento possam se adequar, criando ou melhorando procedimentos para o exercício dos direitos.

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações “estritamente necessárias à atividade”.

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de design, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

Pergunta	Resposta ABRANET
1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?	Entende-se que estas perguntas são focadas alguns setores de forma mais enfática, tais como redes sociais, jogos e outras plataformas de entretenimento ou outras aplicações destinadas ou mais utilizadas por crianças e adolescentes. Ainda assim, a ABRANET destaca a importância de que a ANPD forneça exemplos ou parâmetros que orientem os agentes de tratamento sobre medidas de segurança consideradas adequadas, sem violar os

	demais princípios da LGPD, em particular no que diz respeito ao setor financeiro e de pagamentos. Essa orientação é essencial devido à possível dissonância entre a eficácia dos mecanismos de segurança e a observância dos princípios estabelecidos pela LGPD. Ademais, considerando que o setor financeiro já é regulado por normativas específicas, é fundamental que a autoridade leve em conta essas normas ao indicar os parâmetros de privacidade e proteção de dados para menores de idade. Portanto, a orientação da ANPD deve integrar não apenas os princípios da LGPD, mas também as exigências regulatórias já aplicáveis aos variados segmentos. Dessa forma, assegura-se uma abordagem harmonizada e eficaz que respeite a complexidade regulatória existente e proteja adequadamente os dados dos menores. Os conceitos de "privacy by design" e "privacy by default" são especialmente relevantes, principalmente quando se trata de serviços financeiros e de pagamento e, portanto, seria de extrema importância um direcionamento da autoridade sobre esse assunto. Por exemplo, com o objetivo de apresentar parâmetros para que os agentes de tratamento consigam lidar com a tensão entre o melhor interesse da criança e do adolescente e demais princípios da LGPD, seria relevante que a autoridade indicasse como os agentes de tratamento podem balancear a necessidade de implementar medidas de design e, ao mesmo tempo, respeitar o direito positivado à autonomia progressiva da criança e do adolescente. Seria suficiente implementar medidas

	mais protetivas como padrão, mas oferecer aos usuários a opção de alterá-las? Ressalta-se que, também em consonância com o melhor interesse da criança, a ANPD poderia indicar exemplos de medidas que permitam algum tipo de supervisão parental. Embora a ANPD deva criar seu próprio guia, documentos internacionais podem auxiliar esse processo. Por exemplo, o Age Appropriate Design Code (ou "Children's Code"), - elaborado pelo Information Commissioner's Office (ICO) do Reino Unido, que contém diretrizes para a proteção e privacidade online de crianças e adolescentes -, possui um capítulo destinado à "Configurações Padrão", cujo início é precisamente a descrição do conceito "privacy by default". O ICO recomenda que as configurações sejam de "alta privacidade" por padrão, exceto quando houver uma justificativa convincente em contrário, sempre levando em consideração o melhor interesse da criança.
2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?	A implementação de ferramentas de verificação da idade dos usuários apresenta desafios técnicos que podem variar significativamente conforme a natureza do serviço oferecido e novas funcionalidades disponibilizadas. É preciso reconhecer também que nenhum mecanismo é infalível e, dessa forma, a autoridade deve levar em conta os esforços razoáveis dos diferentes agentes de tratamento para implementá-los, levando em conta o estado da arte da tecnologia. Nesse sentido, seria benéfico que a autoridade fornecesse parâmetros

	de adequabilidade flexíveis, orientando os agentes de tratamento sobre formas adequadas de adaptação das ferramentas, por exemplo, como o já citado guia elaborado pela ICO, Age Appropriate Design Code (ou “Children's Code”), ou o Children's Online Privacy Protection Rule ("COPPA"), que impõe certos requisitos aos operadores de websites ou serviços online direcionados a crianças menores de 13 anos. Ambos os guias apresentam exemplos de mais de um método que pode ser considerado adequado. A ANPD pode seguir esses exemplos e indicar algumas práticas que podem ser avaliadas com bons olhos pela autoridade, tal como a verificação da idade por meio de validação de cartão de crédito; estimativa de idade com base em detecção facial (sem intenção de identificar o indivíduo), análise de documentos de identidade, dentre outros. Além disso, considerando a falibilidade de qualquer mecanismo implementado, a ANPD deve levar em conta que existe a possibilidade de menores e pais contornarem esses mecanismos *offline*, por exemplo, quando responsáveis fornecem seus próprios aparelhos para uso pelo menor. Assim, destaca-se a importância de não impor ônus excessivo sobre essa verificação aos controladores. Por isso mesmo, deve ser levado em conta o fato de que métodos de verificação de idade não devem substituir a função de cuidado dos pais e responsáveis. Por fim, conforme já apontado anteriormente, a ANPD deve apresentar parâmetros para que os agentes de tratamento consigam

	lidar com a tensão entre a eficácia de mecanismos de verificação de idade e demais princípios da LGPD, em especial o princípio da minimização de tratamento de dados pessoais. Como feito em outros guias, sugere-se que algumas situações sejam utilizadas como exemplos, a fim de esclarecer como tal sopesamento deve ser feito pelos agentes de tratamento - indicando, por exemplo, se mecanismos de detecção de menores de idade em plataformas pode ser uma forma de mitigar a coleta de mais dados no momento de acesso à plataforma. Em especial, a ABRANET entende que a ANPD deveria se manifestar sobre a prática de requisição de identidade para os exercícios de direitos dos titulares menores.
3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?	Considerando que a própria LGPD não impõe restrições automáticas ao tratamento de dados de menores, desde que respeitadas as bases legais adequadas e medidas de segurança, a ABRANET destaca que **a coleta de dados de crianças e adolescentes não deve ser limitada por padrão**, salvo quando necessário para proteger seus melhores interesses. Conforme indicado na pergunta anterior, medidas de segurança são de extrema relevância no setor financeiro e de pagamentos e, portanto, parece ser contra o melhor interesse da criança e do adolescente que se colete menos dados desses titulares se isso prejudicar sua segurança. Ao coletar dados de crianças e adolescentes, deve-se considerar a necessidade dos dados para o modelo de negócio sem comprometer a segurança e privacidade dos usuários. Dessa forma, a ABRANET ressalta que o tratamento desses

	dados deve ser analisado caso a caso, considerando os riscos específicos. Nesse sentido, **reforça-se que não há tratamentos de dados pessoais que sejam maléficos a priori**. Especificamente no setor financeiro e de pagamentos, o tratamento de dados pessoais, incluindo a formação de perfis comportamentais e a personalização de anúncios, não deve ser visto de maneira necessariamente negativa, pois pode oferecer benefícios significativos, principalmente no sentido de auxiliar os menores a desenvolverem habilidades financeiras de maneira segura e informada. A formação de perfis comportamentais pode inclusive ajudar a personalizar programas educativos financeiros, adaptando o conteúdo ao nível de entendimento e interesse do jovem. Isso pode tornar o aprendizado mais eficiente e relevante, ajudando a desenvolver habilidades financeiras desde cedo. Um outro exemplo diz respeito à segurança e proteção: perfis comportamentais podem ser usados para identificar padrões incomuns ou riscos de fraude, protegendo assim os menores contra atividades financeiras não autorizadas ou prejudiciais. Assim, a ABRANET entende que a ANPD deve se atentar para esses mecanismos que, se utilizados de maneira responsável e transparente, não são inerentemente maléficos e podem contribuir significativamente para a educação financeira e a segurança dos jovens. Assegurar que essas práticas sejam implementadas com controle parental é fundamental para equilibrar

	a proteção dos dados pessoais com a promoção da autonomia e do desenvolvimento financeiro saudável dos menores.
4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?	A autonomia progressiva, conforme reconhecida no Estatuto da Criança e do Adolescente (ECA), estipula que crianças e adolescentes devem ter sua capacidade de decisão respeitada e ampliada conforme crescem e amadurecem. A relação entre a autonomia progressiva da criança e do adolescente é crucial para garantir que jovens possam gradualmente assumir responsabilidades de maneira segura e informada. Nesse sentido, é importante que a ANPD incentive soluções que permitam a participação gradual e supervisionada de jovens que paulatinamente transforme o *controle* dos pais e responsáveis em uma *supervisão*, até que se atinja a maioridade já com relevante autonomia digital. Podemos citar como exemplo a criação de plataformas e serviços que ofereçam contas vinculadas ou supervisionadas para menores de idade, permitindo aos pais monitorar e autorizar atividades online. Isso promove a educação digital e o uso responsável da internet enquanto garante a supervisão necessária. Outro exemplo relevante é o controle parental, que pode ser utilizado para proteger os dados e a privacidade dos jovens, garantindo um ambiente digital seguro e educativo.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?	A ABRANET sugere que há algumas práticas que podem garantir a transparência direcionada aos menores, sem, no entanto, desconsiderar o salutar incentivo ao diálogo de pais e responsáveis com os menores de idade. Exemplos incluem: canal de comunicação aberto, sessões de perguntas frequentes e transparência nas atualizações de políticas e termos de uso. No entanto, a ANPD deve reconhecer alguns limites à prestação de transparência pelos agentes de tratamento. Esses limites incluem as limitações técnicas e o estado da arte da tecnologia, o segredo comercial e industrial dos agentes de tratamento, e o fato de que, dependendo da informação oferecida, pode haver risco de uso indevido por atores mal-intencionados, o que poderia potencialmente levar a riscos adicionais para a segurança de menores, em especial no que diz respeito a produtos e serviços financeiros. A ANPD deve reconhecer que algumas práticas de transparência podem ser contraproducentes. Por exemplo, é importante que a Política de Privacidade esteja facilmente acessível na documentação dos agentes de tratamento, mas não há necessidade de ser exibida constantemente ao usuário, evitando assim a fadiga. Retomar informações específicas em momentos diretamente relevantes para o tratamento de dados em questão pode ser uma abordagem mais eficaz.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?	A ABRANET destaca a importância de que a autoridade se manifeste em relação à retenção de dados pessoais de titulares após atingirem a maioridade. Essa manifestação é um aspecto fundamental para garantir segurança jurídica aos agentes de tratamento e, ao mesmo tempo, a conformidade com a LGPD, assegurando que os direitos dos indivíduos sejam plenamente respeitados à medida que transitam da infância e adolescência para a idade adulta. Por fim, a ABRANET reforça que seria benéfico que a ANPD implementasse orientações e ações educativas sobre o tratamento de dados pessoais de crianças e adolescentes, principalmente no que tange à introdução de tecnologias inovadoras.

A member of

World Federation of Advertisers

TOMADA DE SUBSÍDIOS DA ANPD
Tema: Tratamento de Dados Pessoais de Crianças e Adolescentes

QUESTIONÁRIO

PRINCÍPIO DO MELHOR INTERESSE

1) Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

A ABA – Associação Brasileira de Anunciantes é uma entidade sem fins lucrativos, atuante há 65 anos no mercado. Na qualidade de uma das fundadoras do CONAR – Conselho Nacional de Autorregulamentação Publicitária, instituição privada sem fins lucrativos, fundada por entidades que representam anunciantes, veículos, agências de publicidade e a sociedade civil, com o objetivo de fomentar a publicidade responsável e ética, e por ser filiada à WFA – *World Federation of Advertisers* e membro de seu *Executive Committee*, entidade que congrega associações de anunciantes de 60 países, a ABA atua ativamente para conscientizar anunciantes contra quaisquer práticas publicitárias que possam implicar desrespeito à legislação e à autorregulamentação existentes, bem como qualquer mínimo abuso ao consumidor.

Neste sentido, suas contribuições se voltam mais especificamente ao tema da liberdade de expressão comercial e a regulamentação aplicável, consignado seu entendimento de que a LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709/18) já estabelece importante proteção e limites quanto à coleta de dados de crianças e adolescentes, no âmbito da publicidade digital.

De acordo com o artigo 14 da LGPD, *"O tratamento de dados pessoais de crianças e de adolescentes* ***deverá ser realizado em seu melhor interesse****, nos termos deste artigo e da legislação pertinente*", prescrevendo, ainda, o seu § 1o que "*O tratamento de dados pessoais de crianças deverá ser realizado* ***com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal***", tendo o Enunciado CD/ANPD 1/23 reforçado que o tratamento de dados do público infantil está autorizado nas hipóteses previstas nos artigos. 7º e 11 da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do artigo 14 da Lei (ou seja: o consentimento parental não é a única base legal para o processamento de dados pessoais de menores de idade). Restringe-se, assim – e apenas para citar um exemplo –, a possibilidade de direcionamento, irresponsável e não consentido, de publicidade baseada em hábitos de navegação das crianças.

Neste sentido, a ABA é favorável que sejam aplicadas as restrições e proibições já existentes em nosso ordenamento jurídico, condenando-se (apenas) eventuais abusos que possam ocorrer em contrariedade à legislação – e não a atividade em si.

A ABA defende o caminho da autorregulamentação como o mais eficaz para a resolução de potenciais conflitos (OCDE – Organização para a Cooperação e o Desenvolvimento Econômico, 2015). As normas e a atuação do CONAR, neste particular, são

fundamentais pois conferem ampla proteção às crianças, cuidando o setor de se autorregrar constantemente. Nesse sentido, traz um extenso rol de restrições à publicidade direcionada a crianças e adolescentes (por exemplo, em seus artigos 27, 33 e 37), aplicando-se, ainda, a LGPD sempre que necessário, em contínua atualização.

Vale notar que esse modelo de atuação para proteção de crianças e adolescentes em ambientes digitais é o caminho seguido pelas jurisdições mais modernas, que a par da legislação já existente, delega à autorregulamentação o aperfeiçoamento e atualização das normas, bem como o seu monitoramento constante, como medida mais efetiva, dinâmica e célere de controle.

Essas são, por exemplo, as recomendações de organismos internacionais tais como OCDE, a ICC –*International Chamber of Commerce*, a ICPEN – International Consumer Protection and Enforcement Network, além da própria Comunidade Europeia.

A OCDE, no documento *The Protection of Children Online* (2012) e citado igualmente em sua publicação de 2020, considera que as melhores práticas em termos de políticas públicas para proteção de crianças e adolescentes em ambientes digitais devem combinar medidas públicas e privadas, normativas e iniciativas voluntárias em diferentes níveis. Não há qualquer orientação ou recomendação de proibições absolutas no ambiente digital. Ainda, a OCDE dispõe, na Recomendação ao Conselho sobre Crianças no Ambiente Digital (atualizada em 2021), que eventuais medidas adotadas por atores do setor público e privado para proteger crianças e adolescentes deveriam ser proporcionais aos riscos, baseadas em evidências, balanceadas e formuladas com vistas a maximizar as oportunidades e benefícios para as crianças no ambiente digital.

Assim, na visão da ABA, em vista do arcabouço jurídico já existente no país, não há necessidade de imediata edição de nova regulamentação específica sobre o tema do legítimo interesse pela ANPD – Autoridade Nacional de Proteção de Dados. Importante, todavia, que eventuais novas regulações não colidam com as disposições já existentes, e que não tragam disposições com termos genéricos que ocasionem insegurança jurídica quanto à sua intepretação.

Para ilustrar o ponto, a ABA pondera, respeitosamente, que o artigo 12, §2º da Resolução nº 245/2024 do CONANDA - Conselho Nacional dos Direitos da Criança e do Adolescente (publicada em 09/04/2024), a despeito de não ser lei e deter caráter meramente orientativo (não vinculante), aportou insegurança jurídica ao mercado, ao prever, em seu trecho final, a garantia da equiparação de dados de crianças e adolescentes a dados pessoais sensíveis, a qual não encontra paralelo na LGPD.

Como é sabido, a LGPD definiu no artigo 5º, II que o "dado pessoal sensível", é o "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natura*". Claramente, não guarda relação com dado pessoal de criança e de adolescente. Nesse sentido, a LGPD regulou o tratamento de dados pessoais sensíveis na Seção II (intitulada "Do Tratamento de Dados Pessoais Sensíveis"), ao passo que regulou o tratamento de dados pessoais de crianças e de adolescentes na Seção III (intitulada "Do Tratamento de Dados Pessoais de Crianças e de Adolescentes").

Ou seja: **sinalizou claramente que são temas e conceitos distintos**, que merecem regulação distinta e específica. O citado §2º do artigo 12 da mencionada Resolução,

como se vê, prevê orientação contrária à regulação cuidadosa, específica e detalhada da LGPD.

2) Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

A ABA tem acompanhado com atenção questões sensíveis recentes acerca: (i) do fato de jogos de azar na internet – dentre eles o que ficou conhecido como "jogo do tigrinho" – estarem alegadamente contratando influenciadores mirins brasileiros para divulgar as casas de apostas para crianças e adolescentes em determinada rede social, direcionando tal divulgação especificamente para os perfis de crianças e de adolescentes – não obstante o próprio estabelecimento e a exploração de jogo de azar em local público ou acessível **já serem proibidos no país** (art. 50 do Decreto-Lei 3.688/41); e (ii) as BETs (casas esportivas na internet), regulamentadas pela Lei 14.790/2023, que também têm atraído crianças e adolescentes não obstante a sua publicidade já ser proibida para menores de 18 anos (cf. artigo 16, III da referida Lei).

O tema já vem sendo endereçado por diversas entidades e empresas, visando à proteção aos direitos das crianças e dos adolescentes. O CONAR, por exemplo, adicionou o Anexo X ao Código Brasileiro de Autorregulamentação Publicitária, o qual prevê que as publicidades de apostas não terão crianças e adolescentes como participantes ou como público-alvo, tendo detalhado diversos cuidados a serem adotados pelos anunciantes e suas agências na elaboração de suas estratégias mercadológicas e na estruturação de suas mensagens publicitárias – todas, como é notório, sujeitos a severas penalidades pelo CONAR em caso de descumprimento.

Nesse contexto, um ponto de atenção é se os dados pessoais de crianças e adolescentes estão sendo coletados e utilizados de forma indevida no contexto desses jogos de azar e de BETs, e se o princípio do melhor interesse foi utilizado como fundamento para tal. Trata-se de tema que poderia ser objeto de análise, debates e de eventual atuação pela ANPD – por exemplo, para impedir a coleta de dados de crianças e de adolescentes para publicidade de BETs –, em vista da sensibilidade das questões envolvidas, e pelo fato de envolver também ações no âmbito de redes sociais.

Para além disso, a ABA gostaria de aproveitar a oportunidade para tecer uma consideração acerca de um exemplo trazido no Guia Orientativo sobre a hipótese legal do legítimo interesse na página 12 (exemplo 3), que versa sobre "*uso de dados de crianças e adolescentes para publicidade*". Nesse exemplo, menciona-se o caso de uma startup do ramo educacional que desenvolve um aplicativo para ensino de geografia para crianças e adolescentes, e, para sua execução, solicita informações como: "*nome do usuário, data de nascimento e endereço residencial*". Durante o uso do app, anúncios publicitários sobre alimentos ultraprocessados e com alto teor de açúcar são exibidos aos titulares, quando na política de privacidade disponibilizada em sua página na internet, consta apenas a informação de que a hipótese legal utilizada é o legítimo interesse do controlador e que tais dados são utilizados para o aprimoramento do aplicativo.

Na análise sobre esse exemplo, apresenta-se crítica no sentido de que: (i) "*a finalidade do tratamento de dados em questão envolve o direcionamento de publicidade para crianças e adolescentes*"; (ii) "o *legítimo interesse não será a hipótese legal mais apropriada, tendo em vista que não há legítima expectativa do titular quanto ao tratamento de seus dados pessoais para fins publicitários, inclusive porque nada é informado a respeito*"; e (iii) "*considerando o teor do anúncio veiculado, qual seja, alimentos ultraprocessados e com alto teor de açúcar, deve-se considerar o risco à saúde que tais produtos implicam e a consequente não observância do melhor interesse da criança e do adolescente na hipótese*".

Sobre essa análise, a ABA sugere, respeitosamente, que a Ilma. ANPD deixe expresso de forma clara que a publicidade em si no app não é o problema – ou seja, que o app pode, sim, veicular publicidade, mas que o problema verificado foi que os dados pessoais coletados não foram aplicados para a finalidade indicada na política de privacidade (que não havia contemplado o uso dos dados para direcionamento de publicidade).

Sobre o fato de a publicidade mencionada tratar de "alimentos ultraprocessados e com alto teor de açúcar", e de o Guia afirmar que tais produtos apresentam risco à saúde e que a sua publicidade no app poderia ir contra o melhor interesse da criança e do adolescente, a ABA pondera que é importante fazer uma distinção entre "alimentos ultraprocessados" e "alimentos com alto teor de açúcar". O termo "alimentos ultraprocessados" se refere ao grau e tipo de processamento do alimento, e não tem correlação necessária com sua qualidade nutricional. Tanto é assim que a rotulagem dos alimentos foi extensamente debatida e regulamentada pela ANVISA - Agência Nacional de Vigilância Sanitária, não tendo esse órgão técnico adotado essa terminologia e nem previsto alerta específico para produtos ultraprocessados.

Assim, a ABA pondera que a referência a alimentos ultraprocessados é inadequada, devendo, quando muito, ser mantida apenas a menção a alimentos com alto teor de açúcar.

CONSENTIMENTO

1) Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

A ABA pede vênia para apresentar contribuições que mostram que o tema ainda está sendo estudado por diversas legislações, contribuindo com exemplos verificados no direito comparado como forma de subsidiar futura análise de impacto regulatório.

No que tange a sites ou serviços direcionados às crianças, a regulação norte-americana do COPPA - *Children's Online Privacy Protection Act* dos EUA – aplicada aos operadores de dados de websites e serviços on-line dirigidos para crianças e, também, àqueles que são voltados ao público em geral, mas que coletam informações sobre o público infantil –, prevê, dentre as condições impostas aos operadores dos dados pessoais infantis, obter o consentimento dos pais para a coleta dos dados pessoais da criança (págs. 284-285 do estudo), na esteira do art. 14, LGPD.

Segundo a regulação do COPPA, o operador como regra geral deve obter o consentimento parental verificável antes de coletar qualquer dado pessoal de crianças menores de 13 anos de idade, excetuados os casos previstos na própria regulação. O COPPA permite o uso de diversos métodos para obter esse consentimento parental verificável (alguns deles descritos na resposta à questão 2 logo abaixo), desde que o método escolhido seja razoavelmente calculado para garantir que a pessoa que fornece o consentimento é um dos pais da criança (ou o responsável por ela). A Regra estabelece diversas opções não-exaustivas, e pode-se solicitar à FTC – Federal Trade Commission norte-americana a pré-aprovação de um novo mecanismo de consentimento, conforme estabelecido na FAQ disponível em: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent >.

A GDPR - *General Data Protection Regulation* europeia, por sua vez, trata sobre a questão do consentimento nos artigos 7 e 8. Prevê, no artigo 7.2, que se o consentimento do titular dos dados for dado no âmbito de uma declaração escrita que também diga respeito a outras matérias, o pedido de consentimento deve ser apresentado de forma claramente distinguível dos demais temas, de forma inteligível e facilmente acessível, utilizando linguagem simples e clara. O artigo 8º dispõe especificamente sobre o consentimento envolvendo crianças, tendo indicado que o processamento de dados pessoais de crianças abaixo de 16 anos apenas será lícito se e na medida em que o consentimento seja dado ou autorizado pelo titular da responsabilidade parental sobre a criança, podendo os Estados Membros preverem por lei uma idade inferior (desde que acima de 13 anos). O Recital (58) do GDPR, por sua vez, traz parâmetros adicionais, indicando que: (i) o princípio da transparência exige que qualquer informação dirigida ao público ou ao titular dos dados seja concisa, facilmente acessível e de fácil compreensão, e que seja usada uma linguagem clara e simples e, quando apropriado, o uso de recursos visuais, podendo as informações serem fornecidas em formato eletrônico; e (ii) dado que as crianças merecem proteção específica, qualquer informação e comunicação, sempre que o tratamento seja dirigido a uma criança, deve ser feita numa linguagem tão clara e simples que a criança possa compreender facilmente.

Contudo, o GDPR não apresenta formas práticas de se obter o consentimento parental, ou para estabelecer que alguém é de fato o titular para conceder o consentimento. O EDPB - *European Data Protection Board*, então, recomendou no documento "Diretrizes 05/2020 sobre Consentimento sob a Regulation 2016/679", nos itens 136 e 137, a adoção de uma abordagem proporcionada, focada na coleta de uma quantidade limitada de dados pessoais, como recomenda também a legislação brasileira. Concretamente, as Diretrizes recomendaram verificar os riscos inerentes ao processamento dos dados pessoais no caso concreto: em casos de baixo risco, a verificação da responsabilidade parental através de e-mail pode ser suficiente. Por outro lado, em casos de alto risco, pode ser apropriado solicitar mais provas, para que o responsável pelo tratamento possa verificar e reter as informações nos termos do artigo 7.º, n.º 1, do GDPR. Serviços de verificação de terceiros confiáveis podem oferecer soluções, que minimizam a quantidade de dados pessoais que o próprio responsável pelo tratamento tem de tratar.

Para além das práticas observadas nas regulações estrangeiras – que podem trazer insumos interessantes para reflexão –, a ABA pondera ser essencial que quaisquer

meios de obtenção de consentimento que venham a ser considerados sejam analisados à luz da realidade concreta brasileira, inclusive para evitar que sejam implementados critérios e parâmetros descolados da realidade tecnológica, econômica e social brasileira. Por exemplo: a coleta do consentimento do responsável via videoconferência pode ser viável no contexto de uma sociedade com maior inclusão digital – o que não é necessariamente a realidade brasileira atual; já fornecer um número de telefone para que o responsável possa ligar gratuitamente para uma central e conceder o consentimento pode ser uma via a ser estudada, desde que adicionadas camadas de segurança para verificação da identidade desse responsável.

2) Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

A regulação norte-americana do COPPA (*Children's Online Privacy Protection Act* dos EUA) – aplicada aos operadores de dados de websites e serviços on-line dirigidos para crianças pode oferecer alguns subsídios interessantes, tendo inclusive um FAQ disponível para endereçar situações mais específicas.

Uma das questões do FAQ (questão 7 do item "Verifiable Parental Consent") indica que muitos operadores entendem ser útil oferecer mais de um método possível para envio do consentimento pelos pais ou responsáveis da criança – por exemplo, caso eles não tenham como se valer do mecanismo primário de consentimento. Com mencionado na resposta à questão anterior, as regras do COPPA permitem o uso de diversos métodos para obter esse consentimento parental verificável, desde que o método escolhido seja razoavelmente calculado para garantir que a pessoa que fornece o consentimento é um dos pais da criança.

Exemplos de métodos já aprovados pelo COPPA incluem, por exemplo:

(i) Fornecer um formulário de consentimento a ser assinado pelos pais e devolvido por correio, fax ou digitalização eletrônica dos EUA (o método "imprimir e enviar");
(ii) Exigir que o pai ou responsável, em conexão com uma transação monetária, use um cartão de crédito, cartão de débito ou outro sistema de pagamento on-line que forneça notificação de cada transação distinta ao titular principal da conta;
(iii) Fazer com que os pais liguem para um número de telefone gratuito com funcionário treinado ou que os pais se conectem a funcionário treinado por meio de videoconferência;
(iv) Verificar a identidade dos pais, verificando um formulário de identificação emitido pelo governo em bancos de dados de tais informações, desde que se exclua imediatamente a identificação dos pais após concluir a verificação;

(v) Exigir que os pais respondam a uma série de perguntas desafiadoras baseadas no conhecimento que seriam difíceis de serem respondidas por outra pessoa que não os pais;

(vi) Verificar uma fotografia de uma carta de condução ou outro documento de identificação com fotografia apresentado pelos pais e, em seguida, comparar essa fotografia com uma segunda fotografia enviada pelos pais, utilizando tecnologia de reconhecimento facial, conforme aprovado separadamente pela Comissão, utilizando os procedimentos estabelecidos na FAQ I.12; e

(vii) Se informações pessoais de crianças forem usadas apenas para fins internos – ou seja, não haverá divulgação das informações a terceiros ou não serão tornadas disponíveis publicamente – então pode-se usar qualquer um dos métodos acima ou o método de consentimento chamado de "email plus". "Email plus" permite solicitar (no aviso direto enviado ao endereço de contato online dos pais ou do responsável) que os pais ou o responsável indiquem consentimento em uma mensagem de resposta.

Naturalmente, trata-se de opções consideradas à luz da realidade norte-americana. Eventual incorporação desses métodos no Brasil demandará estudo prévio sobre a sua pertinência, adequação e viabilidade à realidade brasileira.

Focando-se na realidade brasileira, a ABA sugere que se avaliem as seguintes recomendações gerais, sujeitas a um maior detalhamento a depender do caso concreto:

(i) que o nível de criticidade para a validação do consentimento dos pais seja proporcional à criticidade do tratamento (ex.1 para o tratamento de dados de saúde/sensíveis, deveria haver uma validação usando o Gov.br; ex.2 para que a criança/ adolescente possa pedir um Uber, bastaria que o responsável clicasse em um e-mail de autenticação e recebesse as informações das corridas do filho ou preenchesse um formulário adicional com seus dados, carregando uma imagem do documento de identificação);

(ii) que se reconheça que muitos dos métodos de verificação poderão ser falhos (ex. uma criança poderia enviar uma foto do documento de identificação do pai sem o seu consentimento) e que poderão inviabilizar atividades do dia a dia ou ser proforma, de maneira que qualquer regulamentação precisará ser muito bem ponderada;

(iii) que, por um lado, devemos nos valer das novas tecnologias para garantirmos uma validação de consentimento eficiente, e, por outro lado, nem todas as atividades (tampouco todos os operadores de dados) poderão se utilizar dessas novas tecnologias sempre, de forma que será necessário pensar em todas as realidades a fim de não se esvaziar a norma.

3) No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a

autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

Segundo os Princípios para um Ambiente Digital Seguro e Benéfico para as Crianças da OCDE (2024) (disponíveis em: https://legalinstruments.oecd.org/public/doc/272/272.en.pdf), item 4, os atores do ambiente digital deveriam ter em conta as diferentes necessidades das diferentes crianças, tendo em consideração a sua idade e maturidade. No mesmo sentido, segundo reconhecido no paper da OCDE intitulado "*Towards digital safety by design for children*" (junho/2024) (disponível em <https://one.oecd.org/document/DSTI/CDEP(2023)13/FINAL/en/pdf>), p. 32, fazer o design de um determinado espaço digital tendo a segurança de crianças e de adolescentes em mente não significa desenhar um espaço para um grupo irrealista homogêneo consistindo apenas de crianças, devendo-se assegurar que esse espaço digital seja apropriado à idade (age appropriate).

Isso requer reconhecer que aquilo que pode ser seguro e apto a um adolescente de 16 anos é inapropriado para uma criança de 8 anos.

Com relação especificamente à observância das disposições do direito civil a respeito das capacidades civis (i.e. o Estatuto da Criança e do Adolescente – que prevê que pessoas até 12 anos são crianças, e de 12 a 18 são adolescentes; e o Código Civil, que prevê que menores de 16 anos são absolutamente incapazes, e que pessoas entre 16 e 18 anos incompletos são relativamente incapazes), seguindo a regra geral de representação e de assistência de pais ou responsáveis, para a questão do consentimento, a ABA não tem comentários específicos sobre o tema nesta oportunidade, reservando-se o direito de se manifestar oportunamente, caso receba subsídios específicos de suas associadas sobre a questão.

JOGOS E APLICAÇÕES DE INTERNET

1) Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Segundo indicado no *paper* da OCDE intitulado "*Towards digital safety by design for children*" (junho/2024), p. 32, um design regulatório centrado nas crianças é sobre possibilitar experiências digitais que permitam às crianças serem criativas, que as ajudem a regular suas emoções, a construir sua confiança, a dar-lhes um senso de propósito e de empoderamento, que facilitem conexões sociais e que tragam alegria. Nesse sentido, espaços digitais que focam apenas em prevenir o dano às crianças em detrimento de considerar os direitos e as necessidades das crianças de forma holística poderão conduzir à exclusão dessas crianças de ambientes digitais que poderiam avançar o seu desenvolvimento e o seu bem-estar. Em outras palavras, quando os

espaços digitais estão focados apenas em prevenir danos em detrimento de possibilitar oportunidades positivas, as crianças poderão se sentir acuadas e decidir se aventurar em espaços digitais que podem não ser seguros.

A ABA compactua com a ponderação acima destacada no *paper* da OCDE, e ressalta que um design regulatório centrado em crianças e em adolescentes deveria ser pautado por evidências técnicas e científicas consistentes – o que pode exigir a realização de estudos, de consultas e de colaboração no que tange ao compartilhamento de determinados dados e de experiências entre atores internacionais. No mesmo sentido, a OCDE recomenda a adoção de políticas baseadas em evidências para apoiar crianças no ambiente digital no item III.4 dos Princípios para um Ambiente Digital Seguro e Benéfico para as Crianças (2024), disponíveis em: <https://legalinstruments.oecd.org/public/doc/272/272.en.pdf>.

No que tange especificamente à proteção da privacidade e dos dados pessoais das crianças e dos adolescentes, o referido *paper* da OCDE pondera que envolve considerar: (i) como as violações da privacidade afetam a segurança das crianças; (ii) como a segurança digital por design regulatório pode ser aproveitada para proteger contra violações de privacidade; e (iii) como equilibrar os riscos para a privacidade das crianças que podem surgir de medidas que procuram garantir a segurança online das crianças (por exemplo, mecanismos de verificação de idade que utilizam dados sensíveis ou biométricos, ou de ferramentas concebidas para detectar ou prevenir danos).

Segundo a Tipologia Revisada de Riscos da OCDE, a violação de privacidade é um risco transversal que pode ter um impacto abrangente na vida das crianças. É essencial que as ferramentas de segurança preservem a privacidade e cumpram as obrigações de privacidade e de proteção de dados existentes. Por exemplo, ferramentas de segurança que monitoram a conduta das crianças online e recolhem informações sensíveis sobre elas podem representar riscos de violações da privacidade. É necessário considerar cuidadosamente o equilíbrio entre as medidas para promover a segurança e a capacidade das crianças de utilizar e desfrutar do ambiente digital sem que a sua privacidade e autonomia sejam violadas.

A nível nacional, segundo o referido paper (p. 36), várias leis protegem a privacidade das crianças e um número crescente exige que os prestadores de serviços digitais tenham em conta a privacidade e a proteção de dados durante as primeiras fases do processo de desenvolvimento e ao longo de todo o processo de design desses serviços (inclusive no que diz respeito à coleta, uso e armazenamento de dados pessoais de crianças).

Por exemplo, o Código dos Direitos da Criança dos Países Baixos – que consiste em dez princípios para designers e desenvolvedores para salvaguardar os direitos fundamentais das crianças em serviços digitais –, estabelece que os designers e desenvolvedores de serviços digitais deveriam fornecer um design de privacidade amigável para crianças, não deveriam processar mais dados pessoais do que o estritamente necessário, e deveriam definir configurações-padrão tão favoráveis à privacidade quanto possível. Nos EUA, por sua vez, a regulação do COPPA exige que os dados sejam retidos apenas pelo período necessário, e que a participação da criança em uma atividade online não seja

condicionada ao fornecimento de mais informações do que o necessário para aquela atividade – em linha com o que prevê hoje o artigo 14, §4º da LGPD brasileira.

2) Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

A ABA recorda que produtos, serviços e conteúdos reconhecidamente para maiores de 18 anos, como aqueles relativos a bebidas alcoólicas – os quais são claramente incompatíveis com crianças e adolescentes – já são devidamente regulados no Brasil por arcabouço jurídico (tanto legal quanto autorregulamentar). Nesse sentido, a regulação aplicável a bebidas alcoólicas no país pode fornecer subsídios úteis relativos a boas práticas e a técnicas para verificação de idade de usuários de plataformas digitais, tanto no que se refere ao acesso a determinadas plataformas e/ou conteúdos, como também à publicidade de determinados produtos e serviços.

O CBAP - Código Brasileiro de Autorregulamentação Publicitária e seus Anexos, editado pelo CONAR prevê a inclusão de mecanismo de acesso seletivo (age gate) nas plataformas dos próprios anunciantes e, em relação à plataforma de terceiros, exige que seja comprovada a audiência majoritariamente adulta para que haja a inserção de publicidade (Anexo A, P e T do CBAP).

Com relação especificamente aos mecanismos em si para verificação de idade de usuários de plataformas digitais, o recentíssimo *paper* da OCDE intitulado "*Towards digital safety by design for children*" (junho/2024) (disponível em <https://one.oecd.org/document/DSTI/CDEP(2023)13/FINAL/en/pdf>), no capítulo 6, traz subsídios interessantes sobre componentes que podem contribuir para o avanço da segurança digital pelo design para crianças – ressaltando que os diferentes componentes têm funções distintas, e que é improvável que a segurança digital para crianças seja atingida com uma única ação, mas sim por diversas ações combinadas.

Segundo o referido *paper*, os componentes podem ser agrupados em: (i) ferramentas práticas e recursos/decisões de design (como mecanismos de verificação de idade, proteções de privacidade etc.); (ii) medidas para criar um ambiente que promove e prioriza a segurança das crianças (por exemplo, promovendo uma cultura de segurança e de bem-estar); e (iii) redes de segurança concebidas para mitigar ou resolver danos, caso venham a ocorrer (i.e. mecanismos de reclamação e ferramentas técnicas para detectar danos).

No que tange aos mecanismos de verificação de idade, o referido *paper* destacou que experts sinalizaram como prioridades nesse tema que: (i) não deveriam ser usadas apenas para barrar crianças de serviços para adultos, mas, na medida do possível, devem ser usados para proporcionar experiências adequadas à idade; (ii) devem ser equitativos, inclusivos e devem refletir o risco; (iii) as leis e as regulações que preveem tais mecanismos devem ser tecnologicamente neutros, deixar espaço para a inovação, e não devem ser excessivamente prescritivos; e (iv) as soluções devem basear-se em

princípios, concentrando-se, por exemplo, na precisão, usabilidade, privacidade e proporcionalidade (cf. págs. 30-31).

Na prática, a verificação de idade pode se dar de diferentes formas, podendo se dividir entre mecanismos ou tecnologias que estimam a idade do usuário ou o range, ou que verificam a idade real do usuário, ou ainda aqueles que preveem um consenso parental verificado. Segundo o *paper*, há debates em curso sobre a precisão e a eficácia de cada mecanismo, sobre a facilidade de sua adoção pelos usuários, sobre a extensão em que podem preservar a privacidade, e sobre a melhor forma de equilibrar a necessidade de autonomia em desenvolvimento das crianças com a necessidade de qualquer envolvimento parental para fins de verificação etária. Além disso, à medida em que a legislação se desenvolve e diferentes jurisdições exigem mecanismos diferentes, podem surgir ambiguidades para os serviços e as plataformas online quanto aos mecanismos apropriados de verificação de idade que deverão utilizar. A proteção da privacidade adiciona uma camada de complexidade à verificação etária, visto que certos mecanismos necessitam de coleta significativa de dados para serem efetivos, como a biometria e o envio de documentos de identificação.

Nesses casos, segundo o *paper* da OCDE, os mecanismos deverão incorporar proteções de privacidade robustas, como princípios de minimização de dados para coletar e reter o mínimo de dados possível. Outra preocupação se refere ao risco de certos mecanismos serem enviesados contra determinados grupos étnicos, ou serem inacessíveis a determinadas comunidades marginalizadas que têm restrições de acesso digital e/ou a documentos de identificação. Nesse contexto, o uso combinado de métodos de verificação de idade poderia fornecer um nível mais elevado de confiança na efetividade e na privacidade, e reduzir o risco de discriminação de métodos usados de forma isolada. A ABA pondera, naturalmente, que se deve presumir a boa-fé das empresas ao tratarem dados de pessoas que informem ser maiores de idade (sem a necessidade de qualquer outro mecanismo de dupla verificação), desde que o conteúdo efetivamente não seja voltado a crianças e/ou adolescentes (por exemplo, em plataforma de e-commerce).

3) Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

A ABA pondera que já existe no país consolidada regulação que prevê um nível elevado de proteção e de segurança que deverá ser observado no tratamento de dados pessoais de crianças e de adolescentes – a citar:

(i) o **artigo 3º do ECA - Estatuto da Criança e do Adolescente (Lei nº 8.069/1990)** já prevê que a criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, bem como da proteção integral prevista na referida Lei. Além disso, o **artigo 100, parágrafo único, inciso V do ECA** prevê a "**privacidade**" como um dos princípios que regem a aplicação das medidas específicas de proteção à criança e ao adolescente, tendo especificado que *"a promoção dos direitos e proteção da criança e do*

adolescente deve ser efetuada no respeito pela intimidade, direito à imagem e reserva da sua vida privada".

(ii) o **artigo 14 da LGPD** já prevê, de forma específica e expressa, que "*o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado* ***em seu melhor interesse****, nos termos deste artigo e da legislação pertinente*". No mesmo sentido, o **Enunciado CD/ANPD nº 1/2023** reforçou a **prevalência do melhor interesse da criança e do adolescente** no tratamento de seus dados pessoais.

Além disso, a ABA ressalta que também já existe no país ampla regulamentação e autorregulamentação para a proteção da criança e para o marketing responsável, inclusive no ambiente digital. A LGPD traz regras que correspondem a mecanismos que coíbem qualquer tipo de abuso por parte de operadores e anunciantes em ambientes online acessíveis por crianças, ao mesmo tempo em que não prevê vedação ao tratamento de dados pessoais de crianças e adolescentes. Ou seja, pode haver tal tratamento, desde que com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, e não há vedação ao perfilamento, desde que autorizado pelos pais ou pelo responsável.

Como já mencionado anteriormente, Roberta Densa, em seu estudo elaborado à Senacon intitulado "Análise da publicidade e práticas comerciais destinadas às crianças e adolescentes e suas limitações pelo ordenamento jurídico brasileiro e no direito comparado", ao comentar o direito comparado sobre a mesma temática, reforça que a regulação norte-americana do COPPA exige o consentimento dos pais para a coleta dos dados pessoais da criança (págs. 284-285 do estudo). Essa exigência está alinhada com as disposições do art. 14 da LGPD, que também impõe a necessidade de consentimento específico dos pais ou responsáveis para o tratamento de dados pessoais infantis.

Com efeito, com relação ao direcionamento de publicidade a crianças e adolescentes, observando o núcleo de liberdades constitucionais, o CDC – Código de Defesa do Consumidor (Lei nº 8.078/90) também admitiu a publicidade a crianças e adolescentes - seja ela em meio audiovisual ou digital – proibindo, naturalmente, qualquer abuso na comunicação. Em mais detalhes:

(i) O CDC traz importante proteção às crianças ao estabelecer o princípio da **identificação da mensagem publicitária** (art. 36, CDC), protegendo-se as crianças de publicidades "ocultas", regra que se aplica integralmente ao ambiente digital. A mesma regra é prevista no art. 9 e 28 do CPAB e fiscalizada regularmente pelo CONAR. Ademais, o CONAR publicou o Guia de Influenciadores, aportando ao mercado novas orientações para o marketing responsável no ambiente digital. Referido Guia estabeleceu, em seu item 1.1.2, regra específica para que, na publicidade realizada por influenciador, haja cuidado redobrado e aprimoramento por todos os envolvidos na sua divulgação quando envolver crianças e adolescentes, devendo ser perceptível o seu intento comercial e destacada a distinção da publicidade em relação aos demais conteúdos gerados pelo influenciador.

(ii) O artigo 37, § 2º do CDC proíbe a publicidade que explorar a deficiência de julgamento e experiência da criança, a ser analisado caso a caso. As mesmas regras estão previstas nos artigos 27, 33 e 37do CBAP do CONAR.

O ECA, por seu turno, protege a criança e o adolescente contra o conteúdo inadequado da publicidade, devendo ser respeitada a sua "condição peculiar de pessoa em desenvolvimento". (art. 71, ECA).

Isso significa que, de acordo com a legislação já vigente e aplicável, qualquer coleta e tratamento de dados pessoais deve ser compatível a idade da criança e do adolescente (não podendo haver direcionamento não autorizado ou incompatível com seu melhor interesse) e não gerar pedido de informações adicionais além do estritamente necessário.

4) Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

A ABA ressalta, de início, que os pais precisam de apoio para ajudar os seus filhos a navegar no mundo digital, e que as próprias crianças devem ser consultadas e reconhecidas como principais partes interessadas e titulares de direitos individuais no desenvolvimento de políticas – conforme revelou trabalho conduzido pela OCDE em 2020.

Do ponto de vista regulatório, uma forma de incorporar a participação dos pais e dos responsáveis seria através de disposições legais sobre o tema, quando necessárias. Nesse sentido, por exemplo, o Senado Francês aprovou uma lei que exige que as plataformas de redes sociais implementem sistemas de verificação de idade e procurem o consentimento explícito dos pais para usuários com 15 anos ou menos. Além disso, previu, dentre outros pontos, que as plataformas de redes sociais são obrigadas a instalar funções que limitem o tempo de utilização das crianças e deem aos pais o direito de suspender contas pertencentes a crianças menores de 15 anos.

Para além da esfera regulatória, há exemplos concretos de empresas que incorporaram um design centrado em crianças – mas com o suporte dos pais e dos responsáveis – no desenvolvimento de aplicativos, citados no paper da OCDE intitulado "*Towards digital safety by design for children*" (junho/2024).

Por exemplo, o aplicativo da LEGO chamado *LEGO's Life App* prevê a capacidade de os pais e tutores monitorarem o uso do app pelos seus filhos. A plataforma *Roblox* (que é uma plataforma de criação de jogos que permite aos usuários desenvolverem seus próprios jogos e a jogar os games criados por outros usuários), por sua vez, oferece dentre as ferramentas de segurança o suporte aos pais e uma variedade de ferramentas de segurança online para proteger seus filhos – o que inclui orientações para os pais explicando os controles parentais que podem ser usados por usuários muito jovens. Além disso, a *Roblox* encoraja os pais a ajudarem os seus filhos a tomarem decisões responsáveis sem se apoiarem no uso extensivo de controle parental.

Os mecanismos acima mencionados são exemplos de formas de incluir os pais e os responsáveis no processo de inclusão das crianças e dos adolescentes no ambiente digital. Nesse sentido, a ABA pondera que o objetivo não deveria propriamente ser ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital, mas talvez aperfeiçoar os controles já existentes e previstos, divulga-los ostensivamente, e complementá-los também com ações de conscientização, com ênfase na educação prévia dos usuários da rede.

5) Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

A OCDE, no *paper* intitulado "*Towards digital safety by design for children*" (junho/2024), concluiu que há diversas características de uma abordagem mais focada na segurança pelo design (das plataformas/dos produtos/dos serviços) que poderiam ser aplicadas no contexto de segurança digital pelo design para crianças e adolescentes, tais como:

(i) a incorporação de abordagens proativas que podem identificar e abordar vulnerabilidades antes que elas surjam e prejudiquem as crianças;

(ii) gestão de riscos contínua e dinâmica, como a incorporação de processos para encontrar e resolver problemas de segurança que surgem a despeito da adoção de abordagens proativas – o que poderia envolver uma avaliação regular dos riscos;

(iii) design (das plataformas/dos produtos/dos serviços) centrado no usuário, por exemplo, pelo fornecimento de informações adaptadas às crianças e que considere aa adequação à idade;

(iv) a responsabilização (*accountability*), que é essencial para a segurança digital, deve exigir a atribuição de responsabilidades dentre as equipes de design e de desenvolvimento, mas também a promoção de uma mentalidade em toda a empresa, incluindo nos mais altos níveis executivos;

(v) a transparência, que no contexto da segurança digital pelo design, envolve informações transparentes sobre riscos, danos reais que já ocorreram nos serviços e ações que estão sendo tomadas para lidar com qualquer risco ou dano.

Especificamente quanto à transparência, o documento da OCDE intitulado "*OECD Guidelines for Digital Service Providers*" (2021), elaborado no contexto da revisão do "*OECD Recommendation of the Council on Children in the Digital Environment*", pode fornecer subsídios interessantes para discussão. As diretrizes da OCDE acima mencionadas dispõem que *"[a]o fornecer informações às crianças e aos seus pais, tutores ou cuidadores sobre serviços para crianças, ou quando for razoavelmente previsível que serão acedidos ou utilizados por crianças, os prestadores de serviços digitais devem fornecer informações* ***concisas, inteligíveis, facilmente acessíveis e formulado em linguagem clara, simples e apropriada à idade****. Isto inclui, mas não está limitado a informações sobre configurações de privacidade, retenção de dados, termos de serviço, políticas e padrões da comunidade*."

6) Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

A ABA acredita já ter apresentado as suas principais considerações ao longo desta manifestação e permanece à disposição para quaisquer dúvidas e esclarecimentos adicionais, ao tempo em que congratula novamente a Ilma. ANPD pelo diálogo ativo e aberto com a sociedade, e pela busca contínua pelo aprimoramento regulatório que o Órgão tem demonstrado na condução de suas atividades.

* * *

Brasília, 16 de agosto de 2024.

À Autoridade Nacional de Proteção de Dados - ANPD

Assunto: Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT) à Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes.

A **Associação Brasileira de Emissoras de Rádio e Televisão – ABERT,** fundada em 27 de novembro de 1962, é uma sociedade civil sem fins econômicos, de duração indeterminada, constituída por empresas de radiodifusão autorizadas a funcionar no País. Tem como principal objetivo a defesa da liberdade de expressão, em todas as suas formas, bem como dos interesses das emissoras de radiodifusão, suas prerrogativas como executoras de serviços de interesse público, assim como seus direitos e garantias.

Na visão da entidade, os seguintes pontos merecem especial atenção, de forma a aperfeiçoar a minuta de regulação proposta:

I - Princípio do melhor interesse

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

O Enunciado CD/ANPD nº 01/2023 deixa claro que a verificação do melhor interesse da criança e do adolescente depende de uma avaliação de cada caso concreto, não sendo possível estabelecer, de antemão, requisitos excessivamente pormenorizados a serem atendidos em toda e qualquer atividade de tratamento.

> O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (lgpd), **desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto**, nos termos do art. 14 da Lei.

No mesmo sentido, o Comentário Geral nº 14, de 2013, do Comitê de Direitos da Criança da ONU, afirma que o "*interesse maior*" da criança abrange (i) um direito, (ii) um princípio jurídico fundamental interpretativo e (iii) uma regra processual. Nota-se, novamente, a existência de uma tomada de decisão diante de situações concretas, a partir de um exercício de interpretação balizado por regras que evitem abusos, protegendo os diretos das crianças e adolescentes, sem, contudo, que se considere a criação de um arcabouço regulatório minucioso e exaustivo.

Tal abordagem revela-se equilibrada, na medida em que dá contornos concretos ao conceito, ou, em verdade, ao princípio do melhor interesse, segundo o qual se deve proteger o menor; sem, porém, impedi-lo de participar da vida em sociedade e desfrutar, com isto, de oportunidades de desenvolvimento. A superproteção dos jovens pode, caso adotada, impedi-los de desenvolver capacidades valorosas. Nesse sentido, é o relatório da UNICEF "*Crescendo em um mundo conectado: compreendendo riscos e oportunidades para crianças na era digita*l", publicado em novembro de 2019.

O documento constata que os menores de idade que participam de mais atividades *online* possuem mais habilidades digitais do que aqueles que têm menor participação; e, além disto, que menores com pais menos restritivos têm mais chances de se envolverem em atividades *online*, não apenas jogando games ou assistindo vídeos, mas também participando de atividades que desenvolvam sua criatividade e curiosidade por novos conhecimentos. Dessa forma, a UNICEF aconselha pais e responsáveis a facilitar o uso da internet pelos menores, auxiliando-os a aprender e se desenvolver nesse meio.

Ainda de acordo com o mesmo documento, "*é importante ter em mente que o risco nem sempre conduz a danos. Crianças expostas a riscos online podem não sofrer danos se tiverem conhecimentos e resiliência para lidar com a experiência*". Portanto, proteger as crianças e os adolescentes e garantir seu melhor interesse não significa limitar suas oportunidades de consumir e produzir conteúdo, bem como informar-se e expressar-se no mundo digital.

O relatório conclui que legisladores e reguladores devem adotar uma abordagem equilibrada e integrada no que se refere à regulamentação do uso da internet por menores de idade, de forma a reduzir os riscos aos quais esse grupo é submetido, mas sem limitar, como já mencionado, as oportunidades positivas para seu desenvolvimento presentes no mundo digital.

Nesse contexto, o Guia orientativo publicado por esta r. ANPD sobre o tratamento de dados pessoais a partir da base legal do legítimo interesse, especificamente no que diz respeito ao tratamento de dados de crianças e adolescentes, traz orientações e procedimentos suficientemente claros, que evitam a violação de direitos e permitem um exame detalhado das situações enfrentadas por cada agente de tratamento. O Guia dispõe que o tratamento deve se limitar ao mínimo necessário, atendendo a finalidade pretendida, adotando, ainda, medidas de transparência adequadas e compatíveis com a condição de crianças e adolescentes dos titulares, conforme art. 14, §6º, LGPD. Como exemplo, é apresentada situação hipotética em que uma escola coleta dados pessoais de estudantes para habilitar acesso à rede wi-fi. Enquanto se avalia a necessidade de obtenção de consentimento de responsáveis legais, o Guia apresenta a hipótese do legítimo interesse como opção para fundamentação legal, em que pese a necessidade de se realizar o teste de balanceamento, conforme disposto no próprio Guia.

Referido Guia não difere, tampouco se revela menos denso que as normas complementares ao Regulamento Geral de Proteção de Dados Europeu (ou GDPR), norma matriz da Lei Geral de Proteção de Dados, nem de sua versão publicada no Reino Unido. O GDPR, por exemplo, dispõe a necessidade de que avisos de privacidade aplicados a pessoas maiores de 13 anos devem ser claros e adequados à idade, de forma transparente para que possam compreender os termos com os quais passam a concordar.

Além disto, deve-se ter em mente que a ANPD sempre poderá estabelecer restrições específicas ao tratamento de dados pessoais de crianças e adolescentes a partir de suas decisões em casos concretos, de modo que, ao deixar de estabelecer, em norma, comandos gerais e abstratos pormenorizados, não estará eliminando a possibilidade de intervir de forma mais minuciosa

quando necessário, fixando precedentes importantes que certamente terão repercussão sobre a conduta dos agentes regulados.

Diante do exposto, a ABERT entende que o aumento da densidade normativa, a partir da instituição de mais instruções e comandos em sede da regulamentação, tende a exceder o grau indicado no Comentário Geral nº 14 da ONU e refletido no próprio Enunciado nº 01/2023 do Conselho Diretor desta própria ANPD, atuando contra o melhor interesse de crianças e adolescentes.

Contribuição completa segue por e-mail.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

Como mencionado por ocasião da resposta à primeira questão, o tratamento dos dados pessoais é necessário para que crianças e adolescentes possam ter acesso a serviços que lhes permitem se entreter, aprender e, enfim, interagir no mundo *online* e fora dele. Alguns desses serviços trazem, sim, maiores riscos, a serem considerados diante do melhor interesse de crianças e adolescentes. A ANPD caminhou no sentido de estabelecer que o tratamento de dados pessoais de crianças e adolescentes deve ser enquadrado, em termos práticos, como de alto risco, impondo aos agentes de tratamento a necessidade de elaboração de relatório de impacto, a partir do qual deverão avaliar "*riscos específicos para esse público e as salvaguardas e medidas de segurança que deverão ser implementadas para as mitigações apropriadas*" (*v.* o Guia Orientativo voltado ao legítimo interesse). A posição brasileira é até mais estrita do que a adotada no continente europeu e no Reino Unido (v. as recomendações do European Data Protection Board, disponíveis em https://ec.europa.eu/newsroom/article29/items/611236), uma vez que, por lá, o tratamento de dados de crianças e adolescentes não é considerado, por si, um tratamento de alto risco e os critérios adicionais a serem preenchidos para que passe a ser são mais específicos e, portanto, menos presentes nas diversas atividades de tratamento a serem analisadas.

Ao tornar a elaboração de relatório de impacto à proteção de dados pessoais uma rotina obrigatória para os agentes que tratem dados pessoais de crianças e adolescentes, a ANPD dá um impulso importante para que o melhor interesse de crianças e adolescentes seja preservado, na medida em que faz recair sobre tais agentes o ônus de indicar quais riscos são causados pelas atividades de tratamento que tem em vista e quais as medidas de mitigação desses riscos identificados estão sendo adotadas, tanto do ponto de vista da segurança de dados quanto da transparência das informações repassadas aos titulares ou a seus responsáveis.

Nesse contexto, o guia orientativo sobre a hipótese de tratamento fundada em legítimo interesse e o guia orientativo sobre tratamento de dados pessoais de alto risco são plataformas importantes para que a ANPD continue a abordar situações que demandem maior rigor dos agentes de tratamento; e ambos os documentos já avançaram bastante nesse sentido (ainda que o segundo esteja em fase final de elaboração).

Para além disto, é também necessário que se tenha em vista que a proteção ao melhor interesse não está ancorada apenas na legislação de proteção de dados, nem poderia estar, na medida em que a proteção integral de crianças e adolescentes demanda uma atenção muito mais abrangente.

Nesse sentido, são as leis e regulamentos que dispõem sobre o acesso de crianças e adolescentes a certos serviços e a conteúdos, disponíveis *online* ou na parte de nossas vidas que ainda resta

‘*desconectada*’, como o Estatuto da Criança e do Adolescente e as normas sobre classificação indicativa. Tais normas estão além da LGPD e precedem-na em uma cadeia de barreiras jurídicas de proteção.

A partir dos mecanismos de controle parental e da própria orientação conferida aos pais a partir da classificação indicativa, associadas da ABERT têm conseguido balizar o acesso a seus serviços (sejam aplicações de *streaming* ou sites acessíveis por *navegadores*) sem a devida autorização e supervisão dos responsáveis por crianças e adolescentes, evitando, em grande parte, o tratamento de dados desses menores de forma contrária a seu melhor interesse. Nota-se, portanto, que nem sempre a realização do melhor interesse dos menores demandará inovações na regulamentação lastreada na LGPD, mas, sim, em outras formas de intervenção, amparadas em outras instâncias estatais e na própria família.

É inegável, contudo, que existem campos para avanços no que diz respeito a outros serviços, como redes sociais, cada vez mais populares entre crianças e adolescentes. Ainda que a regulação de contorno desses serviços esteja por vir, é evidente que a regulamentação ligada à legislação de proteção dos dados pessoais se fará, como já se faz, de suma importância. Nessa seara, a implementação de mecanismos de validação da maioridade do responsável indicado para abertura de contas por menores em tais aplicações desponta como uma medida de proteção proporcional e que deveria ser considerada pela ANPD como parte de sua avaliação dos cuidados tomados por agentes de tratamento no sentido da concretização do melhor interesse de crianças e adolescentes.

Contribuição completa segue por e-mail.

II - Consentimento

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento “específico e em destaque” de pais ou responsáveis legais?

O consentimento, para adolescentes compreendidos na faixa etária entre 12 e 16 anos, deve ser concedido por meio de acesso à página exclusivamente voltada para este fim, de modo que as pessoas diretamente interessadas, notadamente o menor titular de dados e seus pais ou responsáveis possam reconhecer sua finalidade, não restando dúvidas sobre (i) o que se trata aquela solicitação e (ii) para qual finalidade o consentimento está sendo solicitado. A página que solicitará o consentimento deverá apresentar características destacadas das demais, que ressaltem a finalidade daquela requisição. Por também ser direcionada a pessoa menor, a página deve apresentar linguagem simples, clara e acessível a este público, afastando-se de rebuscamentos da linguagem jurídica eminentemente técnica.

Deve-se considerar, ainda, as regras gerais, pelas quais essa solicitação de consentimento seja limitada pela (i) minimização de dados estritamente necessários ao tratamento; (ii) exclusiva finalidade pretendida – obtenção do consentimento dos pais ou responsáveis e (iii) transparência das informações, adequada e compatível ao público-alvo daquela solicitação.

Por fim, a solicitação de consentimento deve ser acompanhada da respectiva política de privacidade.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de “todos os esforços razoáveis”, quais medidas e mecanismos os

controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

Não há dúvidas que a viabilização e a verificação do consentimento de pais ou responsáveis por crianças e adolescentes devem se orientar pelos princípios que norteiam o tratamento de dados pessoais, conforme a LGPD, recebendo especial atenção o princípio da necessidade, pelo qual é limitado o tratamento "*ao mínimo necessário para a realização de suas finalidades*". Por sua vez, o princípio da necessidade deve ser analisado dentro de parâmetros do que é razoável e proporcional, de modo que eventual tratamento, ainda que sob o fundamento de manutenção do melhor interesse da criança, seja realizado sem excessos, restringindo-se ao estritamente necessário para determinada finalidade.

Isso posto, entende-se que ao controlador devem ser facultadas diferentes alternativas para a verificação (i) da idade do titular de dados, assim como (ii) da identidade dos pais ou responsáveis. Essa medida tem como fundamento a conjunção do resguardo dos direitos de crianças e adolescentes, ao mesmo tempo em que proporciona ao controlador a possibilidade de identificar o mecanismo mais adequado, dentro de seu contexto comercial e suas limitações operacionais, sem que incorra em uma coleta de dados pessoais excessiva.

Nesse contexto, dentre as diversas alternativas possíveis, são sugeridas as seguintes, tendo em vista atingirem a finalidade esperada, sem que excedam aos limites razoáveis de tratamento de dados: (i) no caso da oferta de produtos e serviços digitais gratuitos, a verificação poderá ser realizada a partir da confirmação da validade do CPF e se pertence à pessoa maior de idade (ii) no caso de oferta de produtos e serviços digitais pagos, a verificação estará condicionada ao método de pagamento escolhido, sendo automaticamente notificado seu titular, reconhecido como pessoa em plena capacidade civil.

Admitindo-se somente a título de argumentação, verifica-se que eventual confirmação por meio de chamada de vídeo ou mesmo a obrigação de encaminhamento de fotografia dos pais ou responsáveis apresentando documento de identificação civil, além de não se conformarem diante da minimização de dados pessoais, seriam desproporcionais, uma vez que resultariam em uma coleta excessiva de dados pessoais – desnecessária para os fins pretendidos – além de onerar demasiadamente os controladores a partir de obrigação que demandará altos investimentos para a garantia da segurança da operação.

Essas sugestões são apresentadas dentro de uma análise sistêmica que considera, principalmente, o melhor interesse da criança e do adolescente – como priorizado no "Manifesto por uma melhor governança de dados de crianças", publicado pelo Fundo das Nações Unidas para a Infância (UNICEF)" -, uma vez que são propostas medidas para resguardar seus direitos, ao tempo em que não são criados empecilhos à participação na vida digital. Dessa forma, são concedidas novas oportunidades positivas de desenvolvimento dessas pessoas no mundo digital.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

A autonomia progressiva dos adolescentes titulares de dados deve ser respeitada também em alinhamento com o seu melhor interesse, como disposto no art. 14, caput, da LGPD. Nesse contexto, faz-se necessário considerar, para a análise mais adequada desse cenário, o disposto no Enunciado nº 692 da IX Jornada de Direito Civil, pelo qual é ratificado que os conceitos de criança e adolescente, dispostos no art. 14, da LGPD, devem ser interpretados à luz do art. 2º, do ECA. Assim, para as matérias atinentes à proteção de dados pessoais, serão consideradas adolescentes todas as pessoas entre 12 anos completos e 18 anos incompletos, possuindo aquelas a partir de 16 anos capacidade para conceder seu consentimento no tratamento de dados pessoais, o que, por sua vez, relativiza os regimes de capacidade dispostos no Código Civil brasileiro.

Conforme justificativa do Enunciado nº 692, a LGPD, então, "reconhece a redução gradual da autoridade parental face ao amadurecimento do menor", principalmente diante de sua inserção digital precoce, ficando sedimentado o entendimento de que "à medida do crescimento, o adolescente adquire paulatinamente a capacidade de discernir e decidir, devendo ser respeitada a dimensão da responsabilidade consequente do ato a ser praticado".

Ainda sob essa perspectiva, há de se ressaltar que a desnecessidade de um consentimento por parte de pais e responsáveis, principalmente nos casos de adolescentes a partir dos 16 anos, revela-se como medida para incentivo à fluidez na utilização dos meios digitais, visto que, em diversas oportunidades, esse consentimento é realizado como mera formalidade para permitir o uso por adolescentes. Em linhas gerais, dispensar o consentimento, nesses casos, configura-se como medida de desburocratização para a interação desses jovens com as plataformas.

Reconhecendo a interpretação trazida pelo ECA, ao tempo em que se resguarda a autonomia progressiva, é importante verificar que essa não é uma política exclusiva brasileira, vez que, por exemplo, tanto os Estados Unidos da América, Reino Unido quanto a União Europeia autorizam que o adolescente, a partir de seus 13 anos, conceda seu consentimento sem a necessidade de uma assistência ou representação.

Nessa esteira, valemo-nos do Comentário Geral nº 25 da Organização das Nações Unidas sobre os Direitos das Crianças em Relação ao Ambiente Digital, pelo qual é reiterada a importância do desenvolvimento progressivo, enquanto um princípio que permite a pessoa menor adquirir competências e compreender suas ações e suas consequências no meio digital, dentro de seus limites de responsabilidade. Como observado, dentro desta gradação estabelecida, a partir do amadurecimento, a decisões tomadas por adolescentes passam a prescindir de assistência ou representação.

Portanto, conciliando o melhor interesse com a autonomia progressiva, ao tempo em que se garante um desenvolvimento maior de sua autonomia, ao adolescente também é permitido o acesso aos meios digitais em suas expressões mais tecnológicas e modernas, sendo ofertados espaços de acesso à cultura, educação e informação, por exemplo.

III - Jogos e aplicações de internet

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Como mencionado na resposta à questão II.2, é necessário que se tenha em vista que a concretização do melhor interesse de crianças e adolescentes não está ancorada apenas na legislação de privacidade e proteção de dados, nem poderia estar, na medida em que sua proteção integral demanda uma atenção muito mais abrangente. Nesse sentido, leis e regulamentos que dispõem sobre o acesso de crianças e adolescentes a certos serviços e a conteúdos, como o ECA e as normas sobre classificação indicativa, são parte importante desse sistema mais amplo de salvaguardas. Tais normas estão além da LGPD e precedem-na em uma cadeia de barreiras jurídicas de proteção. No caso específico de jogos eletrônicos e aplicações *streaming*, são oferecidos mecanismos personalizáveis de controle parental, além do "modo infantil", em que grande parte do catálogo de conteúdos deixa de ser disponibilizado, tomando por base que uma criança estará diante da tela. Todas essas medidas acabam contribuindo para que se evite um acesso indevido a determinados serviços e conteúdo e, por conseguinte, para que atividades de tratamento de dados sejam evitadas, senão em absoluto, mas em grande parte.

Ainda que a regulamentação e as orientações apoiadas na LGPD não sejam capazes de disciplinar propriamente as condições de acesso de crianças e adolescentes a serviços e conteúdos *online*, elas podem ser de grande valia ao disporem sobre as medidas de transparência a serem adotadas na comunicação com menores e seus responsáveis, bem como nos mecanismos de verificação da maioridade daqueles que validam a criação de contas junto aos provedores desses serviços e conteúdos. A esse passo, vale lembrar que o controlador deve ter diferentes alternativas para a verificação (i) da idade do titular de dados, assim como (ii) da validade do CPF indicado que pertença à pessoa maior de idade de modo a que se conjugue a proteção dos direitos de crianças e adolescentes, ao mesmo tempo em que proporcione ao controlador a possibilidade de identificar o mecanismo mais adequado, dentro de seu contexto comercial e suas limitações operacionais, sem que incorra em uma coleta de dados pessoais excessiva. Mais destalhes a esse respeito seguem na resposta à questão II.2.

Enquanto jogos eletrônicos e aplicações de *streaming* incorporam avanços significativos no sentido de controle parental e verificação da maioridade daqueles que se apresentam como responsáveis por crianças e adolescentes, existem campos para avanços no que diz respeito a outros serviços, como redes sociais, cada vez mais populares entre crianças e adolescentes. Nessa seara, a implementação de tais mecanismos desponta como uma medida de proteção proporcional e que deveria ser considerada pela ANPD como parte de sua avaliação dos cuidados tomados por agentes de tratamento no sentido da concretização do melhor interesse de crianças e adolescentes.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

Conforme exposto na resposta à questão II.2, entende-se que ao controlador devem ser facultadas diferentes alternativas para a verificação (i) da idade do titular de dados, assim como (ii) da validade do CPF indicado que pertença à pessoa maior de idade. Essa medida tem como fundamento a conjunção do resguardo dos direitos de crianças e adolescentes, ao mesmo tempo em que proporciona ao controlador a possibilidade de identificar o mecanismo mais adequado, dentro de seu contexto comercial e suas limitações operacionais, sem que incorra em uma coleta de dados pessoais excessiva.

Nesse contexto, dentre as diversas alternativas possíveis, são sugeridas as seguintes, tendo em vista atingirem a finalidade esperada, sem que excedam aos limites razoáveis de tratamento de dados: (i) no caso da oferta de produtos e serviços digitais gratuitos, a verificação poderá ser

realizada a partir da confirmação da validade do CPF a ser indicado no ato de solicitação de acesso e se o CPF pertence à pessoa maior de idade; (ii) no caso de oferta de produtos e serviços digitais pagos, a verificação estará condicionada ao método de pagamento escolhido, sendo automaticamente notificado seu titular, reconhecido como pessoa em plena capacidade civil.

Admitindo-se somente a título de argumentação, verifica-se que eventual confirmação por meio de chamada de vídeo ou mesmo a obrigação de encaminhamento de fotografia dos pais ou responsáveis apresentando documento de identificação civil, além de não se conformarem diante da minimização de dados pessoais, seriam desproporcionais, uma vez que resultariam em uma coleta excessiva de dados pessoais – desnecessária para os fins pretendidos – além de onerar demasiadamente os controladores a partir de obrigação que demandará altos investimentos para a garantia da segurança da operação.

Essas sugestões são apresentadas dentro de uma análise sistêmica que considera, principalmente, o melhor interesse da criança e do adolescente – como priorizado no "Manifesto por uma melhor governança de dados de crianças", publicado pelo Fundo das Nações Unidas para a Infância (UNICEF)" -, uma vez que são propostas medidas para resguardar seus direitos, ao tempo em que não são criados empecilhos à participação na vida digital. Dessa forma, são concedidas novas oportunidades positivas de desenvolvimento dessas pessoas no mundo digital.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

Sem contribuições.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

A comunicação transparente com os próprios pais e responsáveis é o primeiro mecanismo a assegurar a proteção dos menores sob sua tutela. Em segundo lugar, mecanismos de validação da maioridade do responsável, tratados ao longo das respostas às demais questões, são de suma importância para que se tenha certeza de que o agente de tratamento está estabelecendo um diálogo com um indivíduo capaz de efetivamente responder por crianças e adolescentes.

Adicionalmente, pais e responsáveis devem ter ao seu alcance, nos casos em que se revelar possível, mecanismos de supervisão, como escolha de conteúdo e funcionalidades a serem acessadas em aplicações, relatórios sobre as atividades de seus filhos, entre outras, sempre tendo em vista os limites técnico-operacionais de cada serviço e a regulação específica de cada setor de atividade econômica, que, em alguns casos, já terá disciplinado de forma competente a matéria, notadamente no que diz respeito à adoção de medidas de controle e supervisão.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Com demonstrado na resposta às questões anteriores, um dos principais vetores para a concretização do melhor interesse de crianças e adolescentes é a comunicação de forma

transparente e apropriada com os pais e responsáveis legais. Eles devem ter ao seu alcance informações claras sobre as atividades conduzidas pelos agentes de tratamento e, para além disto, nos casos em que se revelar possível, mecanismos de supervisão, como escolha de conteúdo e funcionalidades a serem acessadas em aplicações, relatórios sobre as atividades de seus filhos, entre outras. No entanto, é crucial que a ANPD considere os limites técnicos dos diversos serviços, e como já exposto, a regulação específica de cada setor de atividade econômica, que, em muitas das vezes, já tratará sobre o fornecimento de informações a pais e responsáveis e a implementação de medidas de controle e supervisão.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

Sem contribuições.

***

Contribuições à Tomada de Subsídios ANPD: Tratamento de Dados Pessoais de Crianças e Adolescentes

Sistema ABRAMGE/SINAMGE/SINOG/UCA

Venho, em nome da Associação Brasileira de Planos de Saúde - ABRAMGE e da Associação Brasileira de Planos Odontológicos - SINOG, na figura de sua Advogada e Encarregada de Proteção de Dados, parabenizar esta autoridade pela condução do tema por intermédio de Tomada de Subsídios, possibilitando à sociedade a participação na construção e maturação da cultura de proteção de dados no Brasil, e também pela importância dada ao tema, a ponto de deliberarem pela aprovação de concessão de prazo adicional para participação social.

Primeiramente, cabe mencionar que o setor de saúde e odontologia suplementares, especialmente as associadas das entidades ABRAMGE e SINOG, acompanha de perto as atividades desta autoridade, sempre que possível contribuindo com as participações sociais propostas pela ANPD, com a ajuda das construções advindas de Grupo de Trabalho sobre Privacidade e Proteção de Dados.

Deste modo, aproveitamos a oportunidade concedida para destacar os principais pontos de preocupação deste setor em relação ao assunto em referência, com foco nas necessidades da operação junto aos titulares de dados pessoais, conforme expomos a seguir.

---

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Tendo em vista que o Enunciado autoriza que o tratamento de dados pessoais de crianças e adolescentes seja realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, há a necessidade de tonar a redação clara sobre a aplicabilidade de umas das hipóteses legais previstas nos referidos artigos, além de tornar mais clara também o melhor interesse do titular nessas hipóteses.

Com relação ao artigo 14, poderia ser excluído, por consequência, a autorização (consentimento) de um dos pais ou responsável legal, como ocorre com os demais tratamentos de dados quando cabe uma das hipóteses legais, com a observância em todos os casos do melhor interesse da criança.

Ainda, com relação ao melhor interesse da criança, cabe à ANPD tonar os critérios mais objetivos ou fazer referência ao que já constam na própria legislação pátria, como os direitos constitucionais, direitos previstos no ECA e demais normas relacionadas existentes e aplicáveis a cada caso concreto.

Além disso, no que tange a jogos de azar, apostas e jogos eletrônicos no geral (com compras dentro do próprio jogo); publicidade, marketing e personalização; inteligência artificial, sendo este rol não taxativo, há a necessidade de uma regulamentação específica.

Associação Brasileira de Planos de Saúde – ABRAMGE
Associação Brasileira de Planos Odontológicos – SINOG
Camila Castioni| advogada e DPO |lgpdsistema@abramge.com.br
Rua Treze de Maio, 1540, Bela Vista, São Paulo – SP

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

Sim, embora jogos de azar sejam proibidos para menores de idade, os bloqueios não são recorrentes e eficientes. A Lei nº 14.852/2024, que cria o marco legal para a indústria de jogos eletrônicos, menciona em seu capítulo III a proteção das crianças e dos adolescentes. Há a promoção de sistemas mínimos de salvaguardas aos direitos e restrição a transações comerciais, porém, não há manual prático no que tange a proteção de dados destes menores.

Sobre publicidade, marketing e personalização, embora existam resoluções do Conselho Nacional de Autorregulamentação Publicitária (Conar), do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda), dentre outros, entende-se por orientação de boas práticas e supervisão pela ANPD.

Há de se dar especial atenção também, as situações em que há tratamento de categorias de dados de crianças e adolescentes em grande escala ou sem finalidade determinada (em excesso), por ser considerado alto risco, considerando cada tipo de tratamento de dado envolvendo alta escala de dados do mesmo indivíduo (criança/adolescente) e em cada caso concreto, não considerando a operação do agente de tratamento em si.

Em relação à inteligência artificial, deve-se aguardar o Projeto de Lei nº 2.338/2023 para eventual futura regulamentação por parte da ANPD.

II - Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

Para que o consentimento seja específico e em destaque, antes do aceite, deve ser explicado cada ponto do termo. Se em aplicativo, pode ser acompanhado através de áudio de leitura, o termo deve ser completo na tela, de fácil escrita e contendo exemplos e demais informações pertinentes, sem se apegar ao "*juridiquês*", outras possibilidades seriam o consentimento conter os dados mínimos da criança e do autorizador e ocorrer a validação por token ou login/senha, ou ainda de forma manual, através documento privado, e não necessariamente público, assinado pelo representante com o seu reconhecimento de firma.

Caso não seja cliente, deve ser realizado contato telefônico e/ou fornecido token para validação pelo responsável legal.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

Considerando as boas práticas, a forma mais prática e célere de viabilizar o consentimento dos pais seria através de biometria facial. A biometria deve ser validada através do envio de cópia de documento que comprove o relacionamento parental, por exemplo, a identidade do responsável e do menor, a certidão de nascimento com a indicação dos pais ou certidão judicial, com a indicação do tutor.

Caso o pai/responsável legal já tenha relação jurídica com a empresa, basta a indicação da informação, sem a apresentação de documentos adicionais.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

O consentimento previsto na LGPD (artigo 14) faz referência apenas a dados pessoais de crianças, ou seja, até 12 anos incompletos (ECA). Para os adolescentes, de acordo com a LGPD, tal consentimento não se faz obrigatório, o que deve ser descartado.

Entretanto, não podemos confundir a autorização de pais e responsáveis considerando as regras gerais aplicáveis no ordenamento jurídico para os atos da vida civil, disponíveis no Código Civil. Tais regramentos são aplicáveis para as pessoas com idade inferior a 18 anos, que possuem a capacidade civil reduzida para os atos da vida civil, o que inclui relacionamento jurídico/negocial desta pessoa natural com uma empresa jurídica em ambiente digital, que pode ter por via transversa o tratamento de dados.

O artigo 5º do Código Civil traz, em seu parágrafo único, as possibilidades, para o menor, de ser cessada a incapacidade. Entende-se que, embora a previsão legal para cessar a incapacidade, os direitos daquele adolescente continuam protegidos pelo ECA, bem como a proteção ao melhor interesse. E, neste sentido, a proteção à privacidade e aos seus dados continuará vigorando de forma mais protetiva.

Apesar disso, como forma de viabilizar o consentimento – seja aceite, seja recusa – se faz necessário entender a realidade fática para que seja gerada a exceção. Nos casos, por exemplo, da concessão pelos pais ou do casamento (incisos I e II, art. 5º, CC), é possível que a pessoa, agora capaz, não esteja geograficamente próxima de seu outrora responsável legal. Portanto, obrigar a manter o consentimento dado pelos pais pode inviabilizar um consentimento que, se dado, pode ser favorável àquela pessoa e inferir em outras proteções e direitos elencados no ECA. Neste sentido, um estudo específico poderá ser realizado.

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo

necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações "estritamente necessárias à atividade".

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de *design*, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Devem ser observados os princípios relacionados a respeito à segurança; direitos individuais; qualidade dos dados; transparência; coleta, uso e retenção; compartilhamento e transferências internacionais seguras; responsabilização e prestação de contas.

Análise da ferramenta por parte de T.I., arquitetura de dados, engenharia de segurança da informação, governança de dados e obrigatoriedade de manutenção dos documentos de homologação por período de vigência do contrato + 5 anos após rescisão contratual. Além disto,

avaliação de cláusulas contratuais e análises de risco vinculadas ao mapeamento de dados. Todos os documentos poderão ser solicitados para análise da ANPD.

Em resumo, as plataformas digitais voltadas exclusivamente para o público em referência poderão conter termos de uso e políticas redigidas de forma clara e didática, a fim de orientar o usuário da plataforma sobre os princípios que estão sendo atendidos, direitos que podem ser exercidos e as respectivas medidas e salvaguardas.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

Para que seja realmente verificada a validade das informações, existem duas opções: consulta da data de nascimento, nome e CPF (para diferenciação de homônimo) em banco de dados legítimo e legal; ou, caso a consulta seja feita na hora, entende-se que a cópia do documento oficial (registro geral) se faz necessária, a fim de confirmar a validade daquele documento.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

O artigo supramencionado refere-se à obtenção de informações pessoais estritamente necessárias de crianças e adolescentes. Caso a ferramenta apresente conteúdo sensível, que pode ser restringido, entende-se que pode ser feito através de consulta da data de nascimento, nome e CPF (para diferenciação de homônimo) em banco de dados legítimo e legal; ou, caso a consulta seja feita na hora, entende-se que a cópia do documento oficial (registro geral) se faz necessária, a fim de confirmar a validade daquele documento.

O ponto de atenção se encontra na foto encontrada no documento oficial, que pode traçar perfil de raça/etnia e deve ser estudado. Todavia, dados sobre geolocalização, cadastro de consumo, dados sensíveis no geral (exceto PCDs para acessibilidade da ferramenta) não devem ser informados. Caso não existam informações a serem restringidas a um público geral, solicitar somente informações básicas para cadastro e recuperação de senha (nome, login, senha, duplo fator de autenticação).

As limitações devem se ater às que já estão previstas na Lei, como a atenção aos princípios.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

As ferramentas podem disponibilizar, a cada período estabelecido (ex. 2x semana em data programada) informações voltadas aos pais, que devem ler e confirmar leitura. Podem ser informações sobre quantidade de uso (número de horas), algum comportamento supostamente indevido da criança/adolescente, ou mesmo dicas práticas (educacionais) de segurança como não registrar a mesma senha para diversas plataformas.

Outra opção é o usuário sendo um cliente, recomenda-se o envio de uma notificação por e-mail (ou outro canal digital disponível) para o pai ou responsável legal cadastrado. Quando não for um cliente, deve ser informado pelo usuário em seu acesso.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Texto didático e claro em seus termos de uso e política de privacidade, redação de maneira simples, clara e acessível, inclusive com uso de recursos audiovisuais, para fornecer informações necessárias aos pais ou ao responsável legal e para possibilitar o adequado entendimento da criança e do adolescente sobre as informações disponibilizadas, podendo inclusive, solicitar que a cada período estabelecido (ex. 2x semana em data programada) os pais leiam e confirmem a leitura. O texto deve ser curto, interativo, deve contar com opção de áudio de leitura (áudio para acompanhamento do texto), vídeos podem ser apresentados e após finalização do conteúdo abrir um chat para perguntas e respostas.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

Sim, para que novas regulamentações sejam implementadas, por exemplo, código de design voltado especificamente para crianças e adolescentes, estas crianças e adolescentes devem ser voz ativa. Deve-se ouvi-los com intuito de compreender a realidade fática de como a tecnologia tem influenciado suas vidas. Neste sentido há a Convenção sobre os Direitos da Criança da ONU (1989) e o Comentário Geral 25 do Comitê dos Direitos da Criança da ONU (2021).

Além disso é importante, a promoção do pensamento crítico sobre o tratamento de dados pessoais entre crianças e os adolescentes pelo Estado por meio de conscientização em escolas e políticas públicas.

CONTRIBUIÇÕES À TOMADA DE SUBSÍDIOS PARA PROJETO REGULATÓRIO SOBRE CRIANÇAS E ADOLESCENTES – ANPD

BRASÍLIA/DF, AGOSTO DE 2024

ALAI
ASSOCIAÇÃO LATINO-AMERICANA DE INTERNET

SUMÁRIO

I - Princípio do melhor interesse **2**
II - Consentimento **6**
III - Jogos e aplicações de Internet **11**

Quem Somos[1]

A ALAI é uma associação civil de caráter internacional, sem fins lucrativos, que busca pensar e desenvolver a Internet na América Latina e no Caribe. A ALAI promove o desenvolvimento inclusivo da economia digital através da manutenção e fortalecimento de uma Internet aberta, com políticas que contemplem e favoreçam o empreendedorismo, a inovação, as oportunidades para novas aplicações da tecnologia, do respeito e do exercício dos direitos humanos.

Entre os temas de nossa atuação, destaca-se a agenda regional relacionada à desinformação, liberdade de expressão e economia digital. Tais temas são relevantes à missão, visão e princípios da ALAI, bem como de seus associados.

[1] Ver: ALAI. Disponível em: https://alai.lat/alai/. Acesso em: 22. mar. de 2022.

CONTRIBUIÇÕES

I - Princípio do melhor interesse

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD? [4200 caracteres]
A Associação Latino-Americana de Internet (ALAI) destaca os seguintes pontos: ● **Definição vaga no Guia de Legítimo Interesse:** A ANPD utilizou diretrizes da OCDE e da ONU para definir o "melhor interesse" da criança e do adolescente, mas essas orientações são vagas e insuficientes para que os controladores de dados atuem com segurança no contexto de proteção de dados pessoais. ● **Papel da ANPD e de outras autoridades competentes na definição do "melhor interesse" no âmbito de proteção de dados pessoais:** A ANPD e outras autoridades competentes (que devem considerar o melhor interesse de crianças e adolescentes na interface com suas respectivas áreas) têm a oportunidade de esclarecer o que constitui o melhor interesse desses usuários, assegurando assim a consistência e eficácia na aplicação das normas de proteção de dados. Isso ajudará a manter um equilíbrio adequado entre a proteção efetiva dos titulares e a promoção da segurança jurídica, beneficiando a todos. ○ .O melhor interesse da criança e do adolescente não deve ser considerado um "cheque em branco", de forma a permitir propostas de regulações esparsas por diferentes autoridades e órgãos. Neste sentido, é importante garantir cooperação entre diferentes atores, para se atingir entendimentos consistentes sobre como alcançar o melhor interesse desses titulares no caso concreto, inclusive considerando os limites e as competências previstas nas legislações e regulações existentes.

    - Por exemplo - Resolução Nº 245/2024 - CONANDA e Projeto de Lei n° 2628, de 2022 - estabelecimento de regras para proteger crianças e adolescentes no ambiente digital. Além de ser questionável se o CONANDA tem a competência para emitir regulamentações impondo novas obrigações não fundamentadas na Lei Federal, ambos faltam com uma análise técnica adequada sobre os desafios e riscos associados à proteção de dados pessoais. Tal deficiência resulta na proposta de obrigações excessivamente onerosas que, paradoxalmente, podem prejudicar a proteção de crianças e adolescentes.

- **Necessidade de segurança jurídica:** A ANPD e outras autoridades competentes devem parametrizar de forma mais objetiva o "melhor interesse" da criança e do adolescente sob a perspectiva de proteção de dados pessoais. Embora não se trate de um conceito fechado e definido *ex ante*, seria essencial conferir maior concretude, por exemplo utilizando mecanismos já mobilizados em outras oportunidades, como exemplos e situações hipotéticas que considerem nuances concretas e esforços tecnicamente disponíveis, mantendo flexibilidade para diferentes contextos e modelos de negócio.

- **Aplicação do princípio da minimização de dados:** Considerando que há uma possível tensão inerente entre o princípio da minimização de dados pessoais e a efetividade de mecanismos de verificação e detecção de idade, é essencial estabelecer parâmetros para que os agentes de tratamento possam se orientar. Coletar determinados dados pessoais pode, em certos casos, atender melhor ao interesse da criança e do adolescente, como na eficácia de barrar o acesso a conteúdos ou plataformas impróprios para a sua idade. Porém, o princípio da necessidade/minimização também determina que a coleta de dados deve contemplar apenas os dados estritamente necessários e não excessivos. Considerando que não há clareza sobre quais dados são considerados “estritamente necessários” neste contexto, e se a existência de salvaguardas pelos agentes de tratamento poderia mitigar eventuais riscos decorrentes dessa tensão, seria importante que a ANPD e outras autoridades competentes enfrentassem esse “*trade-off*”, para se garantir maior segurança jurídica aos agentes de tratamento.

- **Demais interesses da criança e do adolescente:** A análise do “melhor interesse” deve ser pautada pela multidimensionalidade, pois não envolve apenas a proteção dos dados do menor, mas outros interesses em disputa,

como a segurança, o acesso à informação, direito à brincar e se conectar, dentre outros[2].

- **Respeito à autonomia progressiva:** Deve-se levar em conta as diferentes características e experiências de um grupo heterogêneo, que variam de acordo com as individualidades, capacidades e circunstâncias de cada jovem (como a idade, gênero, deficiências, localização geográfica, origem étnica, perfil socioeconômico, etc). Assim, é importante que haja orientação sobre como garantir que o "melhor interesse" seja adaptável ao desenvolvimento de cada indivíduo.

    - É importante que a ANPD e outras autoridades competentes respeitem as expectativas de privacidade e os direitos de crianças e adolescentes conforme a progressão de sua autonomia e desenvolvimento, ao mesmo tempo em que garanta a importância da representatividade desses atores e experiências adequadas às suas vulnerabilidades/necessidades em produtos e serviços oferecidos a esses titulares, a fim de garantir o melhor interesse dessas crianças e adolescentes.

- **Caráter contextual da definição de "melhor interesse"**: a ANPD e outras autoridades competentes devem considerar que os melhores interesses de crianças e adolescentes podem variar de acordo com as atividades de tratamento de dados pessoais realizadas em casa concreto - ou seja, determinadas operações de tratamento não devem ser consideradas *per se* arriscadas para o melhor interesses desses titulares.

    - Por exemplo, o perfilamento, que costuma ser uma atividade de tratamento considerada "arriscada", pode ser analisado por outra perspectiva. Neste sentido, a identificação de usuários adolescentes para determinar se conteúdos específicos devem ou não ser direcionados para estes titulares (de acordo com a sua idade) é uma forma de perfilamento

[2] Este ponto é inclusive reconhecido pela ICO - *Information Commissioners' Office* (autoridade de proteção de dados do Reino Unido) em seu "*Age appropriate design: a code of practice for online services*", que reconhece que, para que os melhores interesses da criança e do adolecente sejam devidamente implementados, os agentes de tratamento devem considerar como, em seus tratamentos de dados, eles podem proteger e auxiliar suas perspectivas e identidade, sua liberdade de associação e de brincar, sua saúde e bem-estar, dentre outros aspectos. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/.

relevante para até mesmo garantir o melhor interesse desses adolescentes.

- Portanto, eventuais restrições a atividades de tratamento e a própria definição do melhor interesse de crianças e adolescentes devem considerar as particularidades do caso concreto e eventuais salvaguardas adotadas por agentes de tratamento para mitigar possíveis riscos dessas operações, bem como a autonomia e desenvolvimento progressivos dos titulares.

-

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas. [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) considera que:

- Em relação ao princípio do melhor interesse, em certos contextos, há maior facilidade em identificar o que seria o comportamento esperado do lado dos agentes de tratamento. No entanto, sua aplicação pode ser mais complexa em outros contextos, em que é difícil equilibrá-lo com os demais princípios da LGPD.
    - **Exemplo 1 - Perfilamento para publicidade personalizada:** há necessidade de equilibrar os benefícios da publicidade personalizada com os riscos à privacidade, afastando-se de um entendimento de que a publicidade personalizada (que não seja abusiva ou ilícita) é negativa em si mesma.
        - A publicidade personalizada envolve a utilização de dados específicos do usuário, como idade e interesses, para direcionar anúncios relevantes ao perfil individual.
        - A personalização da publicidade pode proteger menores ao tornar os anúncios mais adequados para eles. Isso evita que anúncios baseados em dados genéricos exponham crianças a conteúdos inadequados. Considerando fatores como idade ou localização, a personalização garante uma filtragem mais precisa e segura, tornando a experiência online mais relevante e segura, e criando um ambiente digital adaptado às necessidades e interesses das crianças.
        - As diretrizes devem garantir que a publicidade respeite a autonomia progressiva dos adolescentes, assegurando uma experiência online segura e adequada.
        - Conforme o Guia do LI, o teor da publicidade é crucial para determinar se ela atende ao melhor interesse do menor. Assim, a publicidade personalizada pode ser adequada dependendo de seu conteúdo, destacando a importância de avaliar o tipo de produto anunciado ao

considerar o legítimo interesse.

- **Exemplo 2 - Perfilamento para direcionamento de conteúdo:** O perfilamento também pode ser uma prática que atende ao melhor interesse da criança, visto que pode ser utilizado para direcionar conteúdos adequados à idade dos usuários (e vedar que conteúdos inadequados sejam exibidos).
    - Diferença de conceito: o perfilamento para fins de publicidade refere-se à coleta e análise de dados especificamente para criar anúncios personalizados, enquanto perfilamento para conteúdo envolve a utilização de dados para oferecer conteúdo relevante e apropriado ao usuário, sem fins publicitários.
- **Exemplo 3 - Processamento de dados pessoais de crianças e adolescentes para protegê-los de interações indesejadas**, através do envio de alertas de segurança quando abordados por adultos. Neste caso, a criação de perfis também pode ser uma prática que serve ao melhor interesse.
- Novamente, a questão do melhor interesse pode ser menos óbvia nestes contextos e por isso é crucial que a autoridade forneça diretrizes e balizas para avaliar e mitigar esses riscos.

II - Consentimento

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) destaca os seguintes pontos sobre o tema apresentado:

- **Escopo do termo "consentimento" na presente contribuição**: É necessário frisar que a autorização concedida para a utilização de produtos/serviços específicos oferecidos (por meio dos Termos de Serviço, por exemplo) é diferente do consentimento para o tratamento de dados de crianças, em situações específicas. As considerações abaixo dizem respeito apenas a este último.

- **Parâmetros para definição de criança e adolescente:** Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente): "Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade."

- **Consentimento parental apenas para crianças**: considerando o ponto acima, e em linha com a legislação brasileira (como o artigo 4, §1º da LGPD) e com posicionamentos internacionais sobre o tema[3], cumpre frisar que, quando o consentimento for a base legal adequada, apenas as atividades de tratamento envolvendo dados de crianças podem exigir consentimento parental.
    - Conforme explicado mais detalhadamente no item 3 abaixo desta mesma seção, levando em conta a autonomia e o desenvolvimento progressivo de menores de idade, é importante considerar que adolescentes devem ser capazes de fornecer seu próprio consentimento.

- **Possibilidade da aplicação de outras bases legais:** o consentimento nem sempre é a base legal mais adequada para o tratamento de dados pessoais de

[3] Neste sentido, a ICO - *Information Commissioners' Office* (autoridade de proteção de dados do Reino Unido) entende, por exemplo, que "1*3 é a idade em que crianças no Reino Unido podem fornecer seu próprio consentimento para o tratamento, se você estiver se baseando no consentimento como a sua base legal para o tratamento no contexto da oferta de um serviço online diretamente para uma criança*".

crianças e adolescentes, conforme os posicionamentos da ANPD, incluindo o Enunciado nº 01/2023 e o Guia de Legítimo Interesse..

- **No caso de o consentimento parental ser considerado a base legal adequada para o tratamento de dados pessoais de crianças**:

    - **ANPD deve esclarecer o conceito de "consentimento específico"**: O critério de "consentimento específico" deve ser esclarecido, de forma a garantir segurança jurídica aos agentes de tratamento sobre o formato esperado desse consentimento.

        - Independentemente de como esse consentimento específico poderá ser atingido, é necessário levar em consideração que uma granularidade do consentimento - no sentido de detalhamento de forma extremamente compartimentalizada - não significa necessariamente maior clareza ao titular e/ou uma decisão mais informada.

        - Ademais, o referido consentimento não deve funcionar como uma ferramenta de "controle" de pais e responsáveis legais sobre as ações de crianças, mas sim como uma forma de consentir com o tratamento dos dados pessoais de crianças para finalidades específicas, conforme informadas aos titulares e seus responsáveis legais, garantindo a legitimidade do tratamento.

    - **ANPD deve esclarecer o conceito de "consentimento em destaque"**: a autoridade deve garantir que o conceito seja flexível o suficiente para considerar tanto os meios técnicos disponíveis quanto às diferentes naturezas e propósitos dos produtos ou serviços. Assim, deve estabelecer parâmetros mínimos sem impor uma padronização rígida, permitindo que os regulados se adaptem aos seus contextos específicos (e.g., ao seu setor de atuação, à interface utilizada, etc.).

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) destaca a possibilidade da aplicação de outras bases legais, por isso considera a importância dos seguintes pontos:

- **Parametrização contextual:** Para definir parâmetros de adoção para viabilizar e verificar que o consentimento foi fornecido pelos pais/ responsáveis, a ANPD deve levar em conta os esforços razoáveis baseados na tecnologia disponível, recursos, nível de risco, naturezas e propósitos dos serviços e produtos. A autoridade não deve estabelecer medidas rígidas, mas diretrizes flexíveis e, em especial, que estejam adequadas à forma como interagem o titular e o agente de tratamento. Além disso, deve esclarecer parâmetros para que esse consentimento possa ser obtido de maneira que respeite a privacidade, garantindo que os métodos sejam práticos e adequados.
    - Exemplo - no Guia da ICO *Children 's code guidance and resources* - *age appropriate application*: a autoridade deixa claro a consideração de esforços razoáveis para a obtenção do consentimento parental. O Guia também esclarece que o consentimento deve ser obtido de maneira menos intrusiva possível à privacidade, coletando o mínimo de identificadores pessoais.
    - Exemplo - FTC/EUA "Regra de Proteção à Privacidade Online das Crianças: Um Plano de Conformidade em Seis Etapas para Seu Negócio" - A COPPA permite que se escolha o método de consentimento, desde que ele seja projetado de maneira razoável para garantir sua concessão pelo pai/mãe, tendo em vista as tecnologias disponíveis.

- **Exemplos**: Seria mais produtivo se a autoridade indicasse exemplos de padrões adequados em determinados contextos, ao invés de buscar definir rigidamente os mecanismos mais apropriados. Essa alternativa reconhece a impossibilidade de padronizar mecanismos para serviços tão variados, mas ainda fornece parâmetros claros aos agentes de tratamento, permitindo uma abordagem mais flexível. Assim, facilitaria a implementação em uma ampla gama de produtos, aumentando a eficácia da proteção.

- **Medidas excessivamente onerosas para obter consentimento podem dificultar que pais e responsáveis concedam esse consentimento de forma efetiva**. É preciso tomar cuidado com a "fadiga do consentimento"- na prática pode levar a que pais, especialmente quando menos familiarizados com a legislação, consintam excessivamente, gerando um efeito contrário ao pretendido

    - Isso destaca a necessidade de explorar outras bases legais, conforme já indicado pelo Enunciado nº 01/2023 e o Guia de Legítimo Interesse, e enfatiza a importância de que as medidas para obter um consentimento parental válido sejam proporcionais e práticas.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) reforça a necessidade de se diferenciar a autorização para utilizar o aplicativo não deve se confundir com o consentimento enquanto base legal para o tratamento de dados pessoais, por isso considera a importância dos seguintes pontos:

- Diferenciar o consentimento enquanto base legal e a concordância relativa a uma relação contratual estabelecida entre o agente de tratamento e o titular. A LGPD não altera a capacidade dos menores de idade de celebrar um contrato legal válido, de modo que o agente de tratamento poderá utilizar qualquer uma das bases legais disponíveis para tratar os dados pessoais de adolescentes.

    - **A autonomia progressiva deve levar a uma redução gradual da interferência parental, respeitando a crescente capacidade dos adolescentes de exercerem seus direitos de forma independente**. É possível considerar a autonomia progressiva de adolescentes no ambiente digital sem necessidade de representação ou assistência dos pais, alinhado ao princípio do melhor interesse. Para tanto, podem ser oferecidos mecanismos de supervisão parental que estejam alinhados ao grau de autonomia do adolescente.

    - **O melhor interesse apenas estará corretamente refletido considerando a autonomia e o desenvolvimento progressivo desses titulares, que pode gerar a desnecessidade de representação ou assistência pelos pais ou responsáveis legais**: o regime de incapacidades do Código Civil Brasileiro não é o melhor parâmetro para o direito à autonomia progressiva, positivada na legislação brasileira.

        - Tradicionalmente, a teoria civilista via as crianças como seres passivos, necessitando de controle adulto, mas essa visão está sendo desafiada

pela ideia de que os jovens devem ser vistos como indivíduos capazes de tomar decisões juridicamente relevantes. Essa mudança é reforçada por orientações internacionais [Comitê da ONU sobre Direitos da Criança, nos Comentários Gerais nº 12/2009 e 25/2016 e recomendações da Comissão Interamericana de Direitos Humanos], que instam os países a adaptar suas legislações para reconhecer e efetivar a autonomia progressiva das crianças e adolescentes, alinhada ao princípio do melhor interesse da criança. (Imperiosa revisão do regime de incapacidades pela comissão de atualização do Código Civil)

- **O Código Civil Brasileiro não foi confeccionado no contexto digital e, portanto, à medida que as interações online evoluíram, é necessário adaptá-lo às realidades do uso moderno de plataformas digitais.**
    - A capacidade civil e as formas de representação ou assistência para adolescentes devem ser mais flexíveis, especialmente em relação às atividades online consideradas "atos corriqueiros" - como o uso de uma plataforma projetada para criação de conteúdo, consumo de vídeos e interação com outros usuários - conforme atualmente defendido por professores e doutrinadores brasileiros (*Leal, Sheila do Rocio Cercal Santos. Contratos eletrônicos: validade jurídica dos contratos via Internet; Schreiber, Anderson. "Releitura das Incapacidades". In: Manual de Direito Civil Contemporâneo; Tepedino, Gustavo. "Esboço de uma classificação funcional dos atos jurídicos". Instituto Brasileiro de Direito Civil*).
    - Há, assim, uma presunção de que os pais estão cientes e concordam com os "atos corriqueiros" realizados pelos menores na internet, tal como acesso a uma plataforma (que possui mecanismos de proteção à criança e ao adolescente e é regida por termos os quais, em geral, os pais já conhecem e já validaram).
    - A lei brasileira não exige a autorização explícita ou expressa dos pais para todas as atividades dos adolescentes. Em vez disso, dentro da lei, **há uma compreensão implícita de que os menores se envolvem em atividades online com algum nível de conhecimento ou autorização dos pais**.

- Essa abordagem legal mantém a expectativa de que os pais orientem e monitorem o uso da internet pelos adolescentes de forma abrangente, mas não invasiva, permitindo que os jovens participem das atividades digitais rotineiras (como por exemplo interações sociais com colegas/amigos) sob a supervisão geral e indireta dos responsáveis, sem a necessidade de um consentimento / representação.
    - Reforçar que consentimento neste contexto não está sendo usado no sentido da base legal, mas de aceitação.

III - Jogos e aplicações de Internet

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) reforça a importância da interpretação contextual do princípio da minimização de dados em relação ao perfilamento como técnica para adequar o conteúdo a menores de idade.

- Torna-se necessário parâmetros flexíveis e adaptáveis a diferentes produtos e serviços, considerando a disponibilidade tecnológica, sua natureza e seu propósito, conforme o melhor esforço. Os parâmetros devem considerar a disponibilidade de soluções tecnológicas já existentes em toda a cadeia de valor, incluindo dispositivos e sistemas operacionais.

- Em respeito à autonomia progressiva, as ferramentas de privacidade devem também acompanhar o crescimento e maturidade do usuário - há exemplos em que usuários de 13 a 15 anos têm suas contas configuradas como privadas por padrão, permitindo que escolham o que compartilhar, quando e com quem. Além disso, há possibilidade de limitar que o envio de mensagens só

esteja disponível para aqueles com 16 anos ou mais, assim como hospedar uma LIVE é limitado aos membros da comunidade que devem ter pelo menos 18 anos.

- Há alguns mecanismos que podem ser citados como boas práticas:
    - **Limites diários de tempo de tela**: Estabelecimento automático de um limite de tempo de uso diário, que promove a consciência sobre o tempo gasto online. Painéis para manter controle do tempo de tela, bem como a possibilidade de silenciar notificações, também são bons exemplos.
    - **Gerenciamento ativo de tempo**: Opções para que os jovens ajustem seus próprios limites de tempo após alcançar o limite padrão, incentivando a tomada de decisão consciente.
    - **Controles parentais expandidos:** Ferramentas que permitem aos pais personalizar os limites de tempo de tela e configurar horários específicos para silenciar notificações, auxiliando na gestão do bem-estar digital, ou que fornecem aos pais informações sobre as interações recentes de usuários menores com outros usuários. Importante que essas ferramentas não invadam a privacidade do usuário menor de idade (como fornecer acesso às mensagens trocadas com outros usuários), mas apenas auxiliem na tomada de decisão.
    - **Notificações programadas:** Configuração de horários para silenciar notificações automaticamente, ajudando a minimizar interrupções durante períodos de descanso ou estudo.
    - **Remoção de contas suspeitas de menores de idade a partir de esforços humanos:** equipe de segurança treinada para identificar sinais de que uma conta pode ser de um usuário jovem, que esteja burlando os mecanismos de verificação de idade.
        - Para auxiliar nessa detecção, utilizam-se informações adicionais fornecidas pelos usuários da plataforma, como palavras-chave e denúncias feitas através do aplicativo pela comunidade, ou por meio de relatórios enviados por não-usuários.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) considera que não há orientações claras por parte da ANPD, o contexto de insegurança jurídica é agravado pela multiplicidade de disposições e atores envolvidos no processo de regulamentação, por isso é importante destacar os seguintes pontos:

- **O papel da ANPD é fundamental para definir balizas para mecanismos de avaliação de idade, que deverão considerar a natureza do serviço prestado e ponderar interesses conflitantes (e.g., robustez da avaliação de idade vs princípio da minimização).**
    - A ANPD, enquanto autoridade no setor, tem a oportunidade de liderar o estabelecimento de balizas s para mecanismos de avaliação de idade desses usuários, assegurando assim a consistência e a eficácia na aplicação das normas de proteção de dados..
- Com base nas terminologias adotadas pelo Center for Informaiton Policy Leadership (CIPL), a ANPD deve considerar que a avaliação de idade pode envolver diferentes métodos, incluindo: (i) verificação de idade, (ii) estimativa/predição de idade, e (iii) declaração de idade.
    - Essa interpretação também é adotada pelo Information Commissioner's Office (ICO), que estabelece que "avaliação de idade" se refere coletivamente às abordagens utilizadas para: (i) garantir que as crianças não consigam acessar conteúdo adulto, nocivo ou inadequado ao utilizar determinados serviços; e (ii) estimar ou estabelecer a idade de um usuário, para que os serviços possam ser adaptados às suas necessidades e para que proteções sejam implementadas, de acordo com a sua idade.
    - Ainda com base no material disponibilizado pelo ICO:

(a) "verificação de idade" seria qualquer método projetado para verificar a idade exata de usuários, ou confirmar que um usuário é

maior de 18 (dezoito) anos;

(b) “estimativa/predição de idade” seria qualquer método projetado para estimar a idade, ou a faixa etária, de um usuário; e

(c) “declaração de idade” seria um método de autodeclaração, em que o usuário é solicitado a declarar sua idade, mas nenhuma outra evidência é necessária para confirmar a veracidade da declaração.

“Técnicas em cascata” seriam os métodos em que diferentes abordagens de avaliação de idade são combinadas.

A ANPD também deve garantir que as medidas de avaliação de idade sejam acessíveis e econômicas para os diversos participantes do mercado, e adequadas ao risco.

Outro fator importante a ser levado em consideração pela ANPD são os esforços razoáveis adotados pelos agentes, considerando o estado da arte das tecnologias disponíveis e padrões internacionais.

- As orientações da ANPD devem levar em conta que medidas de avaliação de idade representam um desafio para toda a indústria e levantam, entre outros, potenciais riscos à privacidade. Especificamente:

    a. A avaliação da idade dos usuários apresenta **desafios técnicos que podem variar significativamente conforme a natureza do serviço**.

        - As orientações devem reconhecer que não há um único método de avaliação de idade superior a outros, pois a escolha depende do contexto específico, incluindo a finalidade e a natureza do tratamento dos dados, as limitações técnicas e o estado da arte das tecnologias disponíveis, bem como o modelo de negócios envolvido (já que, dependendo dos serviços/funcionalidades sendo oferecidos, mecanismos de avaliação de idade podem se basear em parâmetros diferentes).

    b. Há debates importantes sobre a necessidade de **equilibrar os riscos dos mecanismos de avaliação de idade**. Por exemplo, a Electronic Frontier Foundation (EFF) indicou, em 2023, que “os sistemas de verificação de idade são sistemas de vigilância” e, por isso, a organização é contrária a leis que obriguem a implementação de mecanismos de verificação de

idade.

- Seria importante reconhecer a possibilidade de implementação de mecanismos de pós-cadastro como uma alternativa para mitigar os riscos de uma coleta excessiva de dados no momento do cadastro – que, ao mesmo tempo, consegue assegurar que eventuais fraudes no cadastro serão detectadas.

    - Exemplo adicional: implementação de ferramentas de dupla verificação de idade no caso de novas tentativas de cadastro caso um usuário menor de 18 anos tente editar sua data de nascimento para uma data de nascimento anterior.

c. **Não há mecanismo infalível**, nem mecanismo que sempre e em todos os contextos será superior aos demais.

- É necessário avaliar o contexto e refletir sobre a razoabilidade - lembrando que esse tipo de ferramenta não será necessário apenas para grandes empresas de tecnologia, mas pode acabar sendo utilizado também por pequenas empresas, para as quais o custo de implementação tende a ser muito mais significativo.

-

- . Os serviços enfrentarão desafios diferentes com base no seu nível de maturidade e tamanho, assim como na natureza dos riscos associados ao seu serviço. Alguns métodos de avaliação de idade podem não ser econômicos para empresas menores, e se essas medidas não forem adequadas ao risco, poderão sobrecarregar indevidamente essas empresas.

- A possibilidade de as crianças burlarem essas verificações, como usar o celular dos pais, é um exemplo da falibilidade dessas medidas. Exigir, por esse motivo, que a plataforma imponha controles ainda mais rígidos além da busca ativa de menores é considerado desproporcional e tecnicamente desafiador.

- Muitas vezes, a decisão de permitir que uma criança acesse a plataforma é tomada pelo responsável legal, ocorrendo fora do ambiente da plataforma. Portanto, seria inadequado e complexo responsabilizar a plataforma por essas decisões externas. Adicionalmente, impor uma responsabilidade jurídica à plataforma que contrarie a decisão dos pais ou responsáveis é desafiador.

- Ademais, é necessário reconhecer que, ainda que a coleta de determinados dados seja necessária (e, portanto, não deve ser restringida), a minimização de dados se faz necessária, para evitar a violação do princípio da necessidade (conforme previsto pelo Art. 6º, III da LGPD), ao coletar mais dados do que o necessário para se avaliar a idade de usuários.

- Em última análise, o objetivo não deve ser criar uma obrigação para que empresas adotem mecanismos de verificação de idade específicos - mas sim que considerem diferentes abordagens para adotar um método/técnica em cascata, dependendo da natureza do serviço/funcionalidade oferecida, inclusive para garantir o alinhamento com outros princípios de proteção de dados (como necessidade e segurança).

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) considera a importância dos seguintes pontos:

- **A coleta de dados pessoais de crianças e adolescentes não deve ser automaticamente limitada por critérios pré-definidos além daqueles já explícitos na legislação (ou seja, finalidades ilícitas).** Qualquer restrição imposta deve considerar o melhor interesse desses indivíduos. A definição de diretrizes claras sobre o que constitui o melhor interesse desses titulares de dados ajudaria a clarificar e orientar essas decisões.

  - Conforme a LGPD e outras legislações, desde que os agentes de tratamento justifiquem uma base legal adequada, implementem as medidas necessárias para cumprir as obrigações estabelecidas pela LGPD e garantam que o tratamento dos dados esteja alinhado com o melhor interesse das crianças e adolescentes, **não existem restrições específicas ao tratamento de dados de crianças e adolescentes, inclusive dados pessoais sensíveis**.

  - **A formação de perfis comportamentais - ou perfilamento - não deve ser vista como uma atividade de tratamento de dados que apresenta riscos inerentes, especialmente para crianças e adolescentes**. Além de personalizar a experiência individual em serviços/produtos oferecidos por agentes de tratamento (permitindo que acessem conteúdos de maior interesse e relevância), a perfilização desempenha papel fundamental na segurança de menores de idade. Dessa forma, o perfilamento pode ser uma prática que atende ao melhor interesse da criança, visto que pode ser utilizado para direcionar conteúdos adequados (e restringir conteúdo inadequado) à idade dos usuários.

  - Dependendo dos objetivos a que se destinam, as atividades de perfilamento podem ser restringidas conforme as leis do panorama regulatório brasileiro;mas restrições devem ser impostas devido à violação do melhor interesse da criança e do adolescente, e não simplesmente pela realização da

atividade em abstrato.

- **O perfilamento não é exclusivo para publicidade.** Note-se que o perfilamento para fins de publicidade refere-se à coleta e análise de dados especificamente para criar anúncios personalizados, enquanto perfilamento para conteúdo envolve a utilização de dados para oferecer conteúdo relevante ao usuário, sem fins publicitários.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) considera a relevância dos seguintes pontos:

- Os mandatos sobre controles parentais devem levar em consideração a privacidade dos adolescentes, assim como a importância do acesso à informação e à comunidade. Eles também devem levar em conta a diversidade de serviços e permitir abordagens flexíveis.
- **Medidas de proteção de privacidade para menores adaptáveis aos níveis de maturidade e autonomia de cada usuário em desenvolvimento:** As configurações de privacidade não devem ser rígidas, mas sim flexíveis, permitindo ajustes que correspondam ao conteúdo apropriado para a idade e ao estágio de desenvolvimento do usuário. Essa abordagem reconhece que diferentes idades e níveis de compreensão requerem diferentes níveis de proteção e interação, levando em conta a autonomia progressiva e, portanto, o melhor interesse da criança e do adolescente, conforme exige a legislação brasileira.
    - A terminologia “supervisão parental/ de responsáveis” é, neste sentido, mais adequada do que “controle”.
- **Exemplo - sincronização familiar:** deve-se permitir que responsáveis legais e adolescentes decidam em conjunto sobre a ativação de ferramentas com graus distintos de proteção especial, que possibilita a vinculação das contas dos pais às dos filhos adolescentes. Isso facilita a gestão de configurações relacionadas a conteúdo, privacidade e bem-estar. Tais configurações, que devem ser ativadas após diálogo com os pais e responsáveis, incluem tornar a conta privada, gerenciar comentários e mensagens diretas, controlar o acesso a conteúdos através da busca, limitar o tempo de tela diário e ativar o Modo Restrito. De maneira mais específica:
    - **Tempo de Tela**: Pais e responsáveis podem vincular suas contas às dos adolescentes para personalizar configurações de segurança, como o tempo de tela diário. Os responsáveis podem

ajustar o tempo de uso, aplicá-lo a todos os dispositivos do adolescente e definir um código de acesso para uso adicional após o limite ser atingido. A possibilidade de monitoramento do tempo de tela também é um recurso que promove a segurança das crianças e adolescentes.

- **Ativação de restrição de funcionalidades específicas, por exemplo**:
  - **Modo restrito**: funcionalidade que reduz a visualização de conteúdos potencialmente inadequados para certos públicos, como temas maduros ou complexos. Ao ativar este modo, algumas funcionalidades da plataforma são desabilitadas - por exemplo, opções de iniciar LIVEs.
  - **Modo Comentário Moderado**: aplicação de filtros a comentários publicados, restringindo, por exemplo, comentários inadequados e ofensivos.
  - **Mensagens diretas**: Restringir ou desativar quem pode enviar mensagens ao adolescente.

- **Promoção da cultura de diálogo dos pais e responsáveis com crianças e adolescentes:** ferramentas que incentivem os pais a discutir e explicar a ativação dessas configurações com os adolescentes são bem-vindas, porque é também de responsabilidade da família/dos responsáveis a proteção da segurança, privacidade e autonomia progressiva do menor, cumprindo com seus os direitos e deveres de educar suas crianças - tal como determina o Artigo 5 da Convenção sobre os Direitos da Criança[4].
  - Essa medida está alinhada com a lógica de promoção de maior conhecimento e compreensão sobre mecanismos digitais, tanto do lado dos pais, quanto do lado dos adolescentes.

[4] "Os Estados Partes respeitarão as responsabilidades, os direitos e os deveres dos pais ou, onde for o caso, dos membros da família ampliada ou da comunidade, conforme determinem os costumes locais, dos tutores ou de outras pessoas legalmente responsáveis, de proporcionar à criança instrução e orientação adequadas e acordes com a evolução de sua capacidade no exercício dos direitos reconhecidos na presente convenção."

- **Transparência direcionada aos pais e responsáveis** - Guias direcionados especificamente aos pais e responsáveis, com linguagem clara e transparente, facilitam a navegação destes em plataformas de nossas associadas, são ferramentas importantes para ajudá-los a compreender as ferramentas e mecanismos disponíveis para auxiliá-los em seu dever de supervisão.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) considera a importância dos seguintes pontos:

- **A Política de Privacidade não precisa aparecer a todo momento ao usuário**: informações devem constar na Política de Privacidade ("PP") dos agentes de tratamento e esta deve estar em local de fácil acesso. No entanto, não necessariamente precisa aparecer a todo momento ao usuário e/ou aos seus pais e responsáveis legais, para evitar fadiga.
    - Em determinados casos, pode ser mais efetivo que informações específicas sejam retomadas na tela em momentos igualmente específicos, relacionados mais diretamente com um determinado tratamento.
- **As informações fornecidas aos usuários ou pais precisam ser relevantes e facilmente compreensíveis**. Meramente aumentar a quantidade de informações disponibilizadas não garante maior transparência, especialmente se essas informações forem complexas ou se houver uma expectativa de que os usuários ou pais provavelmente não as lerão.
- **Outros meios além da PP são bem-vindos e corroboram com o dever de transparência:** em não havendo qualquer tipo de proibição legal (ou determinação) de que a PP deve ser o único meio para o fornecimento de transparência, informações adicionais sobre o tratamento de dados de crianças e adolescentes podem constar em documentos apartados, além da PP, tais como de artigos disponibilizados via central de transparência e ajuda,

ou mesmo notícias veiculadas pelos agentes.

  - A PP não deve ser o único meio de transparência para se aferir se os dados tratados por agentes de tratamento estão associados a finalidades legítimas, específicas, explícitas e informadas ao titular. A "especificidade" da transparência pode ser desenvolvida nestes outros recursos – especialmente durante a utilização de produtos e serviços pelos adolescentes, através de notificações, por exemplo.

- **A transparência fornecida deve ser adequada/adaptada aos usuários que a utilizam.** Para isso, é possível fornecer portais e outros meios específicos, que possuam elementos que facilitem a compreensão das informações por adolescentes (como ícones/apelos visuais, vídeos/áudios, conteúdo interativo, linguagem facilitada, etc). A fim de garantir o melhor interesse, também é importante dar suporte e fornecer transparência apropriada aos pais e responsáveis legais, de modo que tenham acesso a informações sobre as práticas de tratamentos de dados pessoais realizadas, recursos de supervisão parental, dentre outros.

- **A transparência a ser fornecida deve observar os limites técnicos e os segredos comerciais e industriais dos agentes de tratamento**: O fornecimento de informações excessivas sobre as ferramentas de tratamento de dados de menores de idade pode servir de subsídio para que agentes mal-intencionados burlem mecanismos de segurança de *websites* e plataformas, colocando em risco a segurança desses usuários – portanto, é necessário estabelecer uma transparência adequada, visando os melhores interesses desses titulares.

- Por fim, é importante manter uma **parceria constante com pais, responsáveis legais e com os próprios adolescentes** sobre como melhorar os recursos de transparência disponíveis, a fim de melhorar cada vez mais a compreensão de definições de privacidade e segurança.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional? [4200 caracteres]

A Associação Latino-Americana de Internet (ALAI) considera importantes os seguintes pontos:

- **Controladores não devem ser responsáveis por estabelecer bases legais para o tratamento de dados que resultam de menores burlando seus mecanismos de verificação de idade.** Considerando que, como dito acima, não há mecanismo de verificação de idade infalível, falhas inevitavelmente ocorrerão. Quando crianças e adolescentes conseguem burlar mecanismos de verificação de idade durante o cadastro em plataformas, é importante que a ANPD determine que não há responsabilidade do controlador em determinar uma base legal apropriada para o tratamento desses dados pessoais coletados de forma equivocada.

- **Elaboração de RIPD e de identificação de tratamentos de dados pessoais de alto risco:** É necessário que a autoridade se manifeste com relação a requisitos para a elaboração de RIPD e de identificação de tratamentos de dados pessoais de alto risco, tendo em vista que a existência de dados pessoais de crianças e adolescentes é considerada como critério a ser levado em consideração para a aplicação desses requisitos.

    - **Crítica ao critério de alto risco:** o estabelecimento de dados pessoais de crianças e adolescentes como um critério de alto risco traz possíveis consequências negativas e ineficiências. Por exemplo, a contaminação de outros tratamentos de dados que poderiam ser inadvertidamente classificados como de alto risco.

    - **: Tratamento de dados para fins de Regulamentação específica para publicidade:** Reforça-se a necessidade da ANPD reconhecer a legitimidade do tratamento de dados pessoais de crianças e adolescentes para fins de publicidade, sugerindo a criação de um guia específico que considere a maturidade progressiva do adolescente e diferencie entre publicidade personalizada e não personalizada.

- **Esclarecimentos sobre controles de escolha:** Necessidade de esclarecimentos sobre parâmetros gerais para o formato de centrais de controle das escolhas dos usuários, especialmente quando direcionados para crianças e adolescentes, levando em conta as diferentes tecnologias disponíveis e naturezas e propósitos distintos de diferentes serviços e produtos.

São Paulo, 09 de agosto de 2024.

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ("ANPD")

Coordenação-Geral de Normatização

Ref.: Tomada de Subsídios a respeito do Tratamento de Dados Pessoais de Crianças e Adolescentes

A ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO ("ANBC"), pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Avenida das Nações Unidas, n.º 14.401, Conjuntos 502 e 503, Cidade de São Paulo, Estado de São Paulo, é uma entidade que reúne os bureaus atuantes no território brasileiro, com o objetivo de representar o setor de bureaus de crédito no país, inclusive junto a agentes internacionais, incentivar a educação financeira e colaborar para a criação de um ambiente legal e regulatório que permita à gestão de crédito contribuir ativamente com a economia brasileira.

Em 16 de junho de 2024, a ANPD disponibilizou, por meio do Espaço Opine Aqui, da Plataforma "Participa + Brasil",[1] a Tomada de Subsídios[2] acerca do Tratamento de Dados Pessoais de Crianças de Adolescentes.

Nessa oportunidade, a ANBC vem apresentar a sua contribuição à ANPD, reiterando seus cumprimentos pela iniciativa de consultar e colher subsídios de todos os setores interessados, com vistas a contribuir para a atuação da Autoridade em torno dessa matéria.

---

[1] Disponível em: < Governo Federal - Participa + Brasil - ANPD - Coordenação-Geral de Normatização (www.gov.br) >. Acesso em: 15.07.2024.

[2] Disponível em: < Governo Federal - Participa + Brasil - Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes. (www.gov.br) >. Acesso em: 15.07.2024.

ANBC
ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO

* * *

TOMADA DE SUBSÍDIOS TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Para além do Enunciado CD/ANPD nº 01/2022 e do Guia Orientativo sobre legítimo interesse, a ANBC entende que a Autoridade Nacional de Proteção de Dados ("ANPD") pode oferecer orientações e esclarecimentos específicos quanto à aplicação do princípio do melhor interesse em diferentes situações e finalidades. Com efeito, o tratamento de dados pessoais de crianças e adolescentes pode fundamentar-se em diferentes hipóteses legais para além do consentimento (artigo 14, § 1º, da Lei Geral de Proteção de Dados Pessoais – Lei Federal n.º 13.709/2018, "LGPD"), de modo a atender a um interesse coletivo e ao interesse do próprio titular, desde que observado e prevalecente o princípio do melhor interesse, em consonância com o Enunciado CD/ANPD n.º 1/2023.

Nesse contexto, a ANPD poderia apresentar orientações específicas a respeito das atividades de prevenção à fraude, o que incluiria o atendimento ao interesse da própria coletividade no combate a atos ilícitos, mas também abrangeria a proteção das crianças e adolescentes vítimas de fraudes ou que tenham os seus dados pessoais vinculados a operações fraudulentas.

É o caso de monitoramento de determinadas operações para evitar-se atividades fraudulentas, visto que criminosos podem utilizar dados pessoais relacionados a crianças ou adolescentes para a obtenção de crédito ou para a realização de transações fraudulentas. Nessa linha, o agente de tratamento poderia, com base no princípio do melhor interesse, tratar os dados do titular para detectar e combater atividades ilícitas e prejudiciais ao titular de dados, contrário dessa maneira ao princípio do melhor interesse.

Pode-se destacar, além disso, a verificação da identidade do titular em transações financeiras, uma vez que dados pessoais de crianças ou adolescentes podem ser operados na qualidade de beneficiários de contas ou investimentos financeiros realizados por seus responsáveis legais, momento em que se faz necessário o tratamento das informações para confirmar que não há uso fraudulento da identidade da criança ou adolescente por terceiros, com fundamento e observância do princípio do melhor interesse.

No mesmo sentido, a utilização de cartões de créditos adicionais, direcionados a filhos de titulares de contas bancárias, também enseja o tratamento de dados de crianças e adolescentes para fins de prevenção à fraude.

Com base no exposto, nota-se como o princípio do melhor interesse pode ser contextualmente avaliado pela ANPD em diversas operações de prevenção à fraude e, até mesmo, de proteção do crédito envolvendo crianças e adolescentes, motivo pelo qual se sugere que a Autoridade apresente, em seu projeto regulatório, orientação específica nesse sentido, indicando a possibilidade do tratamento de dados pessoais de crianças e adolescentes fundamentado nas bases legais previstas na LGPD.

Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

De acordo com o Comentário Geral n.º 25/2021, do Comitê dos Direitos da Criança, da Organização das Nações Unidas, os Estados devem garantir a existência de salvaguardas adequadas para proteger crianças contra crimes que ocorram no ambiente digital, inclusive fraudes e roubos de identidade. Alinhado a essa orientação, recomenda-se que o projeto regulatório da ANPD inclua um detalhamento específico quanto à licitude de atividades de prevenção à fraude que envolvam o tratamento de dados pessoais de crianças e adolescentes, conforme situações específicas como a tentativa de obtenção de crédito ou de realização de transações financeiras e/ou fraudulentas.

Assim, a conformidade de atividades de prevenção à fraude com o princípio do melhor interesse corresponde a um contexto específico que pode demandar maior atenção e detalhamento por parte da ANPD, especialmente para que a Autoridade aponte expressamente aos agentes de tratamento a licitude dessas operações, tal como realizado pela autoridade de proteção de dados do Reino Unido ("ICO"), no documento "Age Appropriate Design": "Legal obligation may be relevant for some fraud prevention, child protection or safeguarding measures, if you can point to a specific legal provision or appropriate source of advice or guidance on your legal obligations." [Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-c-lawful-basis-for-processing/>].

Entende-se que uma previsão e um direcionamento específico por parte da ANPD, complementando o Enunciado CD/ANPD nº 1, de 22 de maio de 2023, de forma a tornar mais claro que os agentes de tratamento que atuam no combate e na prevenção a fraudes, devem realizar o tratamento de dados de menores com base no princípio do melhor interesse nesses contextos e situações, em que o tratamento de dados pessoais de menores ocorre à luz do interesse legítimo de prevenção à fraude (artigo 7º, IX, LGPD) ou, ainda, com base na hipótese legal de garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (artigo 11, II, "g", LGPD).

Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

Os critérios e parâmetros que devem ser observados para a obtenção do consentimento específico e em destaque de pais ou responsáveis legais (artigo 14, § 1º, LGPD) correspondem aos mesmos previstos no artigo 11, I, da LGPD, combinado com o seu artigo 5º, XII. Assim, deve-se compreendê-lo como uma manifestação livre, informada, inequívoca, específica e em destaque pela qual os pais ou responsáveis legais concordam com o tratamento dos dados pessoais da criança para uma finalidade determinada. Dessa forma, independentemente de o conceito referir-se à obtenção do consentimento do próprio titular ou à manifestação concedida pelos pais ou responsáveis legais da criança, os critérios e parâmetros não devem ser alterados a depender da pessoa que forneça a autorização para o tratamento.

Nesse sentido, o consentimento precisa corresponder a uma escolha verdadeira, sem que a sua recusa represente um prejuízo ilícito ou abusivo ao titular (requisito da autorização livre), após a devida transparência do agente de tratamento quanto à operação a ser conduzida com os dados pessoais do titular (requisito da informação). Ademais, a manifestação de vontade deve representar indubitavelmente a concordância do titular com um tratamento (requisito da autorização inequívoca) específico e destacado de outras operações, a fim de conferir maior granularidade ao consentimento (requisito da autorização específica e em destaque), em conformidade com as melhores práticas de mercado e as "Guidelines 05/2020 on Consent" do European Data Protection Board ("EDPB"). [Disponível em: <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>].

Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

Os controladores devem adotar, especialmente no ambiente digital, medidas e mecanismos que viabilizem e verifiquem o consentimento fornecido pelos pais ou responsáveis das crianças de acordo com as tecnologias e os recursos disponíveis ao agente de tratamento, conforme o risco das atividades a serem conduzidas, o que pode ser aferido por um relatório de impacto à proteção de dados. Dentre as opções disponíveis aos agentes de tratamento em operações de risco mais elevado, consoante documento "Age Appropriate Design" da autoridade de proteção de dados do Reino Unido ("ICO"), os controladores poderiam verificar a própria idade dos pais ou responsáveis e atestar a relação de parentesco entre a criança e a pessoa que fornece o consentimento. Outra possibilidade indicada pelo

ICO seria a contratação de terceiros que adotem mecanismos de controle e responsabilizem-se diretamente pela confirmação do consentimento pelos pais ou responsáveis. Por sua vez, atividades de baixo risco, com pouco impacto significativo aos interesses e direitos dos titulares, poderiam se valer do consentimento fornecido por mecanismos simples de autodeclaração. [Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-c-lawful-basis-for-processing/>].

É o caso, no contexto brasileiro, de atividades que não impeçam o exercício de direitos ou a utilização de serviços, ou que não ocasionem danos materiais ou morais às crianças – como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras e roubos de identidade. [Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>]

No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

Entende-se que é possível considerar a autonomia progressiva dos adolescentes para, em determinados contextos e situações, eles próprios fornecerem o seu consentimento para o tratamento de dados pessoais, sem a necessidade de representação (dos doze aos dezesseis anos) ou de assistência (dos dezesseis aos dezoito anos) dos pais ou responsáveis legais, desde que observado e prevalecente o princípio do melhor interesse.

Tanto é assim que a própria LGPD prevê, em seu artigo 14, § 1º, a necessidade de consentimento do pai ou responsável legal no caso de autorizações em nome de crianças, não mencionando a legislação a figura dos adolescentes nesse caso, o que fortalece uma interpretação pela viabilidade da autonomia dos adolescentes para a prática de determinados atos compatíveis com a sua maturidade, sempre em atenção ao princípio do melhor interesse.

Segue-se, com isso, o artigo 5º da Convenção sobre os Direitos da Criança, da Organização das Nações Unidas, segundo o qual deve-se proporcionar instrução e orientação adequadas às crianças e aos adolescentes, de acordo com sua capacidade em evolução, no exercício dos direitos que lhe cabem. Em sentido semelhante, o artigo 12.1. da Convenção estabelece que deve ser assegurado à criança e ao adolescente o direito de expressar suas opiniões livremente sobre todos os assuntos relacionados a ela ou ele, e tais opiniões devem ser consideradas, em função da sua idade e da sua maturidade. Portanto, a ANPD poderia considerar a autonomia progressiva dos adolescentes para o fornecimento

do consentimento ao tratamento de dados pessoais, desde que observado o princípio do melhor interesse pelo agente de tratamento no caso concreto, consoante *caput* do artigo 14 da LGPD.

Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

As plataformas digitais devem observar o princípio do melhor interesse, à luz do artigo 14 da LGPD, de modo a promover e assegurar níveis elevados de privacidade e proteção de dados pessoais, bem como mitigar riscos decorrentes do uso dessas plataformas. Dentre os parâmetros que podem nortear as operações dos agentes de tratamento, destacam-se medidas de *design* que viabilizem o combate a fraudes nas plataformas. Isso inclui, a título de exemplo, atividades de identificação da idade do titular, a partir do tratamento de seus dados pessoais.
Nesse sentido, o documento "Age Appropriate Design" da autoridade de proteção de dados do Reino Unido ("ICO") indica que os padrões técnicos de design de informações que possam ser acessadas por crianças ou de serviços atrelados à idade da criança observem o melhor interesse.
[Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/standards-of-age-appropriate-design/ >].

Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

O documento "Age Appropriate Design" da autoridade de proteção de dados do Reino Unido ("ICO"), aponta alguns métodos de confirmação de idade que podem ser adotados pelos agentes de tratamento, a depender das especificidades técnicas utilizadas. A lista inclui a autodeclaração pelo usuário da plataforma, o emprego de sistemas de inteligência artificial que estimem a idade do titular, a contratação de serviços de verificação de idade terceiros, a confirmação da idade por um adulto cadastrado e verificado na plataforma, a adoção de medidas técnicas que coíbam a criação de contas por crianças ou adolescentes – conforme cabível –, bem como a coleta de documentos de identificação oficiais emitidos pelo Estado. [Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-c-lawful-basis-for-processing/>].

Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre

outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

As limitações específicas que devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais devem ater-se ao caso concreto analisado. Dessa forma, a escolha das restrições e dos limites a serem observados pelos agentes de tratamento deve considerar a existência de particularidades identificadas a partir da análise de situações concretas e específicas. Em todo caso, os agentes de tratamento precisam atender os princípios da finalidade, adequação e necessidade (artigo 6º, I a III, LGPD), de forma a garantir a conformidade de suas operações com a legislação de proteção de dados.

Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Dentre as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível, as plataformas digitais podem adotar políticas de privacidade e termos de uso específicos, tornando também possível a opção por seções específicas nesses documentos que abordem o tratamento de dados pessoais de crianças e adolescentes, em conformidade com o princípio da qualidade dos dados e da transparência (artigo 6º, IV a VI, LGPD), em atenção aos requisitos dos artigos 9º e 14, § 6º, da LGPD. Outra medida adequada para a garantia da informação aos titulares é a disponibilização de canais de atendimento com o controle de identificação dessas pessoas ou de seus pais ou representantes legais.

Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

A ANPD poderia reforçar em seu projeto regulatório a disposição do Enunciado CD/ANPD n.º 1/2023, segundo o qual o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no artigo 7º ou no artigo 11 da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do artigo 14 da LGPD, complementando referido enunciado conforme sugerido nesta manifestação..
Para tanto, recomenda-se que a ANPD indique aos agentes de tratamento exemplos em que a base legal do consentimento (artigo 14, § 1º, LGPD) não seja a mais adequada para a fundamentação do tratamento, uma vez que não há garantir da prevalência do princípio do melhor interesse do menor. Dessa forma, algumas operações que poderiam constar nessa orientação da Autoridade incluem atividades voltadas para propósitos como a prevenção à fraude, validação cadastral, justificada pelo

legítimo interesse (artigo 7º, IX, LGPD) ou pela garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (artigo 11, II, “g”, LGPD) ou, até mesmo, cumprimento de obrigação legal (artigo 7º, II) e a garantia de crédito, conforme a base legal do artigo 7º, X, da LGPD.

* * *

CONTRIBUIÇÕES

Informamos aos interessados em participar deste procedimento de participação da sociedade que as informações e o conteúdo de todas as manifestações apresentadas serão disponibilizados ao público pela ANPD ao final do processo, na íntegra, em transparência ativa.

I - Princípio do melhor interesse

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD? [4200 caracteres]
A ANPD utilizou diretrizes da OCDE e da ONU para definir o "melhor interesse" da criança e do adolescente no Guia de Legítimo Interesse. No entanto, essas orientações são vagas para uma atuação segura dos agentes de tratamento. Embora a amplitude e abstração do princípio sejam naturais, pois não se trata de um conceito fechado e definido *ex ante*, a ANPD pode criar diretrizes e parâmetros para melhor esclarecer, com algum nível de concretude, o que constitui o melhor interesse desses titulares no âmbito do tratamento de dados pessoais, assegurando consistência e eficácia na aplicação das normas de proteção de dados. Portanto, é crucial que a ANPD parametrize de forma mais objetiva o "melhor interesse" da criança e do adolescente na proteção de dados pessoais. Seria essencial conferir maior concretude utilizando mecanismos como exemplos e situações hipotéticas que considerem nuances específicas e esforços tecnicamente disponíveis, mantendo flexibilidade para diferentes contextos e modelos de negócio. Vale ressaltar que, por exemplo, a ANPD já manifestou na Nota Técnica nº 6/2023/CGF/ANPD que a restrição de acesso aos produtos e serviços do TikTok para crianças (indivíduos com até 12 anos) seria uma forma de garantir o melhor interesse. Seria relevante, para fins de orientação geral e clareza ao mercado, esclarecimentos acerca dos motivos pelos quais determinadas restrições auxiliam na concretização do princípio, na visão da autoridade. A tensão entre o princípio da minimização de dados pessoais e a eficácia dos mecanismos de verificação e detecção de idade é um bom exemplo da relevância deste tipo de esclarecimento. Atender ao melhor interesse - como adotar medidas para impedir o acesso a conteúdos ou plataformas inadequados para sua idade - pode exigir a coleta de mais dados pessoais. Por isso, é crucial que os agentes compreendam com algum nível de clareza quais são as balizas concretas que a ANPD considerará na análise deste tipo de cenário, para que possam determinar a melhor forma de implementação de ferramentas. Sem clareza sobre se a autoridade considerará esses mecanismos válidos - ou se entenderá mecanismos mais invasivos como contrários ao princípio da minimização - o

mercado dificilmente saberá como agir. Assim, é crucial garantir que os controladores não sejam penalizados por eventual flexibilização do princípio da minimização, quando justificada pelo melhor interesse da criança e do adolescente.

Além disso, é importante que as orientações da autoridade sobre o que constitui o melhor interesse da criança e do adolescente em situações específicas sejam fornecidas não só por meio de casos concretos, mas principalmente através de guias e outros documentos com eficácia geral. Isso oferece maior segurança jurídica, permitindo que os agentes se antecipem e ajustem suas práticas conforme parâmetros estabelecidos. Além disso, dessa forma, os agentes não precisam esperar por casos específicos para agir e podem se preparar com antecedência - o que contribui para a construção de uma cultura de proteção de dados no Brasil. Também, essa forma de atuação auxilia a estabelecer um *level playing field* no mercado, evitando que agentes com políticas menos protetivas continuem a operar sem maiores consequências.

O TikTok destaca que a análise do "melhor interesse" deve considerar múltiplas dimensões, não se limitando à proteção de dados, mas também tendo em vista a segurança, acesso à informação, direito de brincar e se conectar, entre outros. Deve-se também levar em conta as diferentes características e experiências de um grupo heterogêneo (idade, gênero, deficiências, localização geográfica, origem étnica e perfil socioeconômico), tendo flexibilidade suficiente para ser adaptável ao desenvolvimento dos vários indivíduos que o compõem.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas. [4200 caracteres]

Em alguns contextos, é mais fácil identificar o comportamento esperado dos agentes de tratamento em relação ao princípio do melhor interesse. No entanto, sua aplicação pode ser mais complexa em outros casos, onde é difícil equilibrá-lo com os demais princípios da LGPD. O TikTok gostaria de trazer dois exemplos que considera particularmente desafiadores. O primeiro refere-se ao direcionamento de publicidade e, o segundo, ao direcionamento de conteúdo: ambas são práticas que tendem a ser vistas com maus olhos, como contrárias ao melhor interesse da criança e do adolescente, a partir de premissas equivocadas. Na realidade, ambas podem assegurar precisamente esse melhor interesse.

1. **Publicidade**: ainda que o TikTok não realize o perfilamento de usuários entre 13 e 17 anos com base em seus interesses, comportamento, gênero e idade para fins de publicidade,a criação de perfis com a referida finalidade exemplificaria a complexidade de harmonizar o melhor interesse da criança e do adolescente com os demais princípios da LGPD para plataformas digitais em geral.

   Isso porque, para plataformas que o fazem, o perfilamento para esse fim poderia vir a proteger menores, tornando os anúncios mais adequados e evitando que

conteúdos inapropriados para a idade sejam exibidos para o público mais jovem. Considerando fatores como idade, a personalização garante uma filtragem mais precisa e segura, tornando a experiência online mais relevante e adaptada às necessidades dos usuários mais jovens. As diretrizes da ANPD devem esclarecer essa complexidade, garantindo que a publicidade respeite a autonomia dos adolescentes e leve em consideração sua vulnerabilidade, assegurando uma experiência online segura e adequada. O mesmo valeria para o direcionamento de conteúdo para usuários mais jovens, como detalhado abaixo.

2. **Perfilamento para direcionamento de conteúdo.** Cabe lembrar a diferença entre o perfilamento para fins de publicidade (coleta e análise de dados para direcionar anúncios) e perfilamento para conteúdo (coleta e análise de dados para direcionar conteúdo relevante ao usuário, sem fins publicitários).

   O perfilamento para direcionamento de conteúdo também pode atender ao melhor interesse, pois pode direcionar conteúdos adequados à idade dos usuários e impedir que conteúdos inadequados sejam exibidos. Por exemplo, o TikTok criou a ferramenta "Níveis de Conteúdo", que tem como objetivo evitar que vídeos considerados inapropriados para menores de 18 anos sejam exibidos para usuários mais jovens. Nesse sentido, os vídeos são classificados e exibidos de acordo com o grau de maturidade dos usuários. Os vídeos denunciados e revisados por moderadores podem receber classificação 18+ e não serão exibidos para os usuários entre 13 e 18 anos. Com esses níveis, usuários e seus pais podem limitar determinados tipos de conteúdo e personalizar a experiência de visualização, evitando que temas maduros cheguem a usuários entre 13 e 18 anos. Esse tipo de iniciativa protege os mais jovens e pode se beneficiar de práticas de perfilamento.

   Como dito, a questão do melhor interesse pode ser menos óbvia nestes contextos, por isso é crucial que a autoridade forneça diretrizes e balizas para avaliar e mitigar riscos. É importante equilibrar os benefícios do perfilamento com os potenciais riscos, sendo essencial fornecer orientação sobre como avaliar e mitigá-los, garantindo que a publicidade direcionada considere a autonomia progressiva do adolescente e seu grau de vulnerabilidade.

II - Consentimento

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais? [4200 caracteres]

De acordo com a Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

Conforme os posicionamentos da ANPD, incluindo o Enunciado nº 01/2023 e o Guia de Legítimo Interesse, o consentimento nem sempre é a base legal mais adequada para o tratamento de dados pessoais destas crianças e adolescentes, sendo admitidas outras bases legais para o tratamento de seus dados pessoais. Além disso, o próprio Enunciado menciona o risco de oneração excessiva dos responsáveis e a necessidade de colaboração multissetorial para a proteção efetiva de crianças e adolescentes.

Especificamente no caso do tratamento de dados pessoais de crianças, caso o consentimento parental seja considerado a base legal mais adequada, cabe destacar que os adjetivos "específico e em destaque" (art. 14, §1º) diferem dos adjetivos "livre, informado e inequívoco" mencionados na LGPD. Essa diferença pode gerar inseguranças jurídicas significativas para os agentes regulados. Especificamente:

1. **A ANPD deve esclarecer o conceito de "específico"**: O critério deve possibilitar que o consentimento seja dado com um nível de granularidade adequado ao caso, desde que o usuário seja informado de forma transparente (informações claras, precisas e facilmente acessíveis) sobre o fluxo de tratamento de seus dados pessoais. Isso se justifica em prol de uma exigência de transparência que seja eficaz, visto que a granularidade do consentimento - no sentido de detalhamento de forma extremamente compartimentalizada - não significa necessariamente maior clareza ao titular e/ou uma decisão mais informada.

2. **ANPD deve esclarecer o conceito de "em destaque"**: a autoridade deve garantir que o conceito seja flexível o suficiente para considerar tanto os meios técnicos disponíveis quanto a diferentes naturezas e propósitos dos produtos ou serviços. Assim, deve estabelecer parâmetros mínimos sem impor uma padronização rígida, permitindo que os regulados se adaptem aos seus contextos específicos.

Considerando a impossibilidade da criação de regras rígidas e inflexíveis dada a vasta discrepância entre produtos e serviços, seria importante que a autoridade fornecesse diretrizes claras sobre quais métodos não são considerados adequados e suficientes para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais. Isso ajudaria a evitar ambiguidades e inseguranças jurídicas para agentes de tratamento.

Além disso, é fundamental que a autoridade, ao estabelecer parâmetros, tenha em mente a necessidade de se respeitar o princípio da autonomia progressiva que, conforme reconhecido no Estatuto da Criança e do Adolescente ("ECA") e na Convenção sobre os Direitos da Criança, estabelece que crianças e adolescentes devem ter sua capacidade de decisão respeitada e ampliada conforme amadurecem. Neste contexto, é importante ter em vista que é possível que o consentimento no caso concreto não seja ofertado unicamente por responsáveis, mas pelo próprio menor. A autonomia progressiva sugere que, em vez de uma abordagem única para todas as idades, os critérios para obter consentimento devem ser adaptados de acordo com o desenvolvimento e a maturidade. Portanto, ao definir critérios ou parâmetros para a obtenção do consentimento, a autoridade deve considerar fatores como idade e compreensão para participação do menor (à medida que os menores amadurecem, eles devem ser mais envolvidos no processo de consentimento, respeitando sua crescente autonomia).

Por exemplo, o Age Appropriate Design Code (ou “Children's Code”), elaborado pelo Information Commissioner's Office (ICO) do Reino Unido, que contém diretrizes para a proteção e privacidade online de crianças e adolescente, reconhece a autonomia progressiva da criança e do adolescente ao estabelecer diferentes parâmetros recomendados para o controle parental conforme faixa de idades.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de “todos os esforços razoáveis”, quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança? [4200 caracteres]

O TikTok reforça a possibilidade, já reconhecida pela ANPD, da adequação de outras bases legais para além do consentimento para o tratamento de dados de menores, em especial o de adolescentes, o que pode ser extraído da própria LGPD. Especificamente no caso do tratamento de dados pessoais de crianças, para definir parâmetros de adoção para viabilizar e verificar que o consentimento foi fornecido pelos responsáveis, a ANPD deve levar em conta os esforços razoáveis, baseados na tecnologia disponível, recursos, nível de risco, naturezas e propósitos dos serviços e produtos. A autoridade não deve estabelecer medidas rígidas, mas sim diretrizes flexíveis e adequadas à forma como interagem o titular e o agente de tratamento, o que pode variar de acordo com o modelo de negócio em questão. Além disso, deve esclarecer parâmetros para que esse consentimento possa ser obtido de maneira que respeite a privacidade, garantindo que os métodos sejam práticos e adequados.

No Guia da ICO, "Children 's Code Guidance and Resources - Age Appropriate Application" a autoridade deixa claro que é importante considerar esforços razoáveis para obter o consentimento parental. O Guia também esclarece que o consentimento deve ser obtido da maneira menos intrusiva possível, coletando o mínimo de identificadores pessoais. Um exemplo semelhante é a "Children 's Online Privacy Protection Act," dos EUA (“COPPA”). A COPPA permite a escolha do método de consentimento, desde que seja projetado de forma razoável para garantir efetiva concessão pelos pais, levando em conta as tecnologias disponíveis. Além disso, a autoridade é clara e específica com relação a possíveis exceções, por exemplo, indicando quando a regra do “contato único” para obtenção de consentimento parental é válida.

A European Data Protection Board, por sua vez, apresenta nas Diretrizes 05/2020 orientações sobre consentimento no contexto do GDPR. Essas diretrizes não especificam métodos exatos para obter o consentimento parental, mas recomendam uma abordagem proporcional baseada na minimização de dados. A verificação da idade adequada e da autoridade parental deve levar em consideração o nível de risco associado ao tratamento de dados e a tecnologia disponível, exigindo esforços adequados dos responsáveis pelo tratamento.

Assim, as medidas de verificação devem evitar a coleta excessiva de dados pessoais, reconhecendo a dificuldade de verificar consentimento quando a identidade da criança ou a responsabilidade parental são incertas. Uma medida que pode ser adotada pelos controladores é a indicação clara, nos Termos de Uso, dos requisitos para a representação dos pais, considerando a autonomia progressiva dos menores. Além disso, devem adotar mecanismos de transparência, permitindo que se compreenda os Termos de Uso dos serviços, respeitando seu desenvolvimento cognitivo e emocional.

Seria mais produtivo se a autoridade indicasse e justificasse, através de exemplos, quais métodos não considera adequados em determinados contextos, ao invés de buscar definir rigidamente os mecanismos mais apropriados. Essa alternativa reconhece a impossibilidade de padronizar mecanismos para serviços tão variados, mas ainda fornece parâmetros claros aos agentes de tratamento, permitindo uma abordagem mais flexível. Assim, facilitaria a implementação em uma ampla gama de produtos, aumentando a eficácia da proteção.

O TikTok destaca o risco de medidas excessivamente onerosas dificultarem a obtenção de consentimento efetivo para crianças e adolescentes (quando for a base legal adequada para o tratamento de dados), levando à "fadiga do consentimento". Vale salientar que a plataforma do TikTok é apenas para adolescentes maiores de 13 anos.

Desta forma, entendemos que seria mais efetivo oferecer uma experiência gradativa, por meio da qual os pais (e/ou responsáveis) e também os usuários mais jovens, teriam acesso a informações claras e acessíveis, podendo realizar escolhas mais factíveis e ter um maior controle do tratamento de seus dados pessoais e de sua respectiva experiência. Daí a importância de explorar outras bases legais e garantir que as medidas para obter consentimento parental sejam proporcionais e práticas. Conforme reconhecido pela ANPD em seu Estudo Técnico Preliminar, a fadiga do consentimento questiona a efetividade do consentimento parental como única base legal e sua adequação para garantir a proteção ao melhor interesse da criança.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais? [4200 caracteres]

Primeiramente, é preciso diferenciar o consentimento enquanto base legal e a concordância relativa a uma relação contratual estabelecida entre o agente de tratamento e o titular. A LGPD não altera a capacidade dos menores de idade de celebrar um contrato legal válido, de modo que o agente de tratamento poderá utilizar qualquer uma das bases legais disponíveis para tratar os dados pessoais de adolescentes.

A autonomia progressiva, conforme positivada pela legislação brasileira, deve levar a uma

redução gradual da interferência parental, respeitando a crescente capacidade dos adolescentes de exercerem seus direitos de forma independente. Portanto, é possível que adolescentes forneçam consentimento no ambiente digital sem a necessidade de representação ou assistência expressa dos pais, alinhando-se ao princípio do melhor interesse. A própria jurisprudência admite que a representação ou assistência possa ser tácita para atos corriqueiros da vida civil no ambiente digital. O melhor interesse será corretamente refletido ao se considerar a autonomia e o desenvolvimento progressivo desses jovens, o que pode prescindir a representação ou assistência expressa a depender do contexto, ato e risco em questão. Nesse sentido, o regime de incapacidades do Código Civil não é o melhor parâmetro para o direito à autonomia progressiva. Isso se verifica por duas razões:

1. O Estatuto da Criança e do Adolescente define "criança" como a pessoa até 12 anos e "adolescente" como aquela entre 12 e 18 anos. Já o Código Civil estabelece que menores de 16 anos são absolutamente incapazes de exercer pessoalmente os atos da vida civil e devem ser representados. Não prescreve, contudo, a forma como uma representação deve ser obtida. Neste ponto, vale destacar ainda que, em termos de representação/assistência, a ausência de exigência de autorização expressa é frequentemente considerada em situações envolvendo adolescentes em transações rotineiras ou interações online, especialmente em plataformas que oferecem os serviços como o do TikTok. Além disso, essa legislação não reflete adequadamente o desenvolvimento e a capacidade crescente dos adolescentes entre 12 e 16 anos de tomar decisões informadas e independentes. Tratar todos os indivíduos de 12 a 16 anos como uma massa homogênea e plenamente incapaz pode criar obstáculos ao seu melhor interesse.

   Tradicionalmente, a teoria civilista via as crianças como seres passivos, necessitando de controle adulto. No entanto, essa visão está sendo desafiada pela ideia de que os jovens devem ser vistos como capazes de tomar decisões juridicamente relevantes. Orientações internacionais, como os Comentários Gerais nº 12/2009 e 25/2016 do Comitê da ONU sobre Direitos da Criança e as recomendações da Comissão Interamericana de Direitos Humanos, instam os países a adaptar suas legislações para reconhecer e efetivar a autonomia progressiva das crianças e adolescentes, alinhada ao princípio do melhor interesse da criança. (Imperiosa revisão do regime de incapacidades pela comissão de atualização do Código Civil).

2. Para o Código Civil, aqueles com mais de 16 e menos de 18 anos são relativamente capazes, podendo praticar atos da vida civil desde que assistidos. No entanto, falta clareza sobre o que está incluído na definição de "atos da vida civil". Como o Código Civil não foi concebido no contexto digital, é necessário adaptá-lo à realidade moderna do uso de plataformas digitais. A capacidade civil e as formas de assistência para adolescentes devem ser mais flexíveis, especialmente em relação às atividades online consideradas "atos corriqueiros". [*Para referências, ver ANEXO I*]. Um adolescente acessar uma plataforma digital para jogar, criar conteúdo ou interagir com amigos em redes sociais deve ser visto de maneira diferente de realizar uma transação financeira de grande porte, embora, para o Código Civil, ambas as atividades sejam "atos civis". Não por outra

razão, aos 13 anos, as crianças no Reino Unido podem fornecer seu próprio consentimento para o tratamento de dados, se o consentimento for a base legal, no contexto de oferecer um serviço online diretamente a um menor de idade.

Há uma presunção de que os pais estão cientes e concordam com os "atos corriqueiros" realizados pelos menores na internet, como o acesso a plataformas com mecanismos de proteção, regidas por termos que os pais conhecem e validaram. A lei brasileira não exige autorização explícita dos pais para todas as atividades dos adolescentes. Em vez disso, há uma compreensão implícita de que os menores se envolvem em atividades online com algum nível de conhecimento ou autorização dos pais. Essa abordagem legal espera que os pais orientem e monitorem o uso da internet pelos adolescentes de forma abrangente, mas não invasiva, permitindo que os jovens participem de atividades digitais rotineiras, como interações sociais com amigos, sob supervisão geral e indireta dos responsáveis, sem a necessidade de aceitação formal e reiterada para qualquer interação.

III - Jogos e aplicações de Internet

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas? [4200 caracteres]

O TikTok destaca que, para tais orientações, é crucial que a autoridade considere os diferentes níveis de maturidade e autonomia dos usuários em desenvolvimento, que exigem níveis variados de proteção. Portanto, as configurações de privacidade para menores devem ser adaptáveis ao conteúdo apropriado para a idade e ao desenvolvimento dos diferentes indivíduos. A resposta sobre controle parental (III.4.) contém mais informações sobre como o TikTok implementa essas diretrizes através da sincronização familiar e guias dedicados aos pais e responsáveis.

O TikTok possui alguns mecanismos que esclarecem o que considera serem boas práticas. Em respeito à autonomia progressiva, as ferramentas de privacidade devem também acompanhar o crescimento e maturidade do usuário. Por exemplo:

- Configuração de privacidade da conta (visibilidade da conta):
    - Para usuários entre 13-15 anos: as contas são configuradas como privadas por padrão, restringindo quem pode segui-las, ver seus vídeos, ler suas biografias e interagir com seus conteúdos.
    - Para usuários entre 16-17 anos: há a opção de escolha, mas se optar por não escolher, a conta é definida como privada.

- Envio de mensagens diretas:
    - Para usuários entre 13-15 anos: não é permitido.
    - Para usuários entre 16-17 anos: configura-se como desligadas por padrão, mas o usuário pode alterar para “amigos” e “amigos sugeridos” (seguidores que o usuário segue de volta e pessoas provavelmente conhecidas).
    - Para usuários +18: é possível, embora configura-se como padrão que as mensagens possam ser enviadas e recebidas por amigos.
- Downloads de vídeos criados pelos usuários:
    - Para vídeos criados por usuários entre 13-15 anos: por padrão e sem possibilidade de alteração, outros usuários não podem fazer o download dos vídeos.
    - Para vídeos criados por usuários entre 16-17 anos: por padrão, outros usuários não podem fazer o download dos vídeos, mas caso o usuário tenha optado por uma conta pública há a possibilidade de ativá-lo.
- Criação de adesivos a partir dos vídeos dos usuários:
    - Vídeos criados por usuários entre 13-15 anos: ninguém pode criar adesivos.
    - Vídeos criados por usuários entre 16-17 anos com contas públicas: por padrão, o controle é ativado apenas para “amigos”.
- Hospedagem de LIVES: só é permitido para usuários com mais de 18 anos.
- Limite de tempo de tela: Usuários entre 13-17: por padrão, esta configuração fica definida como uma hora.
- Notificações silenciosas: há autonomia para os pais definirem um cronograma para silenciar as notificações para contas de adolescentes. No entanto, por padrão:
    - Para usuários entre 13-15 anos: notificações são desativadas a partir das 21h.
- Para usuários de 16-17 anos: notificações são desativadas a partir das 22h.Ferramentas de recomendação e de interação com conteúdo:
    - Conteúdos criados por usuários entre 13-15 anos: Não aparecem no feed “Para Você”.
        - As configurações de comentários são restritas apenas para amigos, sem possibilidade de alteração.
        - A configuração "Sugerir sua conta para outros" está desativada por padrão, e, mesmo quando ativada, contas de adolescentes não são recomendadas a adultos.
    - Conteúdos criados por usuários entre 16-17 anos: passam a ser elegíveis para estarem no feed “Para Você”.

O ANEXO II apresenta, de forma visual e mais completa, as medidas de design adotadas pelo TikTok para promover e assegurar níveis adequados de privacidade e proteção de dados aos seus usuários.

Por fim, mas não menos importante, o TikTok possui diversas medidas de transparência, direcionadas tanto para os pais e responsáveis, quanto aos próprios adolescentes usuários (ver resposta III.5).

Essas são algumas medidas - não exaustivas - que o TikTok implementou para garantir a privacidade e melhor interesse dos adolescentes que utilizam a plataforma. No entanto, chama atenção para o fato de que a autoridade deve levar em conta a necessidade de parâmetros flexíveis e adaptáveis para diferentes produtos e serviços, considerando a disponibilidade tecnológica, a natureza e o propósito de cada um. Além disso, é essencial considerar o princípio do melhor esforço ao implementar essas medidas, garantindo que as soluções adotadas sejam práticas e proporcionais às capacidades e recursos de cada empresa.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais? [4200 caracteres]

O TikTok destaca que orientações claras da ANPD são necessárias para a segurança jurídica, dada a multiplicidade de disposições e atores na regulamentação. Parâmetros claros e flexíveis são cruciais para garantir práticas eficazes e proporcionais, respeitando a proteção dos dados dos menores e sua autonomia progressiva. Isso mitiga riscos e cria um ambiente mais seguro e estável juridicamente para todos.

O TikTok chama atenção para alguns temas que a ANPD deve levar em conta na formulação destas orientações.

Em primeiro lugar, o fato de que a verificação da idade dos usuários apresenta **desafios técnicos que podem variar significativamente conforme a natureza do serviço**. As orientações devem reconhecer que não há um único método de verificação superior a outros, pois a escolha depende do contexto específico, incluindo a finalidade e a natureza do tratamento dos dados, bem como o modelo de negócios envolvido.

Além disso, **não há um mecanismo infalível ou sempre superior em todos os contextos**. As orientações da ANPD devem considerar a necessidade de avaliar o cenário e a razoabilidade das ferramentas de verificação de idade para garantir sua eficácia e pertinência, considerando ainda a tecnologia atualmente disponível que seja minimamente segura para tal finalidade. Isso é crucial, especialmente considerando que esses mecanismos não são necessários apenas para grandes empresas de tecnologia, mas também para pequenas empresas, onde o custo de implementação pode ser significativamente mais impactante.

A possibilidade de as crianças burlarem verificações, como usar o celular dos pais, exemplifica a falibilidade inerente dessas medidas. Exigir que plataformas imponham controles exageradamente rígidos além da busca ativa de menores (o que já é uma

realidade para muitas plataformas que se preocupam em manter menores de 13 anos fora da plataforma) tende a ser desproporcional e tecnicamente desafiador. Muitas vezes, a decisão de permitir que uma criança (indivíduo com até 12 anos) acesse a plataforma é tomada pelo responsável legal fora do ambiente da plataforma, tornando inadequado responsabilizar o agente de tratamento. Adicionalmente, impor uma responsabilidade jurídica à plataforma que contrarie a decisão dos pais ou responsáveis pode ser desproporcional. Portanto, é essencial que as orientações da ANPD sobre mecanismos de verificação de idade considerem esses desafios e busquem um equilíbrio entre proteção e viabilidade técnica e contextual.

Por fim, a autoridade deve considerar que **as medidas de verificação de idade representam um desafio para toda a indústria e levantam potenciais riscos à privacidade.** Há debates importantes sobre a necessidade de equilibrar os riscos dos mecanismos de verificação de idade. Por exemplo, a Electronic Frontier Foundation (EFF) indicou, em 2023, que “os sistemas de verificação de idade são sistemas de vigilância” e, por isso, colocou-se contrária a leis que obriguem a sua implementação.

Conforme já indicado anteriormente, seria importante que a autoridade levasse em consideração, por exemplo, o princípio da minimização de dados em conjunto com o do melhor interesse, visto que ferramentas mais robustas podem implicar em maior coleta de dados, embora em certos casos garantam mais segurança e proteção.

O TikTok, inclusive, possui um sistema de verificação de idade neutro (que exige a inserção da data exata do nascimento pelo titular) para acesso à sua plataforma - destinada para usuários com mais de 13 anos - que busca equilibrar esses risco. [Para referência visual das ferramentas de verificação de idade para o acesso à plataforma ver o ANEXO III].

Destaca-se que a empresa busca equilibrar os riscos à privacidade com a necessidade de mecanismos de detecção eficazes. O TikTok tem sido proativo na remoção de usuários menores de 13 anos, implementando uma combinação de tecnologia e trabalho humano para detectar e remover eventuais contas de menores de 13 anos presentes na plataforma, dando o devido cumprimento aos Termos e Condições de Uso.

Além da identificação de menores, usuários podem denunciar contas, as quais serão revisadas por uma equipe devidamente capacitada para identificar e remover contas de usuários mais jovens que tenham eventualmente ingressado na plataforma. Há também verificação de idade para funcionalidades específicas na plataforma, nos casos em que o TikTok identificou um risco maior aos usuários mais jovens e tomou medidas para implementar níveis adicionais de verificação de idade.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais? [4200 caracteres]

O TikTok entende que a coleta de dados pessoais de crianças e adolescentes não deve ser limitada para além daquelas proibições já explícitas na legislação (ou seja, finalidades ilícitas), ao menos não de forma absoluta e sem consideração contextual.

Eventuais restrições devem levar em consideração violações ao melhor interesse desses titulares. Conforme já ressaltado, o fornecimento de balizas sobre o melhor interesse ajudaria a esclarecer esse ponto. Com relação à natureza dos dados, a LGPD e outras legislações não trazem qualquer tipo de limitação ao tratamento de dados de crianças e adolescentes (nem mesmo caso envolvam dados pessoais sensíveis, por exemplo). Desde que os agentes de tratamento indiquem uma base legal apropriada, adotem as medidas necessárias para garantir o cumprimento das obrigações da LGPD com relação a esses dados e que a atividade de tratamento seja compatível com o melhor interesse, não deve haver restrições para o tratamento de dados desses titulares.

Já com relação às finalidades do tratamento, o TikTok reforça que a formação de perfis comportamentais não deve ser considerada como uma atividade de tratamento que representa risco inerente aos usuários, inclusive no caso de crianças e adolescentes. Conforme já indicado na pergunta I.2., o perfilamento para fins de direcionamento de conteúdo - i.e., para oferecer conteúdo relevante ao usuário, sem fins publicitários - pode permitir que os usuários entrem em contato somente com conteúdos apropriados à sua faixa etária, evitando que os adolescentes se exponham a conteúdo mais maduro quando da utilização desses serviços e produtos. Nesse sentido, a prática de perfilamento pode desempenhar papel fundamental na segurança de menores de idade, em conformidade com seu melhor interesse.

Em concreto, a implementação dos "Níveis de Conteúdo" no TikTok é um exemplo. Para usuários entre 13 e 18 anos, o TikTok implementa medidas para que o conteúdo seja exibido de acordo com o nível de maturidade do titular. Em respeito à autonomia progressiva, essa ferramenta permite que adolescentes explorem e interajam com a plataforma de maneira adequada ao seu estágio de desenvolvimento, respeitando sua capacidade crescente de tomar decisões informadas e independentes. Ao limitar conteúdo mais maduro, o perfilamento protege os jovens enquanto apoia seu desenvolvimento, garantindo que a experiência online seja segura e apropriada para sua idade e maturidade. Alguns mecanismos disponíveis no modo de “sincronização familiar” (i.e., controle parental, conforme explicado na questão abaixo) também dependem de mecanismos que consigam adequar o conteúdo ao público-alvo - tais como os filtros necessários para possibilitar que os pais e responsáveis limitem a exposição de seus filhos adolescentes a conteúdo que pode não ser apropriado ou adequado para eles (i.e., configuração “modo restrito”).

Nesse sentido, restrições a atividades de perfilamento devem ser impostas devido à violação do melhor interesse da criança e do adolescente, conforme as leis do panorama regulatório brasileiro, e não simplesmente pela realização da atividade em abstrato.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital? [4200 caracteres]

O TikTok entende que medidas de proteção de privacidade para menores devem ser adaptáveis aos níveis de maturidade e autonomia de cada usuário em desenvolvimento, respeitando a autonomia progressiva. Assim, as configurações de privacidade não devem ser excessivamente rígidas, mas flexíveis e adequadas, permitindo ajustes que correspondam ao conteúdo apropriado para a idade, ao estágio de desenvolvimento do usuário e ao modelo de negócio em questão. Essa abordagem reconhece que diferentes idades e níveis de compreensão requerem diferentes níveis de proteção e interação, levando em conta a autonomia progressiva e, portanto, o melhor interesse da criança e do adolescente, conforme exige a legislação brasileira.

O já citado Guia da ICO menciona a Convenção das Nações Unidas sobre os Direitos da Criança (UNCRC), que indica reconhecer o direito do menor de acordo com suas capacidades em evolução, de ter voz em assuntos que a afetam. No capítulo sobre controle parental, o Guia exemplifica essa abordagem, indicando, dentre outros fatores, que é necessário que pais e responsáveis sejam transparentes com as crianças e adolescentes caso os controles parentais estejam ativados e caso estejam sendo rastreados e/ou monitorados. Para isso, devem ser apresentadas informações apropriadas, garantindo que o menor entenda que esses controles estão em uso - e que ferramentas não invadam a privacidade do usuário menor de idade.

Como exemplo deste tipo de mecanismo, o TikTok possui a ferramenta de sicronização familiar, que permite a vinculação das contas dos pais às dos filhos adolescentes, facilitando a gestão de configurações relacionadas a conteúdo, privacidade e bem-estar. Com esta ferramenta, pais, mães ou responsáveis podem configurar controles específicos visando à segurança do usuário adolescente. Este modo de sincronização familiar permite que pais e responsáveis personalizem configurações, como o tempo de tela diário. Os responsáveis podem ajustar o tempo de uso, aplicá-lo a todos os dispositivos do adolescente e definir um código de acesso para uso adicional após o limite ser atingido. Além disso, a ferramenta permite a ativação do Modo Restrito, que reduz a visualização de conteúdos potencialmente inadequados para certos públicos, como temas maduros ou complexos. Ao ativar este modo, algumas funcionalidades da plataforma são desabilitadas. Outras funcionalidades que visam à segurança dos adolescentes incluem a aplicação de filtros a comentários publicados, restringindo comentários inadequados e ofensivos, e a restrição ou desativação total de quem pode enviar mensagens ao adolescente.

O TikTok também reforça a importância da promoção da cultura de diálogo dos pais e responsáveis com os menores, e o papel que a ANPD pode desempenhar nesse contexto. Incentivar os pais e responsáveis a discutir e explicar a ativação dessas configurações com os adolescentes é fundamental, pois a proteção da segurança, privacidade e autonomia progressiva do menor também é responsabilidade da família, conforme determina o Artigo 5 da Convenção sobre os Direitos da Criança[1]. Tendo isso em vista, o TikTok elabora guias direcionados especificamente aos pais e responsáveis, com linguagem clara e transparente, facilitando a navegação na plataforma e o entendimento das ferramentas e mecanismos disponíveis para auxiliá-los em seu dever de supervisão. Especificamente, o Guia para Pais e Responsáveis explicitamente incentiva a discussão dos recursos de Controle Parental com os adolescentes e explica a decisão de ativá-los. Essa medida está alinhada com a lógica de promover maior conhecimento e compreensão sobre mecanismos digitais tanto do lado dos pais quanto

dos adolescentes. O Guia em questão também fornece informações gerais sobre preocupações comuns de segurança na internet.

Outro exemplo de boa prática é a exibição de uma tela de aviso, para usuários entre 13 e 18 anos, que incentiva os adolescentes a manterem seus pais ou responsáveis legais informados sobre o uso do aplicativo. Ao exibir o aviso de forma clara e proeminente, a tela funciona tanto como um lembrete de que os pais e responsáveis legais devem ser informados sobre o uso do TikTok, quanto como uma ferramenta educacional para os usuários menores. O aviso enfatiza efetivamente a importância da supervisão parental e contribui para uma experiência online segura para menores.

Para uma referência visual de algumas das medidas implementadas pelo TikTok para manter o ambiente seguro e de apoio para famílias e adolescentes, ver o ANEXO IV.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes? [4200 caracteres]

O TikTok entende que, com relação à transparência e ao fornecimento de informações simples, claras e acessíveis, há algumas boas práticas que podem ser observadas pelos mais diversos agentes de tratamento de forma adaptável a seus modelos de negócios, natureza do produto/serviço e tendo em vista as tecnologias disponíveis.

A primeira delas consiste no entendimento de que a Política de Privacidade (“PP”), embora instrumento fundamental e indispensável, não precisa ser exibida constantemente para o usuário e/ou ao seu responsável legal, como fonte exclusiva de informação sobre tratamentos, sob o risco de resultar em fadiga. A exibição contínua da PP pode causar desatenção e desinteresse, reduzindo a eficácia da comunicação e a compreensão das informações importantes. O usuário pode ignorar alertas críticos, comprometendo a transparência e a confiança no tratamento de dados.

Para evitar essa sobrecarga e garantir uma comunicação efetiva, o TikTok entende como mais eficiente apresentar a PP e outras informações em momentos específicos e relevantes (e.g., relacionados diretamente a um determinado tratamento), assegurando que o usuário esteja atento e receptivo às informações necessárias. As informações fornecidas aos usuários ou pais precisam ser específicas e facilmente compreensíveis. Assim, apenas aumentar a quantidade de informações não garante maior transparência, especialmente se estiverem diante de informações complexas.

O TikTok, em particular, opta por manter a PP visível e em local de fácil acesso, na página inicial da plataforma. A empresa não apenas deixa a PP visível, mas também fornece um link para a "Central de Privacidade", que direciona o usuário a uma página explicando, de forma breve e simples, a preocupação da empresa com a privacidade, contextualizando-o antes de direcioná-lo à PP.

Outros meios além da PP são bem-vindos e corroboram com o dever de transparência. Ausente a proibição legal de que a PP seja o único meio para fornecer transparência, informações adicionais sobre o tratamento de menores podem ser incluídas em

documentos separados, como artigos na central de transparência e ajuda, ou mesmo notícias veiculadas pelos agentes, que indiquem como os dados tratados estão associados a finalidades legítimas, específicas, explícitas e informadas ao titular. A especificidade da transparência pode ser desenvolvida em outros recursos, especialmente durante a utilização de produtos e serviços pelos adolescentes, através de notificações, por exemplo.

A transparência fornecida deve ser adequada aos usuários. Para isso, o TikTok entende que meios como portais podem facilitar a compreensão das informações por adolescentes, em particular ao incorporar ícones visuais, vídeos, áudios, conteúdo interativo e linguagem simplificada e cotidiana a este público.

É também importante dar suporte e fornecer transparência apropriada aos pais e responsáveis legais, para que tenham acesso a informações sobre as práticas de tratamento de dados pessoais realizadas, recursos de supervisão parental, entre outros. Nesse contexto, o TikTok reconhece a importância de permitir que os agentes de tratamento sejam criativos na elaboração de instrumentos de transparência.

Ressalta-se, no entanto, que a autoridade deve levar em conta que a transparência deve observar os limites técnicos e os segredos comerciais e industriais dos agentes de tratamento. Fornecer informações excessivas sobre as ferramentas de tratamento de dados de menores pode permitir que agentes mal-intencionados burlem mecanismos de segurança, colocando em risco a segurança desses usuários. Portanto, é necessário estabelecer uma transparência adequada, visando os melhores interesses desses titulares.

Por fim, é importante manter uma parceria constante com pais, responsáveis legais e os próprios adolescentes para melhorar os recursos de transparência disponíveis, visando aumentar a compreensão das definições de privacidade e segurança.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional? [4200 caracteres]

Por fim, o TikTok entende que há um outro ponto que merece atenção da autoridade no que diz respeito a orientações de tratamento de dados pessoais de crianças e adolescentes:

É necessário que a autoridade se manifeste sobre os requisitos para a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a identificação de tratamentos de dados pessoais de alto risco. Atualmente, a existência de dados pessoais de crianças e adolescentes é considerada um critério para classificar um tratamento de dados como de alto risco. No entanto, estabelecer automaticamente essa classificação pode trazer consequências negativas e ineficiências. Por exemplo, tratamentos de dados que não deveriam ser considerados de alto risco podem ser inadvertidamente classificados dessa forma apenas por envolverem dados de menores. Isso pode resultar em processos excessivamente rigorosos e desnecessários para certos tratamentos de dados, sobrecarregando os controladores e desviando recursos que poderiam ser melhor

empregados em áreas realmente críticas. Portanto, é crucial que a autoridade forneça orientações claras e específicas sobre como identificar e tratar dados pessoais de crianças e adolescentes, evitando generalizações que possam levar a ineficiências e classificações equivocadas.

ANEXO I - Doutrina Civilista

Conforme indicado na resposta II.2., o Código Civil não foi concebido no contexto digital. É, portanto, necessário adaptá-lo à realidade moderna do uso de plataformas digitais. A capacidade civil e as formas de assistência para adolescentes devem ser mais flexíveis, especialmente em relação às atividades online consideradas "atos corriqueiros". Professores e doutrinadores brasileiros corroboram com esse entendimento, defendendo uma abordagem flexível dos institutos de representação e assistência como o uso de uma plataforma projetada para criação de conteúdo, consumo de vídeos e interação com outros usuários.

a) Trechos de SCHREIBER, Anderson. Manual de Direito Civil Contemporâneo. Capítulo sobre "Releitura das Incapacidades".

“O instituto das incapacidades tem sido objeto de substanciosa releitura crítica nos últimos anos. A proteção à dignidade humana, que se reflete na garantia de autodeterminação da pessoa natural, impõe a flexibilização do regime codificado das incapacidades, que pretendia retirar por completo o incapaz da vida privada.

A lógica empregada no Código Civil, segundo a qual a pessoa ou é capaz ou é incapaz (lógica do tudo ou nada), não mais se coaduna com a máxima proteção à pessoa. Hoje, impõe-se a modulação da incapacidade, reconhecendo-se à pessoa a mais ampla participação possível nos atos da vida civil, como já se vê em exemplos preciosos como o Estatuto da Criança e do Adolescente, que reconhece o direito do adolescente maior de 12 anos de ser ouvido no processo de adoção.

As ‘escolhas’ do incapaz ficavam, assim, pendentes de participação alheia, indispensável à validade e eficácia da sua própria declaração de vontade. A esse modelo abstrato e puramente estrutural contrapôs-se, com especial força nas últimas décadas, a realidade concreta: em numerosas situações, os incapazes acabavam tolhidos de uma parcela de autonomia que estavam em plenas condições de exercer livremente, não apenas no campo patrimonial, mas também no campo existencial. Quem não tem plenas condições de gerir sozinho seu patrimônio não será necessariamente inapto para realizar escolhas existenciais.

E mesmo no campo patrimonial é possível elencar atos que uma pessoa não tem condições de realizar (aquisição e alienação de imóveis, por exemplo) e outros cuja prática não oferece perigo aos seus interesses (contratos de menor monta, recebimento de aluguéis etc.). Um regime abstrato e geral de “proteção” ao incapaz

acabou, na prática, se convertendo em instrumento de abordagem excludente. A própria designação de certa pessoa como "incapaz" – expressão que, por si só, já é carregada de significado negativo – assume, não raro, caráter discriminatório, que se vê com alguma frequência em casos envolvendo silvícolas, pródigos ou toxicômanos. O rótulo generaliza situações inteiramente distintas, que mereceriam da ordem jurídica remédios diferenciados em grau e natureza. O Código Civil de 2002 falhou nesse sentido, ao reproduzir com impressionante dose de desatualidade o regime de incapacidade contido na codificação de 1916. Transcorrido quase um século, nada se alterou para os incapazes".

b) Trecho de TEPEDINO, Gustavo. Esboço de uma classificação funcional dos atos jurídicos. Instituto Brasileiro de Direito Civil.

"*O que se pretende propor, para a reflexão contemporânea, é a necessidade de se reler a doutrina dos comportamentos socialmente típicos, a partir, não já do afastamento do elemento volitivo como motor da livre iniciativa, mas da distinção entre a vontade negocial e a vontade contratual. O negócio jurídico mantém-se vinculado ao controle estabelecido pelo Código Civil. Ao seu lado, contudo, uma série de atividades socialmente típicas, decorrentes de atos não negociais, é valorada positivamente e a ordem jurídica reconhece, como jurígenos, seus efeitos. Enquanto no negócio jurídico a declaração de vontade hígida é um prius para a sua validade (elemento essencial), nas atividades socialmente típicas a vontade suscita verificação in posterius, a partir dos efeitos por elas produzidos, independentemente de declaração destinada à instauração do vínculo, conferindo-se juridicidade a situações jurídicas que, de outra forma, não poderiam ser admitidas.*

A rigor, a admissão da relação contratual sem negócio permite atribuir juridicidade a efeitos socialmente reconhecidos, a partir de qualificação a posteriori da função da atividade realizada, estabelecendo-se, dessa forma, controle de merecimento de tutela, à luz da legalidade constitucional, acerca de atos praticados sem negócio jurídico de instauração (mas que, nem por isso, podem ser considerados fora da lei), cuja eficácia, de ordinário, é mais restrita do que a gama de efeitos almejados pelo negócio. Basta lembrar as hipóteses do funcionário público cujo acesso à carreira não se deu por concurso público; ou do vínculo empregatício do apontador de jogo do bicho; ou do policial militar em empresa de segurança privada, a despeito de vedação legal expressa; ou do menor que adquire, por si mesmo, produtos ou serviços; ou ainda o exemplo dos sócios de sociedade irregular ou da pessoa que integra modalidade de família inadmitida pelo direito.

Em todos esses casos, a invalidade dos negócios não exclui a admissibilidade, para certos fins, de eficácia jurídica à atividade desenvolvida. E somente graças a

artificialismo retórico se poderia afirmar que se pretendeu, em tais hipóteses, celebrar ou extinguir uma série de negócios, alçando-se o mesmo efeito rejeitado ora pela vontade expressa do declarante, ora pela lei. Torna-se, assim, incongruente, nesses casos, falar-se em negócio jurídico, cuja admissão colidiria com matéria de ordem pública, que pauta a teoria das capacidades, das formas ad substantiam e da licitude dos bens passíveis de circulação."

c) Trecho de LEAL, Sheila do Rocio Cercal Santos. Contratos eletrônicos: validade jurídica dos contratos via Internet.

"Embora as normas sobre incapacidade tenham por escopo final a proteção dos incapazes, a doutrina e a jurisprudência têm amenizado a sua aplicação, considerando válidos alguns atos corriqueiros praticados por menores, como, por exemplo, a compra de um lanche, de entrada para o cinema, o transporte de ônibus, enfim, atos nos quais pode presumir a autorização dos pais".

d) Trechos de SILVA, Bruno César da; FRASSETTO, Flávio Américo; SCHWEIKERT, Peter Gabriel Molinari. Imperiosa revisão do regime de incapacidades pela comissão de atualização do Código Civil. Conjur, 26 nov. 2023. Disponível em: https://www.conjur.com.br/2023-nov-26/imperiosa-revisao-do-regime-de-incapacidades-pela-comissao-de-atualizacao-do-codigo-civil/

"A autonomia progressiva das crianças e adolescentes está expressamente prevista no artigo 5º da Convenção das Nações Unidas sobre os Direitos da Criança (CDC) [5], segundo o qual os Estados devem respeitar as responsabilidades, os direitos e os deveres dos pais ou dos responsáveis de proporcionar à criança instrução e orientação adequadas e acordes com a evolução de sua capacidade no exercício dos direitos reconhecidos.

Uma compreensão mais abrangente da capacidade evolutiva passa também pelo reconhecimento do direito de participação como uma das bases na qual se assenta a Convenção dos Direitos da Criança. Nesse sentido, o artigo 12 da referida Convenção que crianças e adolescentes têm o direito de participar ativamente de todas as decisões que lhe afetem, devendo sua opinião ser considerada avaliando-se o nível de maturidade.

A leitura conjunta dos artigos 5º e 12 da Convenção conduz ao entendimento de que toda criança e todo adolescente tem o direito a sistemas de apoio, bem como

ao incentivo e ao reconhecimento de suas habilidades para tomar decisões de acordo com suas preferências e desejos. Impõe-se, assim, segundo Kalline Eler, um ônus aos pais e ao Estado, que devem permitir que a criança assuma progressivamente a responsabilidade pelas decisões sobre as quais elas demonstram estar aptas e dispostas a tomar [6].

Isso impacta o próprio exercício da responsabilidade parental, na medida em que deve também levar em consideração a capacidade de crianças e adolescentes exercerem seus direitos por conta própria, reduzindo-se a ingerência parental progressivamente, na medida em que os sujeitos em desenvolvimento adquiram competências cada vez maiores.

Trata-se de um conceito central para o equilíbrio almejado pela Convenção entre o reconhecimento de crianças e adolescentes enquanto agentes ativos de sua própria vida e a necessidade de sua proteção em função da maturidade em desenvolvimento.

Não por outro motivo que o Comitê da ONU sobre Direitos da Criança, nos Comentários Gerais nº 12/2009 e 25/2016 reforça a obrigação de que os países signatários garantam em suas legislações internas mecanismos para dar efetividade a este direito. Na mesma linha, a Comissão Interamericana de Direitos Humanos, desde 2017, recomenda aos Estados membros a revisão de toda a legislação relativa à capacidade e ao exercício jurídico de direitos autônomos e acesso a serviços no caso das crianças e adolescentes, à luz do princípio da autonomia progressiva e de forma compatível com o direito à proteção e o princípio do superior interesse da criança [7].

Logo se nota, portanto, uma verdadeira e irremediável incompatibilidade do regime de incapacidades estabelecido pelo Código Civil com a Doutrina da Proteção Integral.

Não se pode fechar os olhos para o fato de que a teoria das capacidades civilista, historicamente, foi fundamentada na necessidade de controle e disciplinamento da infância, advinda de um contexto que concebia crianças como seres passivos, destinatários da ação dos adultos, sem opinião ou vontade juridicamente relevantes. Partia-se da ideia de que os adultos sabiam o que seria o melhor para crianças e adolescentes, podendo, assim, determinar o que é importante em suas vidas [8].

Por outro lado, sociologicamente, a incapacidade civil de crianças e adolescentes representa(va) uma justificativa naturalizada da invisibilidade cívica deste grupo, repercutindo diretamente no condicionamento e restrição de seus direitos cíveis, políticos, sociais, culturais e econômicos. [...]"

Segurança e proteção à privacidade de adolescentes no TikTok

No TikTok, nos preocupamos com as necessidades específicas de desenvolvimento dos adolescentes, oferecendo experiências diferentes para adolescentes de 13 a 15 anos e de 16 a 17 anos.

Recurso	13-15	16-17	18+
Mensagens diretas	Não permitido	Desligadas, por padrão	Amigos, por padrão
Visibilidade da conta	Privada, por padrão	Pré-selecionada como Privada, com opção para definir como Pública	Pública
Elegibilidade para o feed Para Você	Inelegível	Elegível	Elegível
Download de vídeos	Não permitido	Desligado, por padrão	Permitido
Regras de comentários	Apenas amigos podem comentar	Apenas seguidores podem comentar, por padrão	Todos podem comentar
Dueto e Costurar	Não permitido	Desligado, por padrão	Permitido
Fazer LIVE	Não permitido	Não permitido	Permitido
Tempo de tela por dia	60 minutos	60 minutos	Escolha pessoal
Presentes virtuais	Não permitido	Não permitido	Escolha pessoal
Notificações noturnas	Desativadas a partir das 21h	Desativadas a partir das 22h	Escolha pessoal

Nós trabalhamos para educar as famílias sobre as proteções disponíveis para ajudá-las a gerenciar sua experiência no TikTok em nossos Portal da Juventude, Centro de Segurança, e por meio de parcerias com organizações de professores, ONGs de segurança para jovens e instituições educacionais em todo o mundo.

TikTok

ANEXO III - Ferramentas de verificação de idade para o acesso à plataforma

Conforme indicado nos Termos de Uso do TikTok, a plataforma é destinada para pessoas com mais de 13 anos de idade. O TikTok implementou recurso de verificação etária neutro, de acordo com os padrões da indústria, que exige que os usuários insiram sua data de nascimento antes de criar uma conta. O ano de nascimento não é padronizado para uma data que identificaria o indivíduo como maior de 13 anos.

As capturas de tela abaixo refletem todo o fluxo de cadastro quando um indivíduo baixa o aplicativo TikTok:

Captura de tela ao abrir o aplicativo do Tiktok pela primeira vez

Captura de tela exigindo a divulgação da idade de nascimento do usuário

Ao clicar na opção de criar uma conta, os usuários são questionados sobre sua data de nascimento, assim como no processo de cadastro do site.

Captura de tela exigindo o número de telefone celular do usuário

Se o usuário tiver menos de 13 anos, o processo de registro da conta é imediatamente interrompido e não poderá ter continuidade. Se o usuário tiver 13 anos ou mais, o usuário deverá fornecer seu número de telefone celular.

Esse ponto é relevante, pois o TikTok pode ser usado por adultos (maiores de 18 anos de idade) e adolescentes (13 a 18 anos de idade). O serviço não se destina a menores de 13 anos de idade e essa restrição é claramente apresentada aos usuários nos Termos de Serviço:

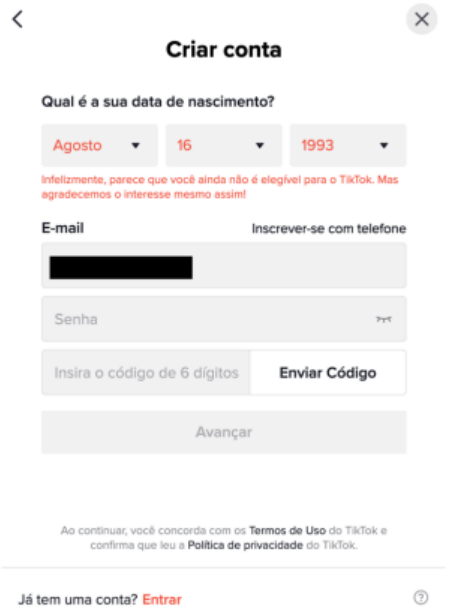
Seção 11, "e", dos Termos de Serviço do TikTok estabelece que o TikTok não pode ser utilizado por pessoas com menos de 13 anos de idade: "11. Condições adicionais (...) e. Limitação etária. Os Serviços destinam-se exclusivamente a pessoas com idade de 13 anos ou mais(sujeito às limitações adicionais porventura estabelecidas nos Termos Suplementares – Específicos da Região). Ao utilizar os Serviços, você estará confirmando que tem a idade mínima aqui especificada. Se chegar ao nosso conhecimento que alguma pessoa com idade inferior à idade mínima estabelecida acima está utilizando os Serviços, encerraremos a conta do usuário em questão."

Esses Termos devem ser aceitos para que os adolescentes possam continuar a utilizar o TikTok

Se um indivíduo inserir uma data de nascimento abaixo de 13 anos, ele não poderá registrar uma conta no TikTok e será impedido de tentar novamente por um período de tempo. O usuário não sabe que o motivo do bloqueio é a sua data de nascimento informada. Se, imediatamente após ser impedido, um menor com idade inferior a 13 anos tentar novamente criar uma conta, mentindo sobre a sua idade e introduzindo uma data de nascimento adulta, o TikTok detecta esta tentativa e a bloqueia, impedindo a criação de uma conta através do mesmo dispositivo ou endereço de e-mail.

Isso pode ser visto nas capturas de tela abaixo:

Captura de tela da mensagem mostrada aos novos usuários no aplicativo, explicando que não é possível criar uma conta caso tenham menos de 13 anos de idade.



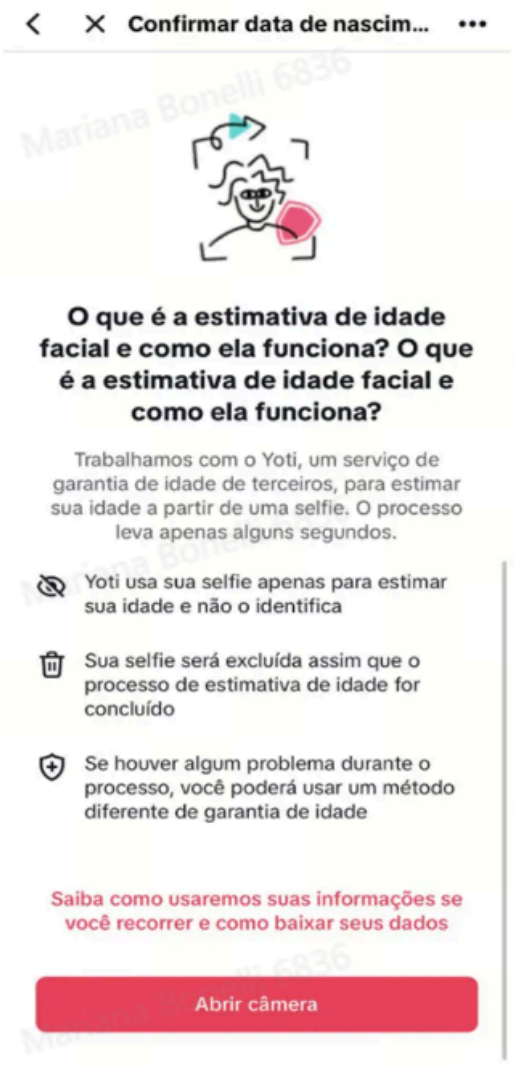
Captura de tela da mensagem que demonstra o impedimento à nova tentativa de criação de conta por menor de 13 anos, que mentiu sobre a sua idade após ter revelado anteriormente que tinha menos de 13 anos de idade

Além disso, com base no compromisso assumido pelo TikTok em proteger seus usuários, foi implementada uma nova tecnologia que visa reforçar as proteções existentes e evitar que menores de 13 anos estejam na plataforma. Nesse sentido, o TikTok implementou o recurso da Yoti, uma empresa que oferece tecnologia para estimar a idade de uma pessoa sem identificá-la. Ela é usada pela plataforma para verificar a idade nos seguintes casos:

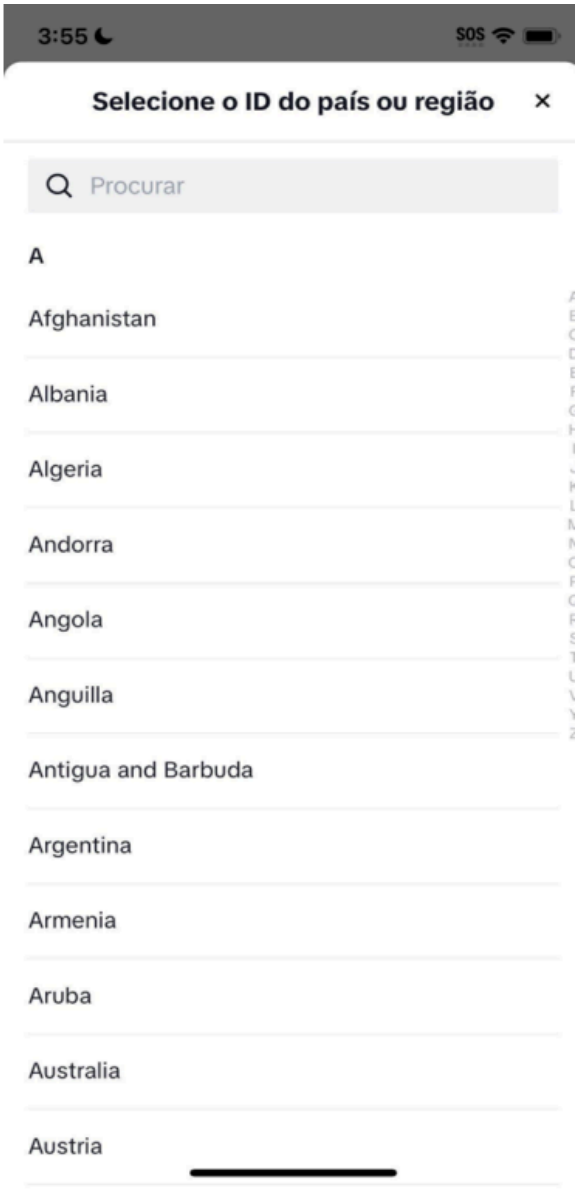
- Quando um usuário menor de 18 anos (13 a 17) tenta editar sua data de nascimento, mudando a sua idade para acima de 18 anos.
    - Em tal situação, o usuário será solicitado a verificar sua idade por meio de um dos diversos métodos implementados pelo TikTok, incluindo a medida de estimativa de idade (Yoti).
        - Para alterar a idade para mais de 18 anos, o usuário deverá demonstrar sua idade por meio da estimativa de idade facial (Yoti), da validação de identidade, ou de um cartão de crédito. Para alterações de idade que ainda mantenham o indivíduo como menor (entre 13 e 17), o usuário poderá fazê-lo por meio da validação de identidade ou de uma foto com um adulto.
- Quando um usuário que teve a conta banida por suspeita de ser menor de 13 anos apela por meio dos canais do TikTok, informando uma idade superior a 18 anos.
- Quando um usuário deseja realizar uma transmissão ao vivo (LIVE), já que o uso desta funcionalidade é permitida apenas para usuários maiores de 18 anos.

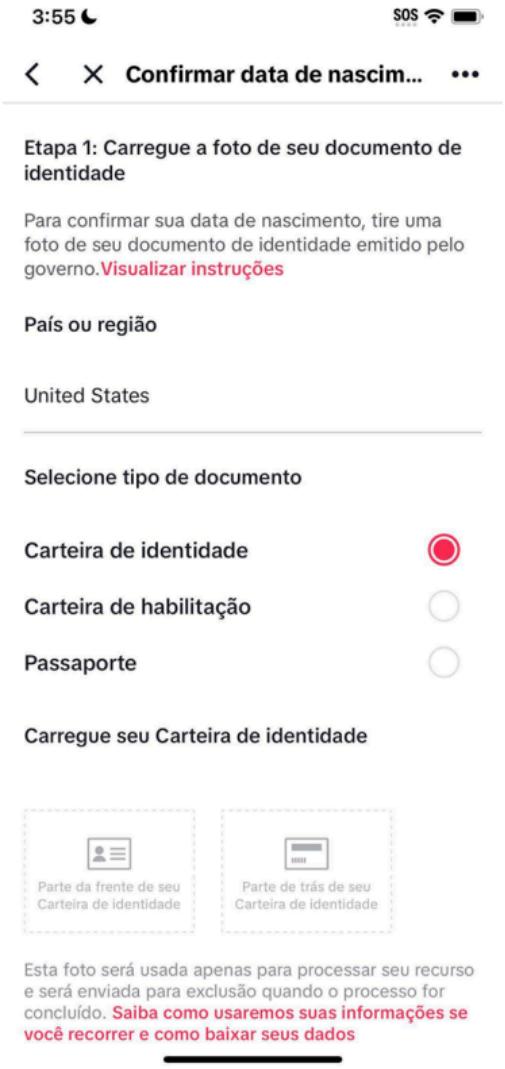
Abaixo estão capturas de tela demonstrando como as ferramentas descritas no primeiro item funcionam na prática no aplicativo TikTok:

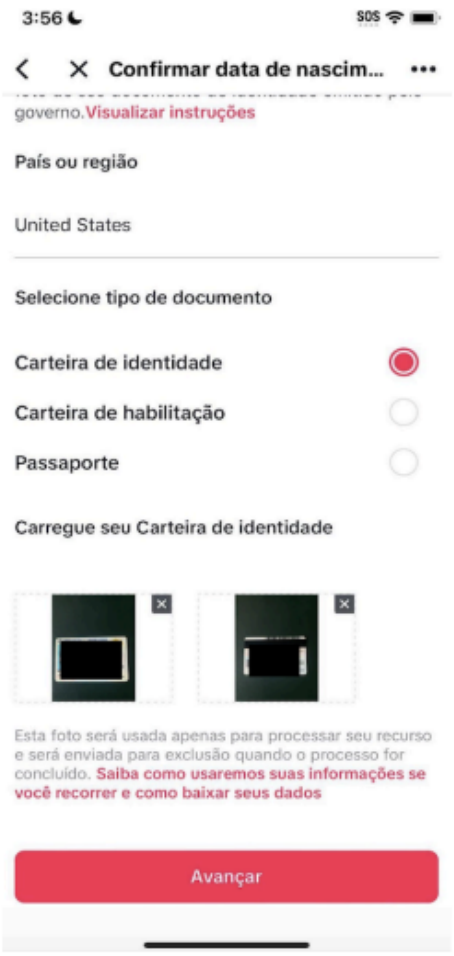
1. Yoti



2. Documento de Identidade


3:55
SOS
Selecione o ID do país ou região
Procurar
A
Afghanistan
Albania
Algeria
Andorra
Angola
Anguilla
Antigua and Barbuda
Argentina
Armenia
Aruba
Australia
Austria


3:55
Confirmar data de nascim...
Etapa 1: Carregue a foto de seu documento de identidade
Para confirmar sua data de nascimento, tire uma foto de seu documento de identidade emitido pelo governo.Visualizar instruções
País ou região
United States
Selecione tipo de documento
Carteira de identidade
Carteira de habilitação
Passaporte
Carregue seu Carteira de identidade
Parte da frente de seu Carteira de identidade
Parte de trás de seu Carteira de identidade
Esta foto será usada apenas para processar seu recurso e será enviada para exclusão quando o processo for concluído. Saiba como usaremos suas informações se você recorrer e como baixar seus dados


3:56
Confirmar data de nascim...
governo.Visualizar instruções
País ou região
United States
Selecione tipo de documento
Carteira de identidade
Carteira de habilitação
Passaporte
Carregue seu Carteira de identidade
Esta foto será usada apenas para processar seu recurso e será enviada para exclusão quando o processo for concluído. Saiba como usaremos suas informações se você recorrer e como baixar seus dados
Avançar

3. Cartão de Crédito

4. Foto com um adulto (pais ou responsável legal)

Por fim, ressalta-se que o TikTok, para garantir que seus usuários sejam de fato indivíduos com mais de 13 anos de idade, não se limita à triagem de idade. A empresa treina sua equipe de moderação de segurança para estar alerta a admissões explícitas de usuários que possam ter menos de 13 anos. Além disso, implementou uma série de medidas para remover a conta de menores de 13 anos que consigam se cadastrar com informações falsas, como canais de denúncia para que outros usuários e terceiros denunciem contas suspeitas de menores de 13 anos.

A Plataforma também está continuamente revisando o conteúdo compartilhado, em busca de evidências de atividades suspeitas de menores de 13 anos de idade, por meio de revisão automática e manual. O TikTok usa informações, como palavras-chave ou relatórios de usuários, para identificar possíveis contas de menores de 13 anos. Se, depois de analisar todas as informações relevantes, a equipe de segurança do TikTok determinar que uma conta possa pertencer a um menor de 13 anos, a conta será suspensa e removida.

TikTok

ANEXO IV

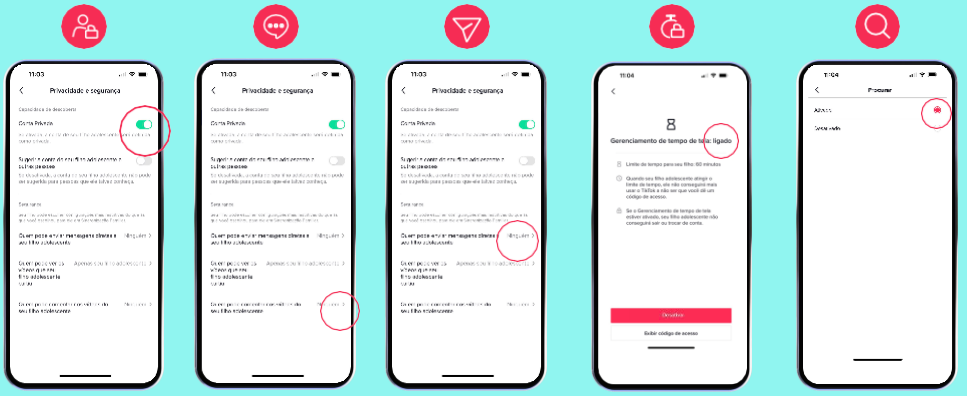
Mantendo o TikTok como um local seguro e de apoio para famílias e adolescentes

Sabemos que nossa plataforma se tornou um importante espaço para que os jovens expressem sua criatividade. Nós tomamos algumas atitudes para fazer do TikTok um lugar confiável e acolhedor para famílias e adolescentes.

Ferramentas para as famílias

A **Sincronização Familiar** permite que um pai ou responsável conecte sua conta TikTok com a conta de seus adolescentes para administrar uma variedade de configurações de conteúdo e privacidade.

As contas dos responsáveis vinculadas às dos adolescentes através da Sincronização Familiar receberão notificações com conselhos sobre como abordar a alfabetização digital e conversas de segurança. Essa informações também podem ser encontradas em nosso **Guia de Pais e Responsáveis**.



Administração de conta: defina a conta dos adolescentes como privada ou pública.

Comentários: restrinja quem pode comentar nos vídeos do seu adolescente.

Mensagens diretas: restrinja quem pode mandar mensagens para a conta.

Limite diário de tela: controle a quantidade de tempo gasto no TikTok diariamente. As contas de usuários com menos de 18 anos são automaticamente definidas para um limite diário de 60 minutos de tempo de tela.

Configurações de busca: restrinja a capacidade de buscar conteúdo.

Notificações silenciosas: defina um horário para silenciar as notificações para contas de adolescentes. Aqueles entre 13 a 15 anos já não recebem notificações a partir das 21 h e contas de pessoas de 16 a 17 anos têm notificações desativadas a partir das 22 h.

Padrão de Privacidade

Quando os jovens começam sua jornada digital, acreditamos que é importante fornecer a eles configurações e controles de privacidade adequados à idade.

Usuários de 13 a 15 anos não têm permissão de enviar ou receber mensagens diretas.

Download de vídeos, Costurar e Dueto estão disponíveis apenas nos conteúdo criados por pessoas com mais de 16 anos.

Apenas pessoas com 18 anos ou mais podem realizar transmissões ao vivo.

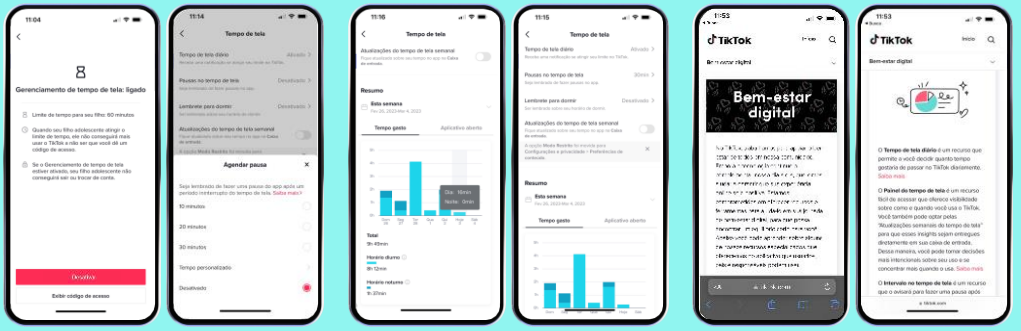
As contas de usuários de 13 a 15 anos são definidas como privadas por padrão, o que significa que apenas alguém que é aprovado como um seguidor pode ver seus vídeos.

Quando alguém de 16 a 17 anos cria uma conta, a definição de quem pode enviar a eles uma mensagem direta é definida como "Ninguém" por padrão.

Ao publicar seu primeiro vídeo, nós pedimos aos jovens de 13 a 15 anos que autorizem quem pode assistir ao seu conteúdo.

Bem-estar digital

Estamos comprometidos em fornecer ferramentas e recursos aos adolescentes e às famílias para ajudar a todos ao longo de sua jornada de bem-estar digital.



Intervalos de tempo de tela: lembra o adolescente de fazer uma pausa do aplicativo após um período de tempo ininterrupto de tela.

Atualizações de tempo da tela: fornece informações semanais sobre o tempo gasto com o aplicativo.

Painel de controle de tempo da tela: compartilha uma visão geral de como muito tempo foi gasto no TikTok.

Recursos para a juventude

No Portal da Juventude do TikTok, os adolescentes podem aprender sobre as melhores práticas para se manterem seguros online e terem uma experiência positiva e enriquecedora no TikTok.

Também fornecemos um resumo de "fácil leitura" de nossa Política de Privacidade projetada especificamente para menores de 18 anos. Desta forma, qualquer pessoa pode ler sobre como usamos, tratamos e armazenamos dados de uma forma livre de jargões.

Parceria com especialistas

Trabalhamos com os principais especialistas da indústria, organizações não governamentais e associações ao redor do mundo, incluindo SaferNet, Instituto DimiCuida, ConnectSafely e Technology Coalition, para ajudar a garantir que nossas políticas e ferramentas continuem a promover um ambiente seguro e mais acolhedor para nossa comunidade.

ENC: Contribuição ABEAR - Tomada de Subsídios sobre o tratamento de dados de crianças e adolescentes

ANPD - Normatizacao <normatizacao@anpd.gov.br>

Ter, 2024-07-16 14:55

Para:Paulo Cesar dos Santos <paulo.cesar@anpd.gov.br>

1 anexos (177 KB)

TOMADA DE SUBSÍDIOS - Tratamento de Dados Pessoais de Crianças e Adolescentes.pdf;

ANPD

Coordenação-Geral de Normatização
Autoridade Nacional de Proteção de Dados - ANPD
☎ **+55** (61) 2025-8144
✉ **normatizacao@anpd.gov.br**

De: Patricia Perez <patricia@snea.com.br>
Enviado: terça-feira, 16 de julho de 2024 11:57
Para: ANPD - Normatizacao <normatizacao@anpd.gov.br>
Assunto: Contribuição ABEAR - Tomada de Subsídios sobre o tratamento de dados de crianças e adolescentes

Você não costuma receber emails de patricia@snea.com.br. Saiba por que isso é importante

Prezados Senhores, boa tarde!

Segue em anexo, a contribuição das associadas da ABEAR à Tomada de Subsídios sobre o tratamento de dados de crianças e adolescentes

Solicitamos a confirmação de recebimento.

Desde já agradecemos e estamos à disposição para eventuais dúvidas.

Att.,

SNEA 90 anos
SINDICATO NACIONAL DAS EMPRESAS AEROVIÁRIAS

Patricia C. R. Perez
Assistente Diretoria
Tel: +55 11 2369-6007 | +55 21 98554-5629
Av. Lavandisca, 777 - Conj. 22
04515-011 | Moema | São Paulo
patricia@snea.com.br | www.snea.com.br

I - Princípio do melhor interesse

1. **Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?**

Identificamos duas questões nas quais a atuação orientativa da Autoridade se mostra relevante: (a) como exercitar o legítimo interesse atrelado à contextos que dizem respeito ao melhor interesse da criança; e (b) apresentação de diretrizes para mitigação de riscos e sopesamento de interesses dos menores.

a) Legítimo interesse e melhor interesse da criança e do adolescente:

Entendemos ser necessário obter da ANPD parâmetros mais claros sobre como exercitar o legítimo interesse atrelado à contextos que dizem respeito ao melhor interesse da criança, por meio de novos exemplos mais complexos, visando superar interpretações contraditórias. O direcionamento pela Autoridade auxiliará a mensurar corretamente e reconhecer o que pode ser flexibilizado quando em conflito de determinados outros interesses, e ainda assim continuar protegendo os menores que dele dependem.

Nesse aspecto, sugerimos que a Autoridade leve em consideração a razão de ser do legítimo interesse e a sua complementariedade com o melhor interesse da criança, de forma a não propor parâmetros que sejam excessivamente onerosos ao controlador, tornando inviável a aplicação da base legal nesse contexto. Por exemplo, entendemos que exigir um teste de balanceamento específico para respaldar os direitos da criança caracterizaria uma onerosidade excessiva e desnecessária aos controladores, além de ser uma medida não necessariamente eficiente no resguardo do princípio do melhor interesse.

b) Orientação para mitigação de riscos inerentes a atividades de tratamento, inclusive quando necessários para buscar o melhor interesse do menor

É relevante que a ANPD apresente critérios para o sopesamento de riscos identificados em casos de tratamentos que se mostram necessários (por exemplo, para execução de um contrato, ou ainda cumprimento de uma obrigação legal à qual o controlador esteja sujeito) e riscos inerentes da atividade que não conseguirão ser afastados em prol do melhor interesse do menor.

Como exemplo, cita-se eventual tratamento de dados biométricos como mecanismo para prevenção à fraude em aplicações, partindo do pressuposto que já tenha sido avaliado sua proporcionalidade. Nesse caso, ao fazer o sopesamento de interesses, é possível enxergar que a proteção à segurança e à identidade da criança está em linha com o resguardo de seu melhor interesse. Contudo, há riscos inerentes ao tratamento de dados biométricos de crianças, por exemplo em relação às suas mudanças enquanto indivíduo em desenvolvimento e a fragilização da acuraria a longo prazo. Assim, questiona-se o que a ANPD poderia orientar os agentes de tratamento em relação aos riscos residuais inerentes à atividade.

Orientações neste sentido são necessárias pois o tratamento de dados pessoais de crianças por diversas vezes é imprescindível e detém papel relevante nas atividades de tratamento de um controlador. Assim, ao invés de vedar essa utilização ou inserir restrições excessivas, a contribuição maior da ANPD é no sentido de indicar caminhos e fornecer insumos sobre como viabilizar esse tipo de operação.

2. **Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.**

Consideramos que as seguintes situações demandam maior detalhamento orientativo pela ANPD acerca do princípio do melhor interesse: (a) indicativos do melhor interesse a serem avaliados pelos controladores; (b) cenários que demonstrem e comparem a observância e a violação ao melhor interesse; e (c) flexibilização ou presunção de melhor interesse em contextos determinados.

a) Orientação sobre indicativos para cumprimento do princípio do melhor interesse

Da perspectiva do princípio de responsabilização e prestação de contas, é relevante que o controlador possua orientações sobre como documentar e gerar evidências sobre o cumprimento do princípio do melhor interesse da criança e do adolescente. Assim, a Autoridade poderá fornecer indicativos práticos, exemplificativos e não taxativos sobre seu entendimento acerca dos aspectos englobados pelo princípio do melhor interesse da criança, inclusive considerando o ambiente digital.

A título de exemplo, a ANPD poderá demonstrar quais elementos poderão ser contemplados em uma avaliação sobre o melhor interesse, como: a opinião da criança; qual(is) direito(s) são promovidos, resguardados ou ao menos não impactados; adoção de meios menos intrusivos; entre outros, ponderados conforme caso concreto.

De toda forma, em que pese seja necessária a orientação sobre indicativos para avaliar e documentar o melhor interesse, não entendemos ser uma medida razoável a exigência de um novo documento não previsto em lei para este fim, como testes de balanceamento específicos que onerem os controladores. Porém, a ANPD poderá indicar sobre o cabimento de incluir tal evidência em instrumentos já existentes como registro de atividades de tratamento ou relatório de impacto à proteção de dados, bem como quais elementos espera que sejam registrados.

b) Orientação sobre situações de observância ou violação ao princípio do melhor interesse

Reforçamos a importância de apresentar vários exemplos de situações detalhadas sobre tratamentos de dados envolvendo o melhor interesse e que afetem a liberdade fundamental do menor enquanto ser em desenvolvimento.

A partir de exemplos concretos, abordando tanto situações simples quanto casos mais complexos, se torna mais factível para os controladores entenderem tanto situações em que o melhor interesse é atendido, quanto os limites para que seja interpretado pela ANPD como uma violação ao princípio.

c) Flexibilização ou presunção de melhor interesse

É relevante que a ANPD se posicione quanto à necessidade de comprovação do melhor interesse da criança por determinados agentes específicos ou situações inerentemente vinculadas à promoção do melhor interesse.

É o caso, por exemplo, de entidades e ONGs voltadas especificamente para os direitos das crianças, como instituições de assistência social, centros de adoção, entre outros. Nessas circunstâncias, especialmente quando a missão institucional estiver atrelada a aspectos de

promoção de interesses de crianças e adolescentes, é relevante questionar até que ponto é razoável e proporcional onerar o agente de tratamento na demonstração do melhor interesse.

Seria relevante a ANPD considerasse eventual legitimidade presumida que permitisse uma flexibilização aos agentes de tratamento para as obrigações relativas às demonstrações de cumprimento ao princípio do melhor interesse.

II – Consentimento

1. **Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?**

Preliminarmente, entendemos que a ANPD deve evitar a adição de critérios exaustivos para a validade do consentimento, além do que a LGPD já apresenta, para não tornar sua aplicação prática algo de difícil operacionalização. Para tanto, poderá observar diretrizes que também se apliquem para especificidades exigidas ao consentimento para tratamento de dados pessoais sensíveis, sem causar ônus adicionais aos controladores.

a) Parâmetros acerca do consentimento "específico"

• Consentimento para finalidades determinadas

A LGPD (artigo 8º, § 4º) determina que as autorizações genéricas para o tratamento de dados pessoais serão nulas e que o consentimento deverá referir-se a finalidades determinadas. Assim, a ANPD poderá guiar-se por esta disposição, considerando a especificidade vinculada a finalidades determinadas.

• Consentimento específico como oposição ao consentimento genérico

A ANPD poderá fornecer aos controladores exemplos de situações que configurariam o consentimento genérico e, portanto, inválido. Assim, os controladores identificariam os elementos que tornam o consentimento inválido para garantir que nenhum desses elementos é preenchido em suas atividades.

b) Parâmetros acerca do consentimento "em destaque"

• Facilidade de identificação do consentimento

Um dos objetivos do consentimento "em destaque" é assegurar que seja identificado facilmente, conforme avaliação contextual e o meio de obtenção deste consentimento. Assim a Autoridade poderá orientar sobre práticas de destaque, com exemplos de aplicações proporcionais ao caso concreto e contextual.

Exemplos contextuais: a criação de uma seção específica para "consentimento para o tratamento de dados de criança" poderá ser razoável em meio a um documento extenso que tenha um sumário facilitado e em camadas, mas poderá ser desproporcional para um formulário simplificado. Ainda, há casos em que recursos visuais poderão ser efetivos, ou ainda pop-ups em aplicativos e plataformas poderão ser utilizados.

• Ausência de técnicas enganosas ou obscuras

A ANPD poderá ilustrar seu entendimento sobre consentimentos mascarados, escondidos ou ofuscados, por exemplo pelo uso de recursos obscuros que desviem a atenção do pai ou responsável, como práticas que tornam o consentimento inválido.

2. **Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?**

Primeiramente, destacamos que as medidas e mecanismos encontrados como boas práticas de mercado e entre as orientações de reguladores internacionais são sempre acompanhadas de uma perspectiva de proporcionalidade e razoabilidade, a depender do risco do tratamento de dados pessoais para o qual o consentimento é solicitado.

O Federal Trade Commission dos Estados Unidos, em material intitulado "A guide for businness and parentes and small entity compliance guide", traz uma lista não exaustiva de exemplos interessantes que podem servir como boas diretrizes para a ANPD ao estipular maneiras de validar o consentimento fornecido pelos responsáveis no ambiente digital, a serem avaliadas de acordo com o contexto do tratamento:

- Exigir que o pai, em conexão com uma transação monetária, use um cartão de crédito, cartão de débito ou outro sistema de pagamento on-line que forneça notificação de cada transação discreta ao titular da conta principal;
- Exigir que os pais liguem para um número de telefone gratuito, ou se conecte via videoconferência, com pessoal treinado para identificar a relação deste adulto com a criança;
- Verificar a identidade de um dos pais por meio de um formulário de identificação emitido pelo governo a partir de bancos de dados com tais informações;
- Exigir que um dos pais responda a uma série de perguntas de desafio baseadas em conhecimentos que seriam difíceis de responder a alguém que não o progenitor;
- Verificar a identidade do adulto a partir da comparação entre a foto de algum documento de identificação enviado pelo responsável com uma segunda foto enviada por este mesmo responsável, usando tecnologia de reconhecimento facial;

Cada medida deverá ser avaliada conforme o risco do tratamento, para não configurar um tratamento excessivo, bem como de uma perspectiva de custos e tecnologias disponíveis à época.

Em conclusão, a verificação do consentimento parental no ambiente digital exige uma abordagem multifacetada, sendo necessário garantir o equilíbrio entre a adequação e proporcionalidade das medidas adotadas, minimizando os riscos e maximizando a proteção dos direitos das crianças, sem onerar excessivamente os controladores.

3. **No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?**

Exigir um consentimento assistido ou a representação dos representantes legais de um adolescente a cada coleta desta autorização para tratamento de dados pessoais seria uma medida que, em muitos casos, poderia contrariar o melhor interesse do menor e representar um ônus excessivo aos controladores.

Assim, o caminho a ser adotado é coerente com o conceito de autonomia progressiva dos adolescentes. Já temos exemplos na legislação pátria de que a capacidade civil não é absoluta, com exceções no código civil e em esferas onde a manifestação de vontade autônoma de adolescente é fomentada – como o direito ao voto facultativo aos 16 anos.

Considerando que a capacidade de discernimento varia entre adolescentes de 12 e 17 anos, a depender do contexto, é relevante buscar da ANPD quais elementos os controladores deverão observar para avaliar este discernimento em sua realidade, viabilizando mecanismos de consentimento "autônomo", ou assistido, caso necessário.

Entendemos necessário obter da ANPD um posicionamento que considere no conceito de autonomia progressiva elementos contextuais, como: tipo de serviço a ser contratado, riscos do tratamento, efeitos do consentimento solicitado, e o discernimento e a opinião do adolescente.

Ainda, é relevante que a ANPD aborde as consequências do consentimento – ou revogação deste - pelo adolescente em relação a eventual consentimento parental prévio.

III - Jogos e aplicações de internet

1. **Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?**

Identificamos os seguintes parâmetros principais: (a) minimização de dados; e (b) privacidade desde a concepção.

a) Minimização de dados

A autoridade britânica ICO no Children's Code - Age Appropriate Design: a code of practice for online service discorre sobre a minimização e a coleta mínima, que devem estar atrelados à finalidade específica do serviço online prestado, de modo se sejam coletados apenas os dados essenciais. Por exemplo, durante a criação de contas dos menores para jogos online, seria razoável coletar dados como nome de usuário e senha, mas devem ser evitadas informações como nome completo, endereço ou dados escolares.

Ainda, a coleta de dados de localização de menores deve ser limitada a situações estritamente necessárias para o funcionamento do serviço, assim como cookies ou quaisquer outras tecnologias de rastreamento que coletam dados pessoais desnecessários. Por exemplo: uma ferramenta de controle parental que disponibilize funções de segurança para que pais localizem onde está o celular da criança e saibam onde ela está representaria uma situação em que a coleta de dados de localização é aceita; já a coleta deste mesmo dado para desbloquear customização de recursos de jogos (como "skins" de personagens), excederia a necessidade.

Neste material, o ICO ainda orienta que a coleta de dados pessoais ocorra apenas quando o menor estiver usando ativamente e conscientemente aquele elemento do serviço. Deve, também, ser ressaltado para os controladores a importância de revisar regularmente a necessidade de armazenamento de dados e excluir qualquer informação desnecessária, minimizando a retenção de dados pessoais, para além da coleta.

Por fim, a autoridade britânica também sugere a desidentificação de dados pessoais de menores antes de utilizações para fins secundários, como pesquisa e desenvolvimento de produtos.

b) Privacidade desde a concepção

Quanto a medidas de design a serem levadas em conta durante o desenvolvimento de ferramentas, como em plataformas de jogos online, indicamos as diretrizes previstas pela autoridade norueguesa de proteção de dados pessoais no guia "Datatilsynet Principles on Children & Online Gaming":

- As configurações que interferem na privacidade e na proteção de dados das crianças sejam desabilitadas por padrão. Isso inclui evitar o rastreamento de localização geográfica, acesso a contatos, gravação de voz, sincronização com mídias sociais, a menos que sejam fundamentalmente necessários para o funcionamento do jogo;
- A natureza dos jogos online pode levar à coleta de uma grande quantidade de dados pessoais sobre as crianças. No entanto, sugere-se que as plataformas devem evitar a coleta automática e análise de dados para fins como a criação de perfis de jogadores, a derivação de dados sobre a personalidade da criança ou suas habilidades cognitivas.
- Por fim, no lugar de coletar dados detalhados sobre as crianças, plataformas devem oferecer opções de personalização que permitam que as crianças escolham o gênero de jogo, o nível de dificuldade, sem a necessidade de coletar dados adicionais.

2. **Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?**

Com base no ICO no Children's Code - Age Appropriate Design: a code of practice for online service e em práticas de mercado, indicamos as seguintes técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais:

- Autodeclaração com mecanismos de dissuasão: permitir que o usuário declare sua idade, mas utiliza mecanismos de dissuasão, como questionários sobre cultura popular ou eventos recentes, para desencorajar declarações falsas.
- Provas de idade digitais: como carteiras de identidade digitais para verificar a idade do usuário.
- Verificação de idade por proxy: solicitar a confirmação de idade por um adulto responsável, como um pai ou responsável legal. Esse método pode ser eficaz para crianças mais novas, mas exige mecanismos seguros para garantir a identidade do adulto e o consentimento informado.

É relevante que a ANPD forneça exemplos de situações práticas sobre verificação de idade, especialmente de cenários em que a verificação de idade provavelmente não será necessária. Por exemplo: quando os produtos e serviços já tenham sido concebidos com a implementação de mecanismos de design específicos para atender ao público de crianças e adolescentes; quando o produto ou serviço requerer a identificação de um usuário único pelo qual já se tenha atribuído sua idade (como serviços de banco ou de plano de saúde).

A verificação de idade implicará em um tratamento de dados pessoais – para o qual já se reconhece uma finalidade legítima.

Assim, o tratamento relativo à verificação de idade não deverá implicar em usos secundários, sendo recomendável a exclusão dos dados coletados durante este processo assim que o nível adequado de confiança quanto à idade do usuário for atingido.

Sobretudo, neste momento de verificação, independentemente do método escolhido, é importante reforçar a necessidade de ser transparente com o usuário sobre como sua idade está sendo verificada.

3. **Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?**

O art. 14, § 4º da LGPD prevê que controladores não deverão condicionar a participação de crianças e adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Nesse sentido, entendemos que a ANPD deve ter cuidado especial ao abordar a questão de formação de perfis comportamentais. Esse tem sido um tema bastante discutido internacionalmente e, dada a sensibilidade das informações que engloba, merece atenção especial da Autoridade.

O objetivo não é que a ANPD determine uma proibição quanto à formação de perfis comportamentais, mas oriente os controladores sobre em que circunstâncias consistiria em um risco a esta categoria, desafiando inclusive o princípio do melhor interesse. Assim, o balizamento para determinar as orientações sobre o tema não precisam fugir do que já se debate acerca do tema de melhor interesse, mas acomodar exemplos claros envolvendo casos de perfilização.

4. **Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?**

É pertinente que a ANPD leve em conta as diferentes idades desses jovens e sua autonomia progressiva. As recomendações de métodos abaixo leva em consideração as faixas etárias definidas pelo ICO no “Children’s Code - Annex B: Age and developmental stages” acerca do desenvolvimento cognitivo em cada etapa:

Para crianças mais novas, em idade pré-escolar e primeiro ciclo do ensino fundamental, sugerimos:

- Restrição de conteúdo: bloquear o acesso a conteúdo impróprio, como violência, pornografia e linguagem inapropriada.

- Limitação de tempo de tela: definir limites de tempo para o uso de dispositivos, incentivando atividades offline e interação social.
- Bloqueio de compras: impedir compras acidentais ou não autorizadas dentro de aplicativos e jogos. Já para crianças mais velhas, no segundo ciclo do ensino fundamental e adolescentes, sugerimos:
- Gerenciamento de redes sociais: supervisionar o uso de redes sociais, orientando sobre privacidade, cyberbullying e contato com estranhos.
- Controle de localização: permitir o compartilhamento de localização apenas com contatos confiáveis e em situações específicas.
- Monitoramento de atividades: acompanhar o histórico de navegação, downloads e interações online, sempre com diálogo e respeito à privacidade.

Embora a ANPD busque mecanismos para ampliar o controle parental, é relevante considerar que implementação efetiva dos controles varia de acordo com a dinâmica familiar e o discernimento da criança, bem como o tipo de tratamento de dados e os riscos atrelados.

Com base em diretrizes do ICO no "Children's Code - 11. Parental controls", o diálogo aberto e constante, a construção de uma relação de confiança e o acompanhamento atento às necessidades de cada criança são fundamentais para garantir uma experiência online segura e positiva.

A orientação às crianças e adolescente deve ser transparente, informando que controles parentais estão em vigor, de forma contextualizada e quais são limites de como podem exercer controle sobre seus dados.

Nesse sentido, as informações a serem fornecidas e formatos adequados poderão variar conforme faixa etária em relação ao desenvolvimento cognitivo de crianças e adolescente, conforme os seguintes exemplos pelo do ICO no Children's Code - 11. Parental controls: para crianças em idade pré-escolar até primeiro ciclo do ensino fundamental, pode ser adequado o fornecimento de materiais de áudio ou vídeo para a criança explicar que seus pais estão sendo informados sobre o que ela faz on-line para ajudar a mantê-la segura; já para adolescentes até estágios próximos da fase adulta é razoável fornecer materiais escritos descrevendo como seu serviço funciona e o equilíbrio entre os direitos de privacidade dos pais e do adolescente.

Por fim, a efetividade de uma experiência online segura e positiva nos ambientes digitais não se esgota apenas na atuação de controladores de dados, sendo uma tarefa compartilhada com os pais e responsáveis.

Assim, a ANPD poderá contribuir com orientações destinadas aos pais e responsáveis abordando, por exemplo, os seguintes aspectos:

- Diálogo e confiança: Priorizar a conversa sobre os riscos online, incentivando a responsabilidade e o uso consciente da tecnologia.
- Acordos familiares: Estabelecer regras claras em conjunto sobre o uso de internet, mídias sociais e jogos, definindo limites e consequências.
- Ferramentas de segurança: Orientar sobre o uso de senhas fortes, softwares de segurança e como identificar e evitar golpes online.

5. **Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?**

Considerando o artigo 14 § 6º da LGPD, o pilar da qualquer comunicação com crianças e adolescentes deve ser a transparência clara, acessível e compreensível, considerando as particularidades deste público-alvo. Assim, entendemos que a ANPD poderá promover orientações não exaustivas que explorem o atendimento ou não dessa adequação de linguagem, para que controladores possam aplicá-las conforme sua própria realidade.

Assim, os controladores devem garantir que o vocabulário, tom e estilo da linguagem usada para transmitir as informações sobre o tratamento de dados pessoais sejam apropriados e ressoem com as crianças para que reconheçam que a mensagem está sendo direcionada a ela.

Nesse sentido, entendemos que podem ser métodos eficientes para o fornecimento de informações de maneira simples, clara e acessível quanto ao tratamento de dados pessoais de crianças e adolescentes:

Uso de métodos não textuais, como desenhos animados, vídeos, imagens, ícones ou gamificação, para transmitir informações sobre proteção de dados de forma mais eficaz. Esses métodos são mais propensos a ressoar com as crianças do que blocos de texto.

- Uso de formatos que sejam mais aplicáveis e relevantes ao serviço que oferecem. Por exemplo, se operam uma plataforma de compartilhamento de vídeos, os vídeos provavelmente são um meio mais apropriado para transmitir informações de transparência para crianças do que uma imagem ou um texto.
- Apresentação de informações de forma atraente, por exemplo, usando tamanhos de fonte grandes, listas de marcadores fáceis de ler, cores. Considerar apresentar trechos breves, de modo a facilitar a compreensão.
- Disponibilizar as informações essenciais sobre proteção de dados no início e incentivar as crianças ativamente pelos controladores a descobrir mais sobre como seus próprios dados pessoais serão usados e como esse uso as afetará, por exemplo, por meio de botões clicáveis.
- Uso notificações oportunas e contextuais ao longo das interações para informar crianças e jovens sobre o tratamento de dados pessoais. Exemplos de momentos oportunos incluem: antes de postar ou compartilhar algo online, antes de alterar as configurações de privacidade padrão.
- Fornecer explicações às crianças sobre o motivo pelo qual determinadas configurações são automaticamente desativadas ou negadas a elas por padrão. Caixas de aviso devem ser exibidas se as crianças usuárias tentarem ativar essas configurações e informações fornecidas explicando por que determinadas configurações de controle de usuário se aplicam a elas.
- Incentivo, por meio de pop-ups ou prompts, por exemplo, a que crianças perguntem aos pais/adultos de confiança se tiverem alguma dúvida sobre as informações de transparência que receberam.

6. **Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?**

Destacamos dois temas principais: (a) direitos dos titulares; e (b) tratamento de dados de geolocalização.

a) Direitos dos titulares

É relevante que a ANPD considere direcionar orientações no que tange ao exercício de direitos de crianças e adolescentes enquanto titulares detentores destes direitos.

É razoável que determinados direitos possam ser exercidos livremente por menores (como confirmação de tratamento, solicitação de informações sobre entidades com as quais houver compartilhamento etc.), e que pais e responsáveis desempenhem seu controle apenas para gestão ou acompanhamento. Já para exercício de direitos que possam gerar consequências aos menores, pais e responsáveis poderiam ser aproximados para ratificar ou intervir nas requisições, como em requisições para correção ou eliminação de dados.

Nesse sentido, para que o controlador verifique se no caso concreto a criança pode entender seus direitos e suas implicações, deve-se levar em conta: o nível de maturidade da criança para tomar decisões como essa; a natureza dos dados pessoais; se há ordens judiciais relacionadas ao acesso ou responsabilidade dos pais; se há dever de sigilo devido ao menor; as consequências de permitir acesso aos responsáveis para exercer os direitos da criança – se houver alegações de abuso ou maus-tratos; qualquer prejuízo para a criança ou o adolescente se os responsáveis não puderem acessar os dados; e a opinião do menor sobre se seus pais devem ter acesso às informações sobre eles.

Assim, é relevante que a ANPD suscite este tema a fim de orientar controladores de que precisarão se preparar para um cenário mutável e viabilizar meios para recebimento e atendimento de requisições neste contexto.

b) Tratamento de dados de geolocalização

Por ser um tipo de dado particularmente crítico, já que pode colocar a segurança física da criança em risco, seria relevante que a Autoridade estabelecesse maiores diretrizes sobre como os controladores devem se portar frente a este tratamento e como garantir que ele está acontecendo da melhor forma.

Caso a geolocalização seja imprescindível para o fornecimento do serviço, sugerimos como salvaguarda a coleta da localização aproximada dos usuários em vez da localização exata, reduzindo o risco de uso indevido dos dados, além da recomendação de que o controlador fornecer controles visíveis para permitir que a criança interrompa o fornecimento da geolocalização a qualquer momento ou após cada sessão, após um curto período ou quando o evento ou recurso que exige localização for concluído.

TOMADA DE SUBSÍDIO SOBRE TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES
Autoridade Nacional de Proteção de Dados (ANPD)

Brasília, 07 de novembro de 2022

Assunto: Tomada de Subsídios sobre Tratamento de Dados Pessoais de Crianças e Adolescentes

A Associação Latino-americana de Internet (ALAI) oferece suas contribuições à Tomada de Subsídios sobre Tratamento de Dados Pessoais de Crianças e Adolescentes, e sugere pontos a serem considerados pela Autoridade Nacional de Proteção de Dados (ANPD) na futura tomada de decisão sobre o tema.

Conforme se verá abaixo:

- (i) entendemos adequado o entendimento disposto no Estudo Preliminar quanto às **limitações jurídicas e dificuldades de aplicação prática do consentimento** (art. 14, §1º) como a única hipótese legal para o tratamento de dados pessoais de crianças, em especial pelo potencial de limitar o tratamento de dados pessoais mesmo quando realizado no melhor interesse da criança e do adolescente;
- (ii) concordamos com a interpretação da Autoridade que afirma a **possibilidade** de tratamento de crianças e adolescentes com base nas hipóteses previstas nos **arts. 7º e 11 da LGPD**, desde que observado o princípio do **melhor interesse;**
- (iii) ressaltamos a importância de que a Autoridade reconheça o **caráter multidimensional** do princípio do melhor interesse, em especial considerando a redação do enunciado proposto na conclusão do Estudo Preliminar da ANPD, que menciona que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado desde que observado o seu melhor interesse, *"a ser avaliado no caso concreto"*;
- (iv) frisamos o entendimento de que o princípio do melhor interesse da criança e do adolescente mencionado pela LGPD exige uma **abordagem multifacetada**, considerando o engajamento de diversos atores;

- (v) reforçamos que **inexistem fundamentos para equiparar dados pessoais de crianças e adolescentes a dados pessoais sensíveis**, tendo em vista que tal interpretação retira desse grupo de indivíduos o direito de ter seus dados sensíveis tratados de acordo com o regime que essa modalidade exige, contrariando o melhor interesse das crianças e adolescentes; e
- (vi) **compartilhamos percepções e experiências da Indústria** alinhadas com o princípio do melhor interesse, que entendemos relevantes para o tema em questão.

A presente contribuição busca, portanto, apresentar os principais pontos a serem considerados pela ANPD para regulamentação do tema, com insumos para **(i)** subsidiar a atuação da Autoridade em torno da multidimensionalidade do princípio do melhor interesse da criança e do adolescente e para **(ii)** demonstrar como a indústria já se preocupa com esse princípio e como já o incorpora em suas práticas, de modo a possibilitar maior proteção aos dados pessoais desses titulares.

Seguimos disponíveis para diálogo e refinamento das ideias aqui expostas de modo colaborativo, à medida que os trabalhos da ANPD avançam.

Respeitosamente,

Sérgio Garcia Alves
Gerente de Políticas Públicas, Brasil

Raúl Echeberría
Diretor Executivo

Assunto: Tomada de Subsídios sobre Tratamento de Dados Pessoais de Crianças e Adolescentes

A Lei Geral de Proteção de Dados (Lei nº 13.709/18) prevê, na sua seção III, diretrizes para o tratamento de dados pessoais de crianças e de adolescentes. O *caput* do art. 14 da lei explicita que o tratamento dos dados desses titulares deve ocorrer em seu melhor interesse, nos termos da legislação pertinente.

O §1º do art. 14 estabelece que *"o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal*". Por sua vez, o §3º do mesmo artigo prevê que a coleta de dados de crianças poderá ser realizada sem o referido consentimento quando for necessário para contatar os pais ou responsável legal ou para a proteção da criança.

A ANPD reconheceu, em sua Tomada de Subsídios, a acentuada controvérsia quanto à interpretação de tais dispositivos da LGPD, o que leva a uma situação de incerteza jurídica para os agentes de tratamento, nomeadamente em razão da indefinição sobre quais hipóteses legais autorizam o tratamento de dados pessoais de crianças e adolescentes.

Diante de tais divergências interpretativas e sua relevantes implicações práticas, a Autoridade elaborou estudo preliminar[1] com objetivo de elaborar análise sobre quais hipóteses legais seriam aplicáveis ao tratamento de dados pessoais de crianças e adolescentes.

Em suma, o estudo delineou três possíveis interpretações sobres os dispositivos da Lei Geral, a saber:

> (i) a aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º, da LGPD, como única hipótese legal para o tratamento de dados pessoais de crianças;
>
> (ii) a aplicação exclusiva das hipóteses legais previstas no art. 11 ao tratamento de dados pessoais de crianças e adolescentes, haja vista a sua equiparação aos dados sensíveis; e

[1]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Estudo preliminar. Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. 2022. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/17636 Acesso em: out. 2022.

(iii) a aplicação das hipóteses legais previstas nos arts. 7º e 11 da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse.[2]

A partir de argumentos favoráveis e contrários a cada uma dessas interpretações, a ANPD concluiu que a terceira alternativa expressa a melhor interpretação da LGPD, de modo que se entende pela "*possibilidade de tratamento de dados pessoais de crianças e adolescentes com base nas hipóteses previstas nos arts. 7º e 11, desde que observado o princípio do melhor interesse, conforme previsto no art. 14 da Lei*".[3]

E a fim de dirimir a controvérsia sobre a questão, de forma a sintetizar sua interpretação sobre a matéria, a Autoridade Nacional, na sua competência para deliberar sobre a interpretação da lei (art. 55-J, XX, LGPD), editou enunciado, com a seguinte redação preliminar:

> *"O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da Lei Geral de Proteção de Dados (LGPD), desde que observado o seu melhor interesse, a ser avaliado no caso concreto, nos termos do caput do art. 14 da Lei."*

(i) A abordagem multifacetada da multidimensionalidade do melhor interesse da criança

Primeiramente, concordamos com a interpretação da Autoridade que afirma a possibilidade de tratamento de crianças e adolescentes com base nas hipóteses previstas nos arts. 7º e 11 da LGPD, desde que observado o princípio do melhor interesse, conforme previsto no art. da Lei. Como a própria Autoridade ressaltou, certamente tal interpretação não implica conferir um "cheque em branco" para o tratamento de dados pessoais de crianças e adolescentes. Pelo contrário, em qualquer situação, o tratamento deverá ser realizado com vistas a atender ao princípio do melhor interesse de crianças e adolescentes.

A possibilidade de aplicação das hipóteses legais previstas nos arts. 7º e 11 da LGPD, desde que observado o princípio do melhor interesse, permite, de fato, maior flexibilidade em face da diversidade de situações concretas, aumentando o rol de possibilidades de

[2] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Estudo preliminar. Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. 2022. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/17636 Acesso em: out. 2022. P. 22.
[3] Idem, p. 22.

tratamento. Além disso, a hipótese mantém a ausência de hierarquia entre as hipóteses legais de tratamento, como preconizado pela LGPD, e evita estabelecer proibições jurídicas abstratas de utilização de determinadas hipóteses legais, sem considerar as limitações e as consequências práticas dessa determinação. Além de enfatizar que a proteção da criança e do adolescente deve sempre estar baseada no princípio do melhor interesse, independentemente da hipótese legal utilizada.

Ocorre que justamente pela centralidade do princípio do melhor interesse na avaliação da legalidade, legitimidade e segurança do tratamento de crianças e adolescentes, é importante que a Autoridade reconheça o **caráter multidimensional** desse princípio, em especial considerando a redação do enunciado proposto na conclusão do Estudo Preliminar da ANPD, que menciona que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado desde que observado o seu melhor interesse, "a ser avaliado no caso concreto".

O caráter multidimensional do princípio do melhor interesse da criança e do adolescente mencionado pela LGPD exige uma **abordagem multifacetada** que i) considere diferentes perspectivas, incluindo a de especialistas, autoridades públicas, reguladores, agentes de tratamento, pais e dos próprios jovens, e que ii) sopese, de um lado, a supervisão de pais e responsáveis e, do outro, a autonomia dos adolescentes. O objetivo de tal abordagem é equilibrar adequadamente a supervisão parental e a autonomia do adolescente, sempre visando a segurança e a proteção da criança e do adolescente enquanto titulares de dados pessoais. O reconhecimento dessa realidade sobre esse princípio será vital para que a ANPD possa regular a respeito do tema e dos critérios a serem levados em consideração quando da "avaliação no caso concreto" na sua aplicação.

A Convenção Internacional dos Direitos da Criança, aprovada pela Organização das Nações Unidas em 1989, ratificada pelo Brasil em 1990 por meio do Decreto nº 99.710/90, estabelece direitos civis, políticos, econômicos, sociais, culturais, bem como aqueles direitos relacionados à saúde de crianças e adolescentes.

O parágrafo 1º do art. 3ª do Documento confere à criança e ao adolescente o direito de ter seus melhores interesses avaliados e levados em consideração em todas as ações ou decisões que lhe digam respeito, tanto na esfera pública quanto na esfera privada. Além disso, tal dispositivo expressa um dos valores fundamentais da Convenção, sendo considerado pelo Comitê dos Direitos da Criança um dos princípios basilares para a interpretação e implementação de todos os direitos da criança e do adolescente.[4]

[4] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. P. 1, p. 9.. Acesso em: out 2022.

A aplicação do princípio do **melhor interesse da criança** é ainda um **conceito dinâmico**, que requer avaliação adequada ao contexto específico, sendo o seu conteúdo determinado caso a caso.[5] Tal conceito é flexível e adaptável, permitindo justamente que ele seja responsivo à situação de cada criança e adolescente, levando em consideração seu contexto pessoal, situação e necessidades. [6]

Em relação ao **ambiente digital**, o Comitê destaca que *"os Estados Partes devem garantir que, em todas as ações relativas à disponibilização, regulação, design, gestão e utilização do ambiente digital, o melhor interesse da criança constitui uma consideração primordial"*.[7]

Nesse sentido, a Lei Geral de Proteção de Dados (Lei nº 13.709/18) estabelece em seu art. 14 que *"o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente"*.

Ao mesmo tempo, deve-se considerar que o direito das crianças e adolescentes, em particular no ambiente digital *"demanda **ações multidimensionais**, que vão além do consentimento e pressupõem o engajamento de variados atores, incluindo pais, agentes de tratamento, organizações da sociedade civil e órgão públicos"* .[8]

É essencial que os direitos de crianças e adolescentes sejam preservados na criação e desenvolvimento de novos produtos e serviços. E para isso, para projetar experiências digitais que atendam ao melhor interesse desses titulares, é necessária a consideração de várias perspectivas diferentes, incluindo a de especialistas, autoridades públicas, agentes de tratamento, reguladores, pais e dos próprios jovens.

Essa abordagem facilita o envolvimento de pais e responsáveis nas experiências *online* de suas crianças e adolescentes, ao mesmo tempo que apoia a autonomia desses

---

[5] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. P. 1, p. 9.. Acesso em: out 2022.

[6] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. P. 9. Acesso em: out 2022.

[7] UNITED NATIONS. General comment No. 25 (2021) on children's rights in relation to the digital environment. Disponível em: https://www.ohchr.org/en/documents/general-comments-andrecommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em: out. 2022.

[8] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Estudo preliminar. Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. 2022. Disponível em: https://www.gov.br/participamaisbrasil/blob/baixar/17636 Acesso em: out. 2022. P. 14.

titulares de dados. Tal equilíbrio é fundamental para que se estabeleça um modelo que seja capaz de implementar, em ações concretas, o princípio do melhor interesse.

(ii) Inexistência de fundamento para equiparação a dados sensíveis

Ratificando os argumentos contrários trazidos pela presente Autoridade na Interpretação no. 02 de seu Estudo Preliminar, entendemos que não há respaldo legal para se equiparar dados de crianças e adolescentes a dados sensíveis - já que a definição legal de "dados sensíveis" não abarcou explicitamente categorias de titulares em seu rol, como dados de crianças e adolescentes.

Complementarmente, compreendemos que o enquadramento de dados pessoais de crianças e adolescentes como dados sensíveis contraria o melhor interesse desses titulares, tendo em vista que retira desse grupo de indivíduos o direito de ter seus dados (de fato) sensíveis tratados de acordo com o regime que essa modalidade exige - e, portanto, discordamos da referida interpretação.

(iii) Práticas da indústria que se coadunam com o melhor interesse

Por fim, baseada nas melhores práticas e parâmetros a serem observados, a Indústria tem se debruçado continuamente para incorporar o princípio do melhor interesse da criança em suas práticas, tendo desenvolvido processos para aplicar a Convenção das Nações Unidas sobre os Direitos da Criança diretamente aos seus produtos e serviços ofertados, tais como:

a) Privacy by design e by default

Proposição de perguntas norteadoras, recursos e exemplos para ajudar as equipes de criação de produtos a tomar decisões equilibradas na criação e no desenvolvimento de tecnologias e aplicações voltadas ao público de crianças e adolescentes;

b) Co-participação

Por meio de programas de co-design, realização de consultas regulares a especialistas, jovens, pais e responsáveis, para garantir o desenvolvimento de produtos que atendam às suas necessidades, considerando justamente a multidimensionalidade do melhor interesse da criança e do adolescente;

c) Transparência

Fornecimento de informações sobre o tratamento de dados pessoais em linguagem simples e adequada ao público a que se destinam os produtos e serviços;

d) Dinamicidade e inovação

Consideração a fenômenos e mudanças sociais relevantes para a adoção de mecanismos tecnológicos para proteger crianças e adolescentes *online*; e

e) Ferramentas de supervisão parental

Adoção de instrumentos para que pais e responsáveis apoiem suas crianças e adolescentes no ambiente digital, acessando ferramentas de supervisão e recursos educacionais elaborados por especialistas da área.

(iv) Conclusão

Por fim, reforçamos que vemos com bons olhos o Estudo Preliminar realizado pela Autoridade Nacional e concordamos com a interpretação que afirma a possibilidade de tratamento de crianças e adolescentes com base nas hipóteses previstas nos arts. 7º e 11 da LGPD, desde que observado o princípio do melhor interesse, conforme previsto no art. da Lei.

Ressaltamos a importância de se pensar o melhor interesse da criança e adolescente como um **princípio multidimensional** - ou seja, voltado para o caso concreto, levando em consideração circunstâncias e características individuais específicas -, que exige uma **abordagem multifacetada** para promover, de um lado, a supervisão dos pais e responsáveis, e de outro, preservar a autonomia dos adolescentes. O desenvolvimento da noção do melhor interesse de crianças e adolescentes deve contar com a participação de diversos atores, a fim de se atingir a efetiva proteção dos dados desses titulares.

Contribuição à Consulta Pública ANPD sobre Tratamento de Dados Pessoais de Crianças e Adolescentes

DANIEL

São Paulo, 16 de agosto de 2024.

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Via e-mail: normatizacao@anpd.gov.br

DANIEL ADVOGADOS vem, respeitosamente, apresentar suas contribuições no âmbito da Consulta Pública sobre Tratamento de Dados Pessoais de Crianças e Adolescentes.

Cumpre ressalvar que este escritório também manifestou suas considerações via "Participa + Brasil", mas, em razão da extensão dos apontamentos e limitação de caracteres da plataforma, entendeu por bem encaminhar a íntegra por meio da presente comunicação.

Por fim, este escritório aproveita para congratular a abertura da Autoridade às Consultas Públicas e renovar seus votos de estima e consideração.

DANIEL ADVOGADOS

I - PRINCÍPIO DO MELHOR INTERESSE

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

É importante harmonizar a compreensão sobre a aplicação do Legítimo Interesse atualmente veiculada pela ANPD com o princípio do melhor interesse das crianças e adolescentes previsto no artigo 227 da Constituição Federal, materializado pelo Estatuto da Criança e do Adolescente (ECA) e com a Convenção sobre os Direitos da Criança ratificada pelo Brasil.

Atualmente, vemos duas possibilidades interpretativas que divergem entre si apesar da sua importância para a aplicação benéfica da LGPD às crianças e adolescentes. A primeira, indica a proteção dos dados pessoais de crianças e adolescentes sob a rubrica de dados pessoais sensíveis. Isso traria como consequência a possibilidade de utilizar somente as bases legais do artigo 11º da LGPD para tratar os dados pessoais desses titulares. É possível ver esse raciocínio, que traz dados pessoais de crianças e adolescentes ao mesmo nível de criticidade de dados pessoais sensíveis, subjacente à Resolução nº 2/2022, para microempresa e empresas de pequeno porte, quando na alínea "d", do inciso II, do §4º a ANPD adota a seguinte redação:

> Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados: II - critérios específicos**: d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.**

Isso também acontece na Resolução de Dosimetria e Aplicação de Sanções Administrativas, quando no §3º, do inciso I, do artigo 8º a autoridade diz que a infração será considerada

grave quando envolver dados sensíveis ou dados de crianças e adolescentes, equiparando novamente essas duas categorias:

Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em § 3º A infração será considerada grave quando: I - verificada uma ou mais hipóteses estabelecidas no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes**: c) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças e adolescentes e de idosos.**

No entanto, a mesma ANPD emitiu posicionamento de que todas as bases legais poderiam ser utilizadas para tratar os dados pessoais desses titulares, inclusive o legítimo interesse. No Enunciado nº 1 de 2023, a ANPD indicou que:

> "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

A harmonização desses dois tipos de compreensão passa pela busca do balanceamento entre o legítimo interesse do controlador e o melhor interesse das crianças e adolescentes, documentadamente, na etapa de balanceamento do teste do legítimo interesse. Para isso, uma sugestão seria o aprimoramento da recomendação de 2023 e do guia de uso da base legal do legítimo interesse, para que esses dois documentos incorporassem dois pontos:

1. O primeiro, é que os controladores de dados devem levar em consideração o contexto específico de tratamento de dados pessoais e quais são os elementos relevantes para avaliar os melhores interesses, atribuindo pesos para o que é mais e menos importante para a preservação do melhor interesse das crianças e adolescentes;
2. O segundo, é que os controladores devem seguir um procedimento que garanta a adoção de salvaguardas adequadas para assegurar o melhor interesse desse tipo de titular de dados.

Além disso, seria interessante que a ANPD evidenciasse quais são etapas adicionais podem ser acrescentadas ao "teste do legítimo interesse" proposto no Guia emitido por ela, para garantir a consideração o balanceamento entre os dois tipos de interesse que estão associados à aplicação dessa base legal.

Novamente, é preciso recorrer ao Comentário Geral 14, do Comitê dos Direitos da Criança da ONU, segundo o qual o melhor interesse deve ser considerado como um (3) direito fundamental autoexecutável, (4) um princípio jurídico interpretativo e (5) uma regra procedimental.

Nesse sentido, os dois pontos iniciais elencados acima (1) e (2), devem ser adicionados à primeira parte do *assessment*, na qual o controlador é convocado a se debruçar sobre o contexto de tratamento de dados pessoais. Depois, os pontos (3), (4) e (5), devem ser abordados minuciosamente na segunda parte do teste, onde são levados em consideração os possíveis direitos fundamentais afetados pela atividade de tratamento e onde se definem os procedimentos que serão adotados para mitigar os riscos identificados durante o restante da avaliação do contexto de aplicação da base legal.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

Sim, existem situações nas quais o ambiente e as condições nas quais as crianças possam estar mais vulneráveis à conteúdo problemático ou interações irrestritas com outras pessoas. Nesse sentido, elencamos as situações que entendemos que devem ser melhor estudadas:

- Controle de acesso a conteúdo;

- Situações e ambientes que demandam verificação de idade de acesso;
- Monitoramento de espaços físicos e lógicos ocupados por esse público – por exemplo: monitoramento do desenvolvimento escolar;
- Reconhecimento facial;
- Prevenção à fraude utilizando nome e dados pessoais de crianças e adolescentes;
- Processos de perfilização, sobre os quais é essencial a manifestação da ANPD, dada sua competência, notadamente a prevista nos arts. 55-J, XX e 55-K, e diante da vedação constante da Resolução CONANDA nº 245/2024[1].

II - CONSENTIMENTO

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

Em primeiro lugar, é necessário ter em mente que obter o consentimento dos pais ou responsáveis legais não exclui o direito de crianças e adolescentes de compreender, dentro de seu contexto e desenvolvimento, o que acontece com os seus dados pessoais, para sua autodeterminação informativa, incluindo o exercício de seus direitos como titulares de dados pessoais.

Por isso, o primeiro critério a ser observado é a necessidade de garantir um aviso de privacidade que possa ser compreendido por crianças e adolescentes. Esse mecanismo de transparência pode até ser o mesmo direcionado para pais ou responsáveis legais, mas é importante que ele seja lúdico, que apresente os esforços do controlador para se fazer entender pelo público infanto-juvenil, nos termos do artigo 14 da LGPD.

[1] "Art. 15 Os dados pessoais de crianças e adolescentes não devem ser utilizados para fins comerciais, como criação e definição de perfis de comportamento, consumo e segmentação mercadológica, tampouco para direcionamento de publicidade ou ampliação de seu alcance, conforme disposto na Resolução CONANDA nº 163 de 13 de março de 2014." Disponível em https://www.gov.br/participamaisbrasil/blob/baixar/48630 .

O segundo critério a ser aplicado é o da especificidade. É preciso que fiquem evidentes as finalidades com as quais os pais ou responsáveis estão consentindo. Nesse sentido, a interpretação dada pela ANPD ao art. 14, LGPD, em seu Enunciado nº 01/2023, que autoriza a fundamentação de atividades de tratamento de dados pessoais nas diversas bases legais, desde que observado o melhor interesse de crianças e adolescentes, fomenta a utilização mais específica e responsável da base legal do consentimento. Não fosse assim, pais e responsáveis seriam mais facilmente instados a consentir com longos textos contendo diferentes finalidades de produtos e serviços. O Enunciado ANPD, ao reiterar a permissão legal para bases diversas, incentivou, na prática, o uso específico, destacado e pormenorizado, da base legal do consentimento.

Como terceiro critério, o campo no qual se coleta o consentimento deve ser fisicamente e visualmente destacado dos demais, de forma que os pais ou responsáveis consigam identificar de forma clara onde podem permitir ou não o uso das informações. Como quarto critério, sugere-se a verificação dos esforços empregados para verificar a idade do responsável legal que está consentindo. Isso é dizer que existe um requisito de verificabilidade para que o consentimento parental seja válido.[2]

Por fim, como quarto critério, sugere-se que os dados não podem ser coletados antes do consentimento parental. Ou seja, todos os esforços devem ser feitos para que a coleta só se inicie de fato após esse processo de registro do consentimento.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os

[2] "Any method to obtain verifiable parental consent must be reasonably calculated in light of available technology to ensure that the person providing consent is the child's parent" .Disponível em: https://www.ftc.gov/system/files/2012-31341.pdf

controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

Como sugestões para a obtenção de um consentimento válido, a ANPD pode se inspirar na lista de métodos elencada pelo COPPA, na seção 312.5 (b) (2): "Fornecer um formulário de consentimento a ser assinado pelos pais e devolvido ao operador por correio postal ou e-mail; Exigir que um pai utilize um cartão de crédito em conexão com uma transação; Pedir que um pai ligue para um número de telefone gratuito atendido por pessoal treinado; Utilizar um documento público; usar e-mail acompanhado por um PIN ou senha obtidos através de um dos métodos de verificação listados pela autoridade".

Outras alternativas sugeridas por diferentes organizações à *Federal Trade Comission,* na oportunidade de uma mesa redonda, tais como: o reconhecimento por imagem, coleta de documento identificador como RG ou CPF, a criação de portais específicos para que os pais possam alterar as preferências de privacidade e coleta de dados pessoais de seus filhos, o método de envio de e-mail ou outro método de comunicação como SMS, para confirmar o consentimento inicialmente dado para o uso dos filhos.

É importante que qualquer lista proposta pela autoridade seja adequadamente adaptada à realidade brasileira e que a ANPD evidencie, por meio dela, o tipo de ação que será considerada como "esforço razoável", ou seja, que implicará o cumprimento das disposições do artigo 14º da LGPD. Nesse sentido, a ANPD deve levar em consideração o modelo de negócio dos controladores sob sua fiscalização e o seu faturamento, assim como as tecnologias que estão à sua disposição para realizar a coleta do consentimento.

Por fim, o julgamento quanto à razoabilidade dos esforços empregados pelos agentes de tratamento também deve levar em consideração o risco que a atividade de tratamento para a qual se coleta o consentimento impõe às crianças e adolescentes. Atividades de tratamento

de risco baixo podem contar com métodos de obtenção e verificação do consentimento mais simples, enquanto atividades consideradas mais arriscadas devem ter camadas mais robustas de captação de evidências sobre a obtenção do consentimento.[3]

Também é importante que os controladores possam submeter as suas alternativas à apreciação da autoridade sem que sejam punidos por isso. Nesse caso, as iniciativas seriam validadas pela própria autoridade como forma de estimular o desenvolvimento de mecanismos para a obtenção do consentimento parental. É importante, no entanto determinar um prazo para a apreciação e parecer da ANPD sobre os casos apresentados, de forma a garantir a segurança jurídica desse processo.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

No Brasil, não se pode dizer que o conceito de autonomia progressiva foi totalmente incorporado pela legislação. A leitura do artigo 3º do nosso Código Civil indica que todas as pessoas com menos de 16 anos são absolutamente incapazes de exercer sozinhas os atos da vida civil. No entanto, em seu artigo 14, §1º, a LGPD determina que o consentimento será exigido para o tratamento de dados de *crianças,* que, nos termos do art. 2º, *caput*, do ECA, são as pessoas com até 12 anos incompletos. Se formos interpretar a LGPD, à luz somente do Código Civil, isso significaria impor aos agentes de tratamento a obrigação de obter o

[3] Disponível em D2.3 Methods for obtaining parental consent and maintaining children rights | Scholarly Publications (universiteitleiden.nl)

consentimento dos pais ou responsáveis legais não apenas de todas as pessoas com menos de 12 anos, mas também de todas entre 12 e 16 anos.

É importante compreender também em que contexto da vida civil essa capacidade é exercida. De acordo com a pesquisa TIC Kids Online de 2023[4], 95% das pessoas de 9 a 17 anos é usuária de internet, o que representa hoje 25 milhões de pessoas. No ano de 2019, a mesma pesquisa demonstrou que 29% dos usuários de 9 a 17 anos ajudaram os pais a fazerem alguma atividade online ou ainda que 28% destes jovens usuários oferecem apoio aos responsáveis pelo menos uma vez por semana.[5]

Por isso, não é possível ignorar a necessidade de viabilizar o acesso das pessoas com menos de 16 anos a aplicações na web. Nesse sentido, a teoria da autonomia progressiva é interessante pois encontra-se positivada em instrumentos legais internacionais que já são utilizados para interpretar as normas brasileiras à luz do melhor interesse das crianças e adolescentes. Nessa toada, é possível citar:

- A Convenção sobre os Direitos da Criança e do Adolescente, que, no artigo 5º, dispõe que os Estados devem reconhecer o direito e o dever dos pais, famílias e tutores de orientar a criança sobre como exercer seus direitos "de acordo com a evolução de suas faculdades"[6]
- A Opinião Consultiva 17/2022, da Corte Interamericana de Direitos humanos, que evidencia existir "um grande variedade no grau de desenvolvimento físico e intelectual, na experiência e nas informações que possu[em]." as pessoas com menos de 18 anos;[7]

[4] Disponível em: https://nic.br/noticia/releases/tic-kids-online-brasil-2023-criancas-estao-se-conectando-a-internet-mais-cedo-no-pais/
[5] Disponível em: https://cetic.br/pt/noticia/criancas-e-adolescentes-conectados-ajudam-os-pais-a-usar-a-internet-revela-tic-kids-online-brasil/
[6] Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca
[7] Disponível em: https://www. corteidh.or.cr/docs/opiniones/seriea_17_esp.pdf.

- O Comentário Geral nº 25 sobre os direitos das crianças e adolescentes no ambiente digital, que reconhece expressamente que a evolução da autonomia da criança e adolescente tem um significado especial no ambiente digital[8]

Assim, entendemos que o conceito de autonomia progressiva deve servir para harmonizar a aplicação do artigo 14 da LGPD e do Código Civil, viabilizando as atividades online de crianças e adolescentes e balizando a aplicação do melhor interesse nas três formas apresentadas na resposta à primeira pergunta. O conceito deve impulsionar uma limitação à necessidade de consentimento parental para toda e qualquer atividade de tratamento de dados, viabilizando o seu tratamento por meio da aplicação de outras bases legais, conforme disposto pela ANPD.

Entendemos que cabe à ANPD interpretar a LGPD à luz do Código Civil, e modular as situações nas quais a autonomia progressiva poderia ser uma alternativa para viabilizar a participação dos adolescentes em determinados contextos da vida civil, em ambiente digital. Contudo, ressaltamos a necessidade de cautela com expansão da autonomia progressiva ao âmbito da responsabilização criminal. O exercício progressivo da autonomia, em ambiente digital, em contextos civis adequados ao desenvolvimento da criança e do adolescente não implica imputabilidade penal e suas gravosas consequências. Este parece um ponto nodal e inescapável ao debate sobre a aplicação do conceito de autonomia progressiva e nos parece que é um bom limite para compreender as situações nas quais ele é ou não aplicável.

III - JOGOS E APLICAÇÕES DE INTERNET

1. **Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar**

[8] Disponível em: https://criancaeconsumo.org.br/biblioteca/comentario-geral-n-25/

níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Para designar os parâmetros e salvaguardas que devem ser adotados para proteger as crianças no ambiente online é preciso estar a par dos riscos que podem afetar esses titulares de dados pessoais. Segundo Elora Fernandes, há uma divisão de quatro tipos de riscos que podem acometer as crianças e adolescentes no ambiente online: riscos relacionados ao contato com conteúdos danosos, riscos derivados do contato – quando elas se engajam em atividades com atores maliciosos que na maioria das vezes são adultos, riscos derivados da conduta de seus pares como situações de *bullying* entre outros tipos de violência e riscos derivados de relações comerciais (contratos) que elas não estão prontas para assumir ou que são acompanhados de pressões comerciais, publicidade direcionada, perda de controle sobre os dados e riscos próprios dos modelos de negócio que envolvem o tratamento massivo de dados pessoais.[9]

Quanto a esse último tipo de risco, a OCDE ampliou a sua abrangência considerando que o ambiente da internet está permeado por alto nível de comercialização de produtos e serviços, de forma que os riscos comerciais foram divididos também em cinco tipos de riscos: de *marketing*, perfilização comercial, financeiros e de segurança. Segundo a OCDE, essas categorias de risco ainda são permeadas por riscos relacionadas ao uso de tecnologias avançadas como a IA, IoT, análises preditivas entre outras.[10]

Dentro da tipologia de risco elencada acima estão condutas específicas já conhecidas socialmente:

---

[9]Disponível em 5RIGHTS FOUNDATION. The risks: Content, Contact, Conduct and Contract. Disponível em: https://www.riskyby.design/the-risks. Acesso em: 11 abr. 2021. Essa tipologia também pode ser encontrada em ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Children in the digital environment. OECD Digital Economy Papers, [s.l.], 8 jan. 2021. http:// dx.doi.org/10.1787/9b8f222e-en. *Apud.* https://criancaeconsumo.org.br/wp-content/uploads/2021/12/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes-its.pdf

[10] Disponível em: https://www.oecd-ilibrary.org/docserver/9b8f222e-en.pdf?expires=1723584196&id=id&accname=guest&checksum=AB55C7629EC44561ED557695EFE49234

Tipo de Risco	Situações abarcadas pelo tipo de risco
Conteúdo	• Conteúdo proibido • Conteúdo prejudicial • Conteúdo de ódio/extremista • Desinformação • Pornografia • Cultura de sexualização • Publicidade imprópria
Conduta	• Comportamento de ódio • *Cyberbullying* • Comunicação hostil entre pares • Assédio sexual • Distúrbios alimentares ou de outra ordem incentivados por comunidades • Comportamentos prejudiciais ou ilegais gerados pelo próprio usuário
Contato	• Assédio • Perseguição • Vigilância indesejada/excessiva • Violência sexual • Extorsão • Aliciamento sexual • Manipulação psicológica • Radicalização • Recrutamento para grupos extremistas
Contratuais/Comerciais	• Roubo de identidade • Fraude • *Phishing* • Tráfico para fins de exploração sexual • Transmissão de conteúdo pago abuso • Jogos de azar • Microsegmentação (perfilização) • Padrões ocultos de design modelando ou persuadindo à compras

Considerando a tipologia de riscos elencada acima e a interpretação sistemática do ordenamento jurídico brasileiro e de normas internacionais que parametrizam a interpretação das leis buscando o melhor interesse de crianças e adolescentes: em primeiro lugar, todo risco associado ao tratamento de dados pessoais desse público deve ser majorado em razão

de sua vulnerabilidade intrínseca; em segundo lugar, e pela mesma razão, é importante tratar os dados pessoais de crianças e adolescentes considerando serem dados de maior criticidade.

O tratamento de riscos associados ao tratamento de dados pessoais de crianças e adolescentes como de maior gravidade diz respeito ao reconhecimento desses sujeitos como titulares de dados vulneráveis. Essa vulnerabilidade decorre da grande assimetria de poder que se configura entre crianças e adolescentes e os agentes de tratamento de dados pessoais. Como decorrência, é importante que atividades nas quais sejam identificados riscos para crianças e adolescentes devem contar com a elaboração de um Relatório de Impacto ao Tratamento de Dados Pessoais.

Especificamente em relação aos riscos de contato identificados acima, sugere-se a adoção de tecnologias de monitoramento que possam ser utilizadas para monitorar com maior amplitude as interações de forma a garantir um ambiente respeitável e saudável. Contudo, é preciso que essas ferramentas sejam avaliadas sob o ponto de vista da privacidade, evitando a hiper vigilância do público infanto-juvenil.

Além disso, é importante que as aplicações e iniciativas direcionadas para crianças contem com medidas de transparência e *design* (pensando na jornada do usuário), que sejam apropriadas para a sua idade. É preciso ter em mente que o *design* e a arquitetura das tecnologias determinam o comportamento dos usuários, nesse caso, de usuários mais vulneráveis e suscetíveis a adotar esses comportamentos, pois possuem capacidade cognitiva ainda em desenvolvimento.

Por isso, como medidas de *design*, sugerimos que os agentes de tratamentos devem estar a par do conceito de *dark patterns*[11], para evitar o desenvolvimento de produtos que contenham designs obscuros, que fazem com que o usuário infanto-juvenil esteja mais suscetível a adotar condutas que não o beneficiário ou são pensadas de acordo com o seu melhor interesse.

Assim, práticas e *designs* que envolvem o desenvolvimento de funcionalidades que sejam assimétricas, ocultas, enganosas, restritiva de direitos devem ser evitadas. Especificamente em relação ao tempo de tela, sugerimos a adoção de avisos em relação à quantidade de tempo que já foi gasta na aplicação, assim como controles para que os pais possam configurar quanto tempo permitem que as crianças e adolescentes as utilizem.

Além disso, arquiteturas construídas para que crianças e adolescentes passem muito tempo em frente às telas e online devem ser evitadas nesse sentido, as práticas conhecidas como *nudges ("empurrões")*[12] também devem ser evitadas. Isso porque, elas significam justamente que foi feta uma escolha de desprivilegiar o interesse da criança e do adolescente para privilegiar o do agente que está por traz da elaboração da aplicação online, mitigando a sua capacidade de agir de forma autônoma.

Ao revés dessas práticas acima descritas, devem ser adotadas práticas de transparência que impulsionam uma conduta adequada e saudável das crianças e adolescentes. Nesse sentido,

[11]"opções de design de interface de usuário que beneficiam um serviço online ao coagir, orientar ou enganar os usuários a tomarem decisões que, caso estivessem totalmente informados e fossem capazes de escolher entre alternativas, eles poderiam não tomar" MATHUR, Arunesh; ACAR, Gunes; FRIEDMAN, Michael J.; LUCHERINI, Elena; MAYER, Jonathan; CHETTY, Marshini; NARAYANAN, Arvind. Dark Patterns at Scale. Proceedings Of The Acm On Human-Computer Interaction, [s.l.], v. 3, n. , p. 1-32, 7 nov. 2019. Association for Computing Machinery (ACM). http:// dx.doi.org/10.1145/3359183, p. 2, . *Apud* FERNANDES. E, Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANPD in Privacidade e Proteção de Dados de Crianças e Adolescentes. ITS. Coord. BRANCO. Sérgio; FERNANDES. Elora; LATERÇA. Priscilla; TEFFÉ, Chiara.

[12] THALER, Richard H.; SUNSTEIN, Cass R. Nudge: Improving Decisions about Health, Wealth and Happiness. New Haven: Yale University Press, 2008, p. 6, tradução nossa. *Apud* FERNANDES. E, Direitos de crianças e adolescentes por design: uma agenda regulatória para a ANPD in Privacidade e Proteção de Dados de Crianças e Adolescentes. ITS. Coord. BRANCO. Sérgio; FERNANDES. Elora; LATERÇA. Priscilla; TEFFÉ, Chiara.

o Guia de Design Apropriado por Idade prevê que a adoção de avisos em formato aumentado, com informação clara em linguagem simples, adequar a informação à idade das crianças.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

Para responder a essa pergunta é preciso levar em consideração que existe uma grande dificuldade técnica e contextual de definir com precisão a idade dos usuários de aplicação da internet. Isso pode ser ultrapassado com empenho, mas não sem custo. Por isso, a exigência de adoção de padrões técnicos que podem impor custos desproporcionais a agentes de tratamento como as organizações da sociedade civil não seria razoável. O cenário é diferente para agentes de grande porte como multinacionais.

Feita essa ressalva, existem diversos meios que podem ser utilizados para verificar a idade dos usuários e eles podem variar de acordo com o risco avaliado de uma atividade de tratamento de dados pessoais para os usuários.

Inicialmente, podemos citar os seguintes métodos[13]:

Atividades de baixo risco	• Auto-declaração - o usuário simplesmente afirma que possui determinada idade mas não há evidência que confirmação. • Medidas técnicas que desencorajam a falsificação da informação – por exemplo, uma conta matemática que uma criança é incapaz de fazer sozinha, campo aberto para preenchimento da idade ao invés de seleção de uma idade pré-definida, impedimento de submeter uma nova idade imediatamente após não conseguir acessar a aplicação com a primeira informação fornecida.

[13]REINO UNIDO. INFORMATION COMMISSIONER'S OFFICE. Age appropriate design: a code of practice for online services. Disponível em: https://ico.org. uk/for-organisations/guide-to-data-protection/key-data-protection-themes/ age-appropriate-design-a-code-of-practice-for-online-services.

Médio Risco	• Tais serviços normalmente funcionam em um sistema de "atributos" onde você solicita a confirmação de um atributo específico do usuário (neste caso, idade ou faixa etária) e do serviço fornece uma resposta 'sim' ou 'não'. • Confirmação de usuário da conta – se o agente de tratamento sabe que a conta está ligada a um adulto, em um serviço subscrito, por exemplo, é possível permitir que esse adulto modele a forma que a criança ou adolescente acesse o serviço, criando senhas e perfis próprios para eles.
Alto Risco	• Inteligência artificial – monitoramento das interações do usuário com o serviço para identificar padrões de comportamento e inferir a idade do usuário. Essa técnica deve vir acompanhada de medidas que garantam a coleta do menor número de dados possível e o bloqueio de uso dos dados para finalidades distintas da identificação de idade dos usuários. • Coleta e apresentação de documentos formais.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

Entendemos que a especificação de limitações ao uso de dados pessoais de crianças e adolescentes devem estar ligadas às finalidades que impõem riscos considerados excessivos para esse público.

Por exemplo, considerando a tipologia de risco da ONU, é possível identificar uma finalidade que é problemática não só sob a ótica da Proteção de Dados Pessoais, mas do próprio Código do Consumidor (CDC), o direcionamento de publicidade para crianças e adolescentes. A prática é proibida de acordo com o artigo 36 do CDC c/c Resolução CONANDA nº 163/2014. Nesse sentido, a prática de microsegmentação com finalidade publicitária também pode ser problemática, pois deixa de levar em consideração o melhor interesse das crianças e adolescentes.

Contudo, o risco excessivo não ocorre com a prática da perfilização para outras finalidades. A exemplo da perfilização para verificação do padrão de comportamento do usuário, a fim de inferir sua idade para permitir ou não o acesso a conteúdo inapropriado ela ocorre em benefício das crianças e adolescentes. Portanto, trata-se de uma prática que, *a priori*, não pode ser considerada incorreta, a menos que sua finalidade esteja em contradição com o princípio do melhor interesse conforme delineado no restante da presente nota técnica.

Dessa forma, compreendemos que a finalidade é a melhor forma de limitar o que pode ou não ser feito com os dados pessoais. A limitação decorrente do tipo de dado pessoal pode levar à exclusão do público infanto-juvenil a priori de espaços importantes para o seu desenvolvimento.. Nesse sentido, a limitação por finalidade deve ocorrer de forma muito específica, a fim de garantir a segurança jurídica para os agentes de tratamento e não excluir as crianças e adolescentes de determinados espaços.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

A primeira boa prática a se levar em consideração para definir as medidas que podem ser utilizadas para ampliar o controle dos pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes é a necessidade de considerar a privacidade dessas pessoas. Muitas vezes, elas usam o ambiente online para desenvolver partes de sua personalidade que não necessariamente são aceitas pelos pais ou responsáveis legais, tais como a sexualidade e a identidade de gênero.

Nesse sentido, a adoção de medidas que permitam a hiper vigilância dos pais ou responsáveis esbarra na necessidade de garantir a privacidade dessas pessoas. Além disso, as crianças e adolescentes devem ser informados quanto ao monitoramento realizado pelos pais de forma que elas entendam até que ponto o que fazem é ou não totalmente privado.

Dito isso, é preciso que se entenda que o controle parental é o uso de ferramentas disponibilizadas pelo arquiteto da aplicação acessada por crianças e adolescentes para limitar e modelar a forma como essas pessoas utilizam essas aplicações. Esse tipo de controle inclui práticas como a possibilidade de configurar quantas horas as crianças e adolescente podem ficar conectadas à aplicação, um horário máximo na noite para o uso da aplicação, restrições de conteúdo e da possibilidade de realizar compras sem supervisão.

Ademais, os pais e responsáveis devem ser adequadamente informados sobre o direito à privacidade dos seus filhos e sobre como podem regular a aplicação para garantir esse direito. Estamos falando aqui da boa-prática de conscientização dessas pessoas para que elas exerçam direitos em nome daqueles por quem são responsáveis.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Atualmente, é necessário consolidar a necessidade de uma linguagem que seja acessível e lúdica para que consultar as informações não seja algo maçante, especialmente para crianças e adolescentes.

Nesse sentido, em resumo, as práticas que entendemos ser mais adequadas para se comunicar com esse público são:

(a) Adoção de *storytelling* para dar transparência à coleta e uso dos dados durante a jornada do usuário e aos caminhos disponíveis para ajustar as configurações de privacidade, isso inclui a criação de personagens e de um enredo que entretenha a criança e o adolescente;

(b) A adoção de vídeos para repassar as informações que, incialmente seriam repassadas em formado de texto;

(c) A Adaptação da linguagem adotada pelo controlador à gírias e modo de falar que seja regional e conectado com o dia a dia do público infanto-juvenil que ele deseja atingir;

(d) Adoção de avisos maiores (em tamanho aumentado) e sem privilégio ou destaque para opções que beneficiem somente o arquiteto da aplicação (*nudges*);

(e) Adotar exemplos que os pais consigam utilizar para explicar como os dados de seus filhos são tratados se as crianças perguntarem ou se eles sentirem necessidade de explicar;

(f) Impedir que a criança e adolescente mude alguma configuração de privacidade sem supervisão.

DANIEL

DESPACHO

Trata-se de consulta aos Encarregados de Proteção de Dados da Defensoria Pública do Estado da Bahia sobre a veiculação de informações contendo dados pessoais e dados pessoais sensíveis em seu site institucional, mídia e matérias institucionais referente a ações e a atuação da Instituição, bem como a sua comunicação com o público interno e externo, sob a ótica da Lei Geral de Proteção de Dados Pessoais (LGPD) - 13.709/2018.

A dinâmica das publicações motivaram este apontamento a fim de se evitar irregularidades e desconformidades com a LGPD, dando continuação com o aprimoramento da cultura organizacional de Proteção de Dados Pessoais na Instituição.

Inicialmente, cabe conceituar o papel atribuído à Assessoria de Comunicação da Defensoria Pública do Estado da Bahia, como descrito no Regimento Interno, art. 42, vejamos:

> CAPÍTULO III - Assessoria de Comunicação e Cerimonial
> Art. 42 - São funções do setor de Imprensa, Publicidade e Relações Públicas:
> I - Realizar as atividades de assessoria de imprensa, publicidade, mídias sociais e comunicação interna da Defensoria Pública do Estado da Bahia;
> II - Elaborar proposta de política de comunicação da Defensoria Pública do Estado da Bahia;
> III - Propor plano e projetos de comunicação social, observado o plano estratégico;
> IV - Assessorar os(as) defensores(as) públicos(as) em assuntos relacionados à comunicação social, inclusive nas estratégias de marketing ideais para projetos;
> V - **Realizar, orientar e supervisionar a atividade de comunicação social nas unidades de atuação da Defensoria Pública do Estado da Bahia;**
> VI - Cuidar da imagem e da promoção da Defensoria Pública do Estado da Bahia frente aos veículos de comunicação, com a divulgação dos programas, ações e projetos estratégicos que se realizam no âmbito da instituição;
> VII - Criar a identidade visual da Defensoria Pública do Estado da Bahia e estabelecer os parâmetros para a sua aplicação;
> VIII - Pautar a imprensa sobre temas de interesse público relacionados às atribuições da Defensoria Pública do Estado da Bahia;
> IX - Indicar, preparar e orientar defensores(as) públicos(as) e servidores(as) para entrevistas de rádio, televisão e imprensa escrita;
> X - Criar e manter canais de comunicação da Defensoria Pública do Estado

da Bahia, bem como extingui-las, com a aprovação do(a) Defensor(a) Público(a) Geral;
XI - **Produzir, editar e revisar o conteúdo jornalístico veiculado pela Defensoria Pública do Estado da Bahia;**
XII - Produzir conteúdo para as redes sociais, inclusive para a difusão do conhecimento em direitos;
XIII - Elaborar, revisar e manter atualizado o conteúdo informativo publicado no sítio eletrônico da Instituição;
XIV - Gerenciar os perfis da Defensoria Pública do Estado da Bahia nas redes sociais;
XV - Desempenhar outras atividades típicas de Assessoria de Comunicação Social que lhe forem atribuídas pelo(a) Defensor(a) Público(a) Geral;
XVI - **Articular junto as Defensorias Especializadas e Regionais, e aos Defensores Públicos, a produção de conteúdo no que diz respeito ao seu âmbito de atuação.**

Alguns pontos precisam ser enfrentados para a melhor orientação da questão, tais como os Princípios aplicáveis previstos na LGPD para que a publicação de dados pessoais de cidadãos em matérias no site da Instituição sejam realizadas em conformidade com a LGPD e outras leis aplicáveis.

A obtenção de base legal para o tratamento, a justificação da necessidade e a implementação de medidas de segurança são essenciais para garantir a proteção dos dados pessoais e a privacidade dos cidadãos. A análise criteriosa de cada caso é fundamental para assegurar a conformidade legal e ética.

Pondera-se o equilíbrio entre intimidade e todos os outros fundamentos elencados, com a avaliação do interesse público com base no critério da intimidade, devendo ocorrer a devida contextualização e justificativa fundamentada para a publicação dos dados**.**

As funções da ASCOM precisam ser guiadas tanto pelo direito dos usuários e dever de informação da Instituição, quanto pelo dever de preservar os dados dos assistidos e assistidas, notadamente a preservação dos chamados direitos da personalidade, entre os quais incluem-se os direitos à honra, à imagem, à privacidade e à intimidade.

Isto porque, no artigo 5º, inciso IX, a Carta Magna consta ser “*livre a expressão intelectual, artística, científica e de comunicação*”, sendo protegida, no inciso X, "*a intimidade, a vida privada, a honra e a imagem das pessoas*" e no inciso XIX, é assegurado o “*acesso à informação resguardado o sigilo da fonte, quando necessário ao exercício profissional*”.

O direito à privacidade, objeto desta orientação, consiste, de fato, no exercício de um direito negativo, ou seja, que incute em outrem um dever de abstenção: **a não exposição ao conhecimento alheio de elementos particulares a que passou a reter**.

Consoante lição de Mendes, o direito à privacidade "*conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral*". (MENDES, Gilmar Ferreira. COELHO, Inocêncio Mártires. BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 4. ed. São Paulo: Saraiva, 2009 p. 423).

Nesse ponto, calha destacar que a Defensoria Pública retém, por ofício e missão constitucional, uma impressionante quantidade de dados pessoais de seus usuários, inclusive dados considerados pessoais sensíveis, além de dados de crianças e adolescentes, estes últimos com especial proteção.

AS BASES LEGAIS

A LGPD, por sua vez, contém dispositivos que regulamentam a forma e as hipóteses da possibilidade do uso dos dados pessoais para a utilização de forma diversa da finalidade para a qual foi originalmente obtida.

Mas não se requer necessariamente o consentimento, pois temos que o consentimento é apenas uma das hipóteses que autoriza o tratamento de dados pessoais na Instituição, não havendo hierarquia ou preferência entre o consentimento e as demais autorizações previstas na lei.

Desse modo, as atividades de tratamento de dados pessoais realizadas pela Defensoria Pública sempre estarão fundamentadas em uma das hipóteses autorizadas pela legislação, como o legítimo interesse ou execução de políticas públicas, vejamos:

> 1. Consentimento do Titular: - O consentimento explícito e informado do titular dos dados é a base mais segura para a publicação de dados pessoais. Esse consentimento deve ser obtido previamente e pode ser revogado a qualquer momento pelo titular.
> 2. Cumprimento de Obrigação Legal: - A publicação pode ser justificada se houver uma obrigação legal ou regulatória que exija a divulgação de dados pessoais.
> 3. Execução de Políticas Públicas: - Dados pessoais podem ser divulgados se forem necessários para a execução de políticas públicas previstas em leis ou regulamentos.
> 4. Interesse Público: - Em situações onde a divulgação é claramente de interesse público, como em questões de saúde pública, segurança ou transparência governamental. Esta justificativa deve ser bem fundamentada.
> 5. Legítimo Interesse: - A divulgação pode ser baseada no legítimo interesse do governo ou de terceiros, desde que esse interesse não prevaleça sobre os direitos e liberdades fundamentais dos titulares dos dados.

Uma análise cuidadosa é necessária para justificar essa base legal.

INTERESSE PÚBLICO

No que concerne à divulgação de notícias de apriorístico interesse público, pode ocorrer de se publicar informações que digam respeito exclusivamente à intimidade e à vida privada do assistido, as quais são objeto de proteção expressa. Por esse motivo, devem ser aferidos no momento da divulgação da notícia **a existência de fato do interesse público** nesta divulgação, passo a passo com noções de inviolabilidade à privacidade, requisitos do qual o informe não poderá se afastar.

Nessa mesma linha, acerca da divulgação de notícias, Mendes, Coelho e Branco (2009) exemplificam as hipóteses em que está presente o interesse público na divulgação de notícias:

> Decerto que interesse público não é conceito coincidente com o de interesse do público. O conceito de notícias de relevância pública enfeixa as notícias relevantes para decisões importantes do indivíduo na sociedade. Em princípio, notícias necessárias para proteger a saúde ou a segurança pública, ou para prevenir que o público seja iludido por mensagens ou ações de indivíduos que postulam a confiança da sociedade têm, prima facie, peso apto para superar a garantia da privacidade (MENDES; COELHO; BRANCO, 2009, p. 426).

As matérias envolvendo a temática de saúde são ainda mais delicadas, pois é necessário o cotejo da Resolução 1.605/00 do Conselho Federal de Medicina que proíbe a divulgação de informações de prontuário ou ficha médica (exceto quando há o consentimento do paciente).

De acordo com a LGPD, em seu art. 5º, **dado pessoal é qualquer "informação relacionada a pessoa natural identificada ou identificável"**. Na verdade, a lógica para entender a definição de dado pessoal é simples: se uma informação permite que você identifique uma pessoa, essa informação pode ser considerada um dado pessoal.

Não há como escapar, a Assessoria de Comunicação Institucional, da avaliação de se tratar, também, do setor de comunicação do Poder Público, o setor de exteriorização dos dados pessoais colhidos, daí precisa-se aproximar-se da LGPD e seus preceitos.

LEGÍTIMO INTERESSE

A ANPD lançou recentemente o guia de **Hipóteses legais de tratamento de dados pessoais com base no legítimo interesse**, que traz luz sobre o tema.

> O legítimo interesse é a hipótese legal prevista no art. 7º, IX, da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), que autoriza o tratamento de dados pessoais (não sensíveis), quando necessário para

> atender aos interesses legítimos do controlador ou de terceiro, desde que tais interesses e finalidades não violem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
> …
> Do mesmo modo, tal qual os demais controladores, o Poder Público, ao realizar o tratamento de dados pessoais com base no legítimo interesse, deve realizá-lo de forma transparente e com a observância dos direitos fundamentais dos titulares, informando-os claramente sobre a finalidade do tratamento, garantindo o acesso a esses dados e **adotando medidas de segurança adequadas para garantir a sua proteção.**

PRINCÍPIOS APLICÁVEIS

Necessário observar os princípios previstos na LGPD e que servem de guia e baliza para orientar a preservação dos interesses e direitos dos assistidos e assistidas pela ASCOM, vejamos:

> 1. Finalidade: - A divulgação deve ter uma finalidade específica, legítima e informada ao titular.
> 2. Adequação e Necessidade: - Os dados divulgados devem ser adequados e limitados ao necessário para alcançar a finalidade específica da publicação.
> 3. Transparência: - Informar os titulares sobre a coleta, uso, armazenamento e eventual divulgação de seus dados pessoais.
> 4. Segurança: - Implementar medidas adequadas para proteger os dados pessoais contra acessos não autorizados, alterações, divulgação ou destruição.
> 5. Responsabilidade e Prestação de Contas: - A instituição deve ser capaz de demonstrar conformidade com a LGPD e adotar medidas para garantir essa conformidade.

Com destaque, há o princípio da **necessidade**, que impõe a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Nesse sentido, deve-se avaliar se a presença de tais dados são imprescindíveis para a comunicação proposta.

Outro princípio de relevo ao tema é o da **segurança**. Segundo tal norma, devem ser empreendidos todos os esforços para utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Já o princípio da **responsabilização** atribui ao agente o ônus de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia

dessas medidas.

Ademais, a LGPD conquanto busque o respeito à privacidade e a proteção dos dados pessoais do titular, ela também preserva a liberdade de expressão, de informação e de opinião, consolidadas no artigo 2º:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem.

Como no restante do ordenamento jurídico, não existe norma absoluta. O respeito aos direitos e garantias fundamentais do indivíduo à privacidade, à intimidade, à honra e à imagem, precisam coexistir em harmonia junto ao direito à informação e a atividade de divulgação de ações da Instituição e, exatamente por isso, elementos como interesse público e técnicas como a anonimização e pseudoanonimização ganham relevância na orientação a ser dada à ASCOM.

Ademais, no **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**, da Agência Nacional de Proteção de Dados (ANPD), são encontradas, de forma bastante didática, orientações sobre a análise dos fins legítimos que os dados pessoais podem ser usados, e os direitos dos usuários.

Desse modo, as atividades de tratamento de dados pessoais realizadas pela Defensoria Pública sempre estarão fundamentadas em uma das hipóteses autorizadas pela legislação, como o legítimo interesse ou execução de políticas públicas.

BOAS PRÁTICAS - ANONIMIZAÇÃO E PSEUDOANONIMIZAÇÃO

Em atenção aos princípios da segurança, da prevenção, da responsabilização e da prestação de contas, órgãos e entidades públicas devem adotar medidas técnicas e administrativas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, observado o disposto nos arts. 46 a 49 da LGPD:

> Art. 46. Os agentes de tratamento devem adotar **medidas de segurança**, técnicas e administrativas **aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.**

No mesmo sentido, conforme o art. 50, § 1º, constitui boa prática realizar o tratamento de dados

pessoais levando em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados.

Entre outras medidas, sempre que possível, os dados pessoais devem ser pseudoanonimizados ou anonimizados, que significa não poder identificar o titular, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

DADOS COLETADOS E PUBLICADOS

Percebe-se que as publicações realizadas através do site da DPE têm caráter informativo e devem observar o disposto no art. 42 do Regimento Interno, buscando atualizar a população da atuação e ações da Defensoria, aproximando, principalmente, os assistidos do estado da Bahia ao serviço público prestado pela Instituição.

Nesse sentido, como já bastante sedimentado, toda e qualquer publicação deve respeitar os princípios constitucionais expressos da Administração Pública, em especial a **legalidade, impessoalidade, moralidade, publicidade e eficiência** (art. 37, caput, CF/88), conciliando o princípio da publicidade com a proteção da intimidade e vida privada (art. 5º, X, CF/88) dos titulares dos dados publicizados.

Destaca-se aqui a necessidade de cuidado com os dados veiculados se consideráveis como "dados pessoais sensíveis", ou seja, dados relativos à o*rigem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, ou dado referente à saúde, à vida sexual, dado genético ou biométrico* (art. 5º, II, da Lei 13.709/19). Tais dados são denominados sensíveis porque pertencem à esfera íntima do indivíduo, sendo ainda capazes de causar estigma ou preconceito.

Noutro ponto, há outra hipótese a que o legislador destinou especial proteção: o tratamento que tenha por objeto dados cujos titulares sejam crianças ou adolescentes.

É fundamental, ainda, que o controlador verifique, previamente, se o tratamento abrange dados de crianças e adolescentes. Sobre o assunto, a ANPD publicou o Enunciado nº 1, de 22 de maio de 2023, com a seguinte redação: "*O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11º da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e* ***prevalecente o seu melhor interesse****, a ser avaliado no caso concreto, nos termos do art. 14 da Lei*".

CONCLUSÃO

Ante o exposto, caso existam publicações que violem as normas de proteção de dados pessoais, na medida em que divulguem o nome completo de assistidos e assistidas, adultos ou crianças, ou outros dados pessoais, inclusive e especialmente os dados pessoais sensíveis, como sua condição médica e imagem, dentre outros, torna-se imprescindível a análise cuidadosa da Assessoria de Comunicação da Defensoria Pública do Estado da Bahia.

Visa-se, assim, proteger os dados dos seus assistidos e assistidas. Ademais, ainda que exista o consentimento do titular para a divulgação de seus dados, é imprescindível a ponderação sobre a exposição dos dados pessoais, avaliando a relevância do interesse público, a importância para o coletivo e a exposição da personalidade, considerando o público vulnerabilizado que fornece seus dados pessoais à Instituição.

Por fim, destaque-se que não é necessária a coleta do consentimento para o tratamento dos dados pessoais pelo Poder Público, tendo em vista que o tratamento dos dados pode ocorrer através de diversas outras bases legais previstas da LGPD, mas a divulgação deve ser ponderada a partir da análise de princípios como a minimização (os dados devem ser tratados apenas na medida necessária para o propósito pretendido), necessidade e do interesse público da exposição.

Salvador, 21 de junho de 2024.

Gil Braga de Castro Silva
Defensor Público
Encarregado de Proteção de Dados

Documento assinado eletronicamente por **Gil Braga de Castro Silva**, **Defensor Público**, em 21/06/2024, às 13:28, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida **aqui** informando o código verificador **0491021** e o código CRC **3AC249F6**.

Referência: Processo nº 01.0004.2024.000006235-1 **Documento SEI nº** 0491021

Universidade do Estado do Rio de Janeiro

Faculdade de Direito

KU Leuven

Faculty of Law and Criminology

Elora Raad Fernandes

Navigating the digital classroom:

Analyzing risks to children's data protection in educational technology

Rio de Janeiro
2024

Elora Raad Fernandes

Navigating the digital classroom:
Analyzing risks to children's data protection in educational technology

Dissertation presented in partial fulfillment of the requirements for the joint degree of Doctor of Law by the Graduate Program in Law at the State University of Rio de Janeiro (Universidade do Estado do Rio de Janeiro - UERJ), Concentration Area: Legal Thought and Social Relations, and by the Catholic University of Leuven (KU Leuven)

Supervisors:

Prof. Dr. Carlos Affonso Pereira de Souza

Prof. Dr. Peggy Valcke

Prof. Dr. Sergio Marcos Carvalho de Ávila Negri

Rio de Janeiro

2024

Elora Raad Fernandes

Navigating the digital classroom:

Analyzing risks to children's data protection in educational technology

Dissertation presented in partial fulfillment of the requirements for the joint degree of Doctor of Law by the Graduate Program in Law at the State University of Rio de Janeiro (Universidade do Estado do Rio de Janeiro - UERJ), Concentration Area: Legal Thought and Social Relations, and by the Catholic University of Leuven (KU Leuven)

Approved on 27 February, 2024.

Examination Committee:

_____ Prof. Dr. Carlos Affonso Pereira de Souza (Supervisor) Faculdade de Direito – UERJ	_____ Prof. Dr. Els Kindt Faculty of Law, Universiteit Leiden
_____ Prof. Dr. Peggy Valcke (Supervisor) Faculty of Law and Criminology – KU Leuven	_____ Prof. Dr. Eva Lievens Faculty of Law and Criminology – Ghent University
_____ Prof. Dr. Sergio Marcos Carvalho de Ávila Negri (Co-Supervisor) Faculdade de Direito – Universidade Federal de Juiz de Fora	_____ Prof. Dr. Daniel Bucar Faculdade de Direito – UERJ
_____ Prof. Dr. Ilse Samoy (Chair) Faculty of Law and Criminology – KU Leuven	_____ Prof. Dr. Laura Drechsler Faculty of Law and Criminology – KU Leuven

ACKNOWLEDGEMENTS

First and foremost, I thank God for all the resources entrusted to me in this existence to undertake the tasks we have set for myself. Firm in my belief that nothing is left to chance, I am immensely grateful for all the opportunities and people I have encountered on the path that has led me here. I view this as an immense responsibility to seize every moment of life and to offer my best to others, and I hope I have completed part of that mission.

I express my profound gratitude to my advisors and co-advisor, Prof. Dr. Carlos Affonso Souza, Prof. Dr. Peggy Valcke, and Prof. Dr. Sergio Negri, for their trust in me and my work, for all the support during the development of this thesis, and for their critical insights that significantly improved the research. I extend my thanks to the professors on my Supervisory Committee and Examination Committee—Prof. Dr. Daniel Bucar, Prof. Dr. Els Kindt, Prof. Dr. Eva Lievens, Prof. Dr. Laura Drechsler, and Prof. Dr. Ilse Samoy—who dedicated time and effort to read, criticize, and discuss this thesis to ensure its best version was defended. A significant work, even if small, is only possible by standing on the shoulders of giants. The Elora who began her academic journey in 2017, and came into contact with the important work of various brilliant scholars within the realm of data protection and beyond, never imagined that she would have the honor of having several of them on her jury.

I thank the State University of Rio de Janeiro (UERJ) and the Coordination for the Improvement of Higher Education Personnel (Capes) for making this PhD possible, as well as KU Leuven, which warmly welcomed me for a joint PhD experience. More specifically, I thank my fellow colleagues at UERJ, who were so important in the beginning of this journey and inspired me to become a more dedicated and serious scholar. I also thank the KU Leuven Centre for IT and IP Law (CiTiP), represented by its Head of Unit Jan de Bruyne, and all my current and former colleagues for providing a stimulating and challenging environment that helps me grow as a researcher and human being every day.

I express my heartfelt gratitude to my family, who always believed in me and my potential with unwavering support, sparing no effort to encourage me even in the face of the most unlikely ideas, and offering me all their love so I could persevere even in the toughest times. In particular, I thank my mother, father, and sister who have been daily by my side, even from across an ocean. My thanks also go to friends and colleagues I have had the pleasure of

meeting along the way on various occasions, who brought company, joy and purpose to my journey.

I thank Alan, who makes my existence immensely happier every day. Thank you for providing me with a light and meaningful relationship, for being my best friend and my anchor, believing in me even in moments when I am most certain I will fail. The finalization of this thesis would definitely not have been possible without all your support, essential feedback, and encouragement.

It is also important to acknowledge my gratitude to those who were present throughout my professional career, providing opportunities for me to gain experience beyond academia. In particular, I thank all former colleagues at ARTICLE 19 Brazil and South America, represented by Denise Dora, Laura Tresca and Paulo José Lara, who believed in my potential and gave me the chance to work in an environment aligned with my ideals. I also thank former colleagues at the European Data Protection Supervisor (EDPS), represented by Brendan Van Alsenoy and Anna Buchta, who provided me with one of the most enriching experiences of my career, altering its trajectory and leading me to consider Belgium my second home.

Finally, I express my gratitude to all those who, even invisibly, enabled these experiences through the funding of public and quality education, both in Brazil and in Belgium. I recognize the privilege and responsibility of completing a PhD, especially at a university in the Global South, where many people still struggle to have their most basic human rights realized.

ABSTRACT

Educational technology (edtech) has vast potential to transform education by improving access, engagement, and equity, especially in the wake of the COVID-19 pandemic. The full realization of these benefits is, however, still a distant prospect. The changes observed thus far seem incremental and uneven, with their impact being heavily contingent on the socio-economic context of the communities where they are implemented, as well as the preparedness and willingness of educators to adopt them.

Moreover, edtech can still yield concerning side effects, particularly in relation to children's rights to privacy and to the protection of personal data. Given that children dedicate a significant portion of their time to educational activities, the detailed digital dossiers created about them can potentially affect their academic performance, university admissions, job prospects, and access to essential public services.

Using the theory of data colonialism as a normative framework, the thesis aimed to map the challenges that edtech presents to children's rights to privacy and to the protection of personal data, and understand the extent to which the current legal framework in Brazil and the European Union (EU) address them. Examining children's experiences with edtech and its impact on their development and learning processes is crucial for understanding the future of individual and collective autonomy, as well as the transformation of citizenship and the trajectory of our society.

The thesis starts by delving into the history of edtech, the interplay between edtech implementation and ongoing education discussions, and the theory of data colonialism as the theoretical framework (Part I). Part II describes and analyzes how the EU and the Brazilian legal framework regulate children's privacy and data protection, focusing on Convention on the Rights of the Child, the GDPR and the LGPD. Part III focuses on mapping horizontal challenges related to children's privacy and data protection arising from the implementation of Artificial Intelligence (AI) in education and specific challenges encountered in some edtech, based on a typology developed in Part I. Part III also includes a study on Google Workspace for Education as a framework to understand the specificities in the implementation of other edtech. Overall, it confirms the research hypothesis that the current operation of AI systems in education and the widespread business model based on data commodification pose challenges to children's best interests that have not yet been addressed in the current data protection frameworks in Europe and Brazil.

Keywords: Educational technology (edtech); Children's data protection; Data Colonialism; Google Workspace for Education.

RESUMO

FERNANDES, Elora Raad. **Navegando pela sala digital**: uma análise de riscos à proteção de dados de crianças e adolescentes nas tecnologias educacionais. 2024. 350 f. Tese (Doutorado) – Doutorado em Direito, Universidade do Estado do Rio de Janeiro; KU Leuven, Rio de Janeiro, 2024.

Tecnologias educacionais (edtech) possuem um vasto potencial para transformar a educação, melhorando o acesso, o engajamento e a igualdade, especialmente após a pandemia de COVID-19. A realização plena desses benefícios, no entanto, ainda é uma perspectiva distante. As mudanças observadas até agora parecem incrementais e desiguais, com seu impacto sendo fortemente condicionado pelo contexto socioeconômico das comunidades onde são implementadas, bem como pela preparação e disposição dos educadores em adotá-las.

Além disso, edtech ainda podem gerar efeitos colaterais preocupantes, especialmente em relação aos direitos de crianças à privacidade e à proteção de dados pessoais. Dado que estas dedicam uma parte significativa de seu tempo a atividades educacionais, os detalhados dossiês digitais criados sobre elas podem afetar potencialmente seu desempenho acadêmico, admissões universitárias, perspectivas de emprego e acesso a serviços públicos essenciais.

Usando a teoria do colonialismo de dados como marco teórico, a tese teve como objetivo mapear os desafios que as edtech apresentam para os direitos das crianças à privacidade e à proteção de dados pessoais, e entender até que ponto o atual marco normativo no Brasil e na União Europeia (UE) os endereçam. Examinar as experiências das crianças com edtechs e o impacto em seu desenvolvimento e processos de aprendizagem é crucial para entender o futuro da autonomia individual e coletiva, bem como a transformação da cidadania e a trajetória de nossa sociedade.

A tese começa explorando a história das edtechs, a interação entre a implementação de edtechs e as discussões educacionais em andamento, e a teoria do colonialismo de dados como marco teórico (Parte I). A Parte II descreve e analisa como o marco regulatório da UE e do Brasil regulamentam a privacidade e a proteção de dados de crianças, com foco na Convenção sobre os Direitos da Criança, no GDPR e na LGPD. A Parte III concentra-se em mapear desafios horizontais relacionados à privacidade e à proteção de dados das crianças decorrentes da implementação de Inteligência Artificial (IA) na educação e desafios que edtechs específicas apresentam, com base em uma tipologia desenvolvida na Parte I. A Parte III também inclui um estudo sobre o Google Workspace for Education como um exemplo para entender as especificidades na implementação de outras edtechs. Ao final, confirma-se a hipótese de pesquisa de que o atual funcionamento de sistemas de IA na educação e o modelo de negócios baseado na comodificação de dados pessoais apresentam desafios para o melhor interesse das crianças que ainda não foram endereçados nas atuais leis de proteção de dados na Europa e no Brasil.

Palavras-chave: Tecnologias educacionais; Proteção de dados de crianças e adolescentes; Colonialismo de dados; Google Workspace for Education.

SAMENVATTING

FERNANDES, Elora Raad. **Navigeren door de digitale klas:** Analyseren van risico's voor de gegevensbescherming van kinderen in onderwijstechnologie. 2024. 350 blz. Thesis (doctoraat) - Doctoraat in de Rechten, Universidade do Estado do Rio de Janeiro; KU Leuven, Rio de Janeiro, 2024.

Educatieve technologie (edtech) heeft enorm potentieel om het onderwijs te transformeren door de toegang, betrokkenheid en gelijkheid te verbeteren, vooral in het licht van de COVID-19-pandemie. De volledige realisatie van deze voordelen lijkt echter nog steeds ver weg. De tot nu toe waargenomen veranderingen lijken geleidelijk en ongelijk, waarbij hun impact sterk afhankelijk is van de sociaal-economische context van de gemeenschappen waar ze worden geïmplementeerd, evenals de bereidheid en bereidheid van opvoeders om ze aan te nemen.

Bovendien kan edtech nog steeds zorgwekkende bijwerkingen hebben, met name met betrekking tot de rechten van kinderen op privacy en de bescherming van persoonsgegevens. Aangezien kinderen een aanzienlijk deel van hun tijd besteden aan educatieve activiteiten, kunnen de gedetailleerde digitale dossiers die over hen zijn aangemaakt potentieel van invloed zijn op hun academische prestaties, universitaire toelatingen, carrièremogelijkheden en toegang tot essentiële openbare diensten.

Met behulp van de theorie van datakolonialisme als normatief kader, had de scriptie tot doel de uitdagingen te in kaart te brengen die edtech presenteert voor de rechten van kinderen op privacy en de bescherming van persoonsgegevens, en te begrijpen in hoeverre het huidige wettelijke kader in Brazilië en de Europese Unie (EU) deze aanpakken. Het onderzoeken van de ervaringen van kinderen met edtech en de impact ervan op hun ontwikkeling en leerprocessen is cruciaal voor het begrijpen van de toekomst van individuele en collectieve autonomie, evenals de transformatie van burgerschap en de koers van onze samenleving.

De scriptie begint met een diepgaande verkenning van de geschiedenis van edtech, de interactie tussen de implementatie van edtech en lopende onderwijsdiscussies, en de theorie van datakolonialisme als theoretisch kader (Deel I). Deel II beschrijft en analyseert hoe het wettelijk kader van de EU en Brazilië de privacy van kinderen en de gegevensbescherming reguleren, met de nadruk op het Verdrag inzake de Rechten van het Kind, de GDPR en de LGPD. Deel III richt zich op het in kaart brengen van horizontale uitdagingen met betrekking tot de privacy van kinderen en gegevensbescherming die voortkomen uit de implementatie van Kunstmatige Intelligentie (AI) in het onderwijs, evenals specifieke uitdagingen die zich voordoen bij sommige edtech, gebaseerd op een typologie ontwikkeld in Deel I. Deel III omvat ook een studie naar Google Workspace for Education als een kader om de specificiteiten in de implementatie van andere edtech te begrijpen. Over het algemeen bevestigt het de onderzoekshypothese dat de huidige werking van AI-systemen in het onderwijs en het wijdverspreide bedrijfsmodel gebaseerd op gegevenscommodificatie uitdagingen vormen voor het beste belang van kinderen die nog niet zijn aangepakt in de huidige kaders voor gegevensbescherming in Europa en Brazilië.

Trefwoorden: Educatieve technologie (edtech); Bescherming van gegevens van kinderen; Datokolonialisme; Google Workspace for Education.

LIST OF ACRONYMS AND ABBREVIATIONS

ABNT	*Associação Brasileira de Normas Técnicas* [Brazilian National Standards Organization]
AEPD	*Agencia Española de Protección de Datos* [Spanish Data Protection Authority]
ADHD	Attention deficit hyperactivity disorder
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AIED	Artificial Intelligence in Education
ANPD	*Autoridade Nacional de Proteção de Dados* [Brazilian Nacional Data Protection Authority]
AP	*Autoriteit Persoonsgegevens* [Dutch Personal Data Authority]
APA	American Psychological Association
API	Application Programming Interface
AR	Augmented reality
Art.	Article
ATS	Applicant Tracking Systems
BIK+	European Strategy for a better internet for kids
BNCC	*Base Nacional Curricular Comum* [Brazilian National Common Curricular Base]
CAI	Computer-Aided Instruction
CBL	Computer-based Learning
CBT	Computer-based Training
CC	*Código Civil* [Brazilian Civil Code]
CDC	*Código de Defesa do Consumidor* [Brazilian Consumer Protection Code]
CD-ROM	Compact Disc-Read Only Memory
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CLR	Comprehensive Learner Records

CLV	Customer lifetime value
CNE	*Conselho Nacional de Educação* [Brazilian National Education Council]
CNIL	*Commission Nationale de l'Informatique et des Libertés* [French Data Protection Authority]
CoE	Council of Europe
Consed	*Conselho Nacional de Secretários da Educação* [Brazilian National Council of State Secretaries of Education]
COPPA	Children's Online Privacy Protection Rule (USA)
COREPER	EU Committee of Permanent Representatives
CRC	Convention on the Rights of the Child
CRFB	*Constituição da República Federativa do Brasil* [Brazilian Federal Constitution]
CRIA	Child-rights Impact Assessment
DA	Data Act
DBTS	Dialogue-Based Tutoring System
DDBM	Data-driven business model
DDDM	Data-driven decision-making
DEAP	Digital Education Action Plan
DGA	Data Governance Act
DINUM	*Directeur Interministériel du Numérique* [French Interministerial Director of Digital Affairs]
DPA	Data Protection Authority
DPC	Data Protection Commission [Irish Data Protection Authority]
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
DSK	*Datenschutzkonferenz* [German Data Protection Conference]
DSSC	Data Spaces Support Centre
DTIA	Data Transfer Impact Assessment
EBIA	*Estratégia Brasileira de Inteligência Artificial* [Brazilian Artificial Intelligence Strategy]

ECA	*Estatuto da Criança e do Adolescente* [Brazilian Child's and Adolescent's Statute]
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDSC	European Digital Skills Certificate
Edtech	Education technology
EEA	European Economic Area
EU	European Union
EWS	Early warning systems
FTC	Federal Trade Commission
FERPA	Family Educational Rights and Privacy Act (USA)
GDPR	General Data Protection Regulation
GEGs	Google Educator Groups
GPAI	General-purpose Artificial Intelligence
HDI	Human Development Index
IBM	International Business Machines Corporation
IBO	International Baccalaureate Organization
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICO	Information Commissioner's Office [UK's Data Protection Authority]
ICT	Information and Communication Technologies
IMEI	International Mobile Equipment Identity
IMY	*Integritetsskyddsmyndigheten* [Swedish Authority for Privacy Protection]
ISS	Information Society Services
ITS	Intelligent Tutoring Systems
KPI	Key Performance Indicator
LAI	*Lei de Acesso à Informação* [Brazilian Access to Public Information Law]

LDB	*Lei de Diretrizes e Bases da Educação Nacional* [Brazilian National Education Guidelines and Bases Law]
LGBTIQA+	Lesbian, gay, bisexual, transgender, intersex, queer/questioning, asexual
LGPD	*Lei Geral de Proteção de Dados Pessoais* [Brazilian General Data Protection Law]
LMS	Learning Management Systems
MAC	Media Access Control
MCI	*Marco Civil da Internet* [Brazilian Internet Bill of Rights]
MCTI	*Ministério da Ciência, Tecnologia e Inovação* [Ministry of Science, Technology, and Innovation]
MEC	*Ministério da Educação* [Brazilian Ministry of Education]
ML	Machine learning
MOOC	Massive Open Online Course
MP	*Medida Provisória* [Provisional Measure]
MR	Mixed reality
MS	Member States
MTST	*Movimento dos Trabalhadores sem Teto* [Brazilian Homeless Worker Movement]
NLP	Natural language processing
NGEU	Next Generation EU
NPRM	Notice of Proposed Rulemaking
OECD	Organization for Economic Cooperation and Development
Ofqual	Office of Qualifications and Examinations Regulation (UK)
PC	Personal Computer
PLE	Personal Learning Environment
PNE	*Plano Nacional de Educação* [Brazilian National Education Plan]
PNED	*Política Nacional de Educação Digital* [Brazilian Policy on Digital Education]
SDGs	Sustainable Development Goals
SDK	Software development kit
SIVON	Dutch cooperative of school boards in primary and secondary education

STF	*Supremo Tribunal Federal* [Brazilian Supreme Federal Court]
SURF	The collaborative organization for IT in Dutch education and research
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
ToS	Terms of Service
UDHR	Universal Declaration of Human Rights
UIS	UNESCO Institute for Statistics
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Program
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children Fund
USA	United States of America
VLE	Virtual Learning Environments
VR	Virtual reality
VTC	*Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens* [Flemish Supervisory Commission for the processing of personal data]
WP29	Article 29 Data Protection Working Party
XR	Extended Reality

LIST OF FIGURES

Figure 1 - Edtech typology 46
Figure 2 - The CO:RE classification of online risks to children 79
Figure 3 - AI Act risk-based approach - pyramid of risks 133
Figure 4 - Global heatmap measuring how well each country's spoken languages are represented by the composition of natural language datasets 173
Figure 5 - Six levels of automation of personalized learning 189
Figure 6 - Google Workspace for Education's core and additional services 210

LIST OF TABLES

Table 1 - Examples of EdTech "products", with % Global Market share (2019) 48
Table 2 - Franglen's Admissions Algorithm 174
Table 3 - Inferring pupils' attention through brain waves 176
Table 4 - Ofqual's algorithms for evaluating students' performance 184
Table 5 – Gaggle and its impacts on privacy and mental health 201

SUMMARIZED TABLE OF CONTENTS

ACKNOWLEDGEMENTS **3**
ABSTRACT **5**
RESUMO **6**
SAMENVATTING **7**
LIST OF ACRONYMS AND ABBREVIATIONS **8**
LIST OF FIGURES **13**
LIST OF TABLES **13**
INTRODUCTION **17**
Research question and methodology **21**
a) Relevance 21
b) Research question(s) 23
c) Hypothesis 23
d) Scope of the research 24
e) Methodological approach and thesis structure 25
PART I. SETTING THE SCENE **29**
Chapter 1. The use of technology in education **29**
1.1 A brief history of edtech 31
1.2 Edtech typology 44
Interim conclusion 48
Chapter 2. Exploring the interplay between edtech and longstanding discussions in education **50**
2.1 Public and private values in education 50
2.2 The “learnification” of education 55
2.3 Learning, calculation and efficiency 57
2.4 Platform learning 59
Interim conclusion 61
Chapter 3. Data Colonialism as a theoretical and normative framework **62**
3.1 The concept of data colonialism 62
3.2 Main components of data colonialism 64
3.3 Colonizing agents 66
3.4 Data Commodification 67

3.5 Data colonialism and its incursion into autonomy 68
Interim conclusion 70
PART II. LEGAL FRAMEWORK ON CHILDREN'S PRIVACY AND DATA PROTECTION 72
Chapter 4. Why children need special privacy and data protection rights 72
4.1 Why do children's data require special treatment? 73
4.2 Privacy and data protection as a cross-cutting dimension of risks to children's online presence 78
4.3 The importance of privacy and data protection for children's development and learning 81
Interim conclusion 84
Chapter 5. The CRC in the digital environment 86
5.1 The right to non-discrimination 88
5.2 The right to have the child's best interests taken as a primary consideration 89
5.3 The right to be given appropriate direction and guidance in a manner consistent with the evolving capacities of the child 92
5.4 The right to have their views given due weight in accordance with their age and maturity 93
5.5 The right to privacy 95
5.6 The right to education 97
5.7 The right to protection against economic exploitation 101
Interim conclusion 103
Chapter 6. EU's relevant legal and policy frameworks 104
6.1 The General Data Protection Regulation (GDPR) 106
6.2 AI Act 132
6.3 EU policy on digital education 138
Chapter 7. Brazil's relevant legal frameworks 142
7.1 The Brazilian General Data Protection Law (LGPD) 143
7.2 The right to education 156
7.3 The Brazilian Artificial Intelligence Bill 157
7.4 Brazilian policy on digital education 159
PART III. CHALLENGES INTRODUCED BY EDTECH TO CHILDREN'S RIGHTS TO PRIVACY AND TO THE PROTECTION OF PERSONAL DATA 163
Chapter 8. Mapping the challenges introduced by edtech 164
8.1 Datafication 165

8.2 Data Generation 169
8.3 Decision-making 176
Interim conclusion 206
Chapter 9. Google Workspace for Education 208
9.1 What is Google Workspace for Education 208
9.2 The main features of Google Workspace for Education 211
9.3 The role of Google Workspace for Education within Google's business model 213
Interim conclusion 219
Chapter 10. The use of Google Workspace for Education in the European Union and in Brazil 221
10.1 Belgium 222
10.2 Denmark 225
10.3 Finland 229
10.4 France 231
10.5 Germany 232
10.6 Netherlands 234
10.7 Norway 237
10.8 Spain 239
10.9 Sweden 241
10.10 Brazil 242
Interim Conclusion 254
Chapter 11. Analysis 256
11.1 Tensions between the GDPR, LGPD and Google Workspace for Education 256
11.2 Appropriation of resources through the lack of compliance with the data protection framework 266
11.3 Unequal data relations and global distribution of the benefits of resource appropriation 267
11.4 Digital sovereignty 268
Interim Conclusion 275
CONCLUDING REMARKS 276
Recommendations and indications for future research 285
COMPLETE TABLE OF CONTENTS 290
REFERENCES 295

INTRODUCTION

1. Education is the cornerstone of any contemporary society. More than an isolated element used as a tool for acquiring knowledge and skills, education plays a multiplying role in the progress of humanity and is the foundation upon which all other spheres of society are built. On an individual level, education has the power to develop critical thinking, hone conflict resolution skills, and unveil each individual's essence. From a collective perspective, it can be used to nurture active, well-informed citizens concerned with the common good. Ultimately, it has the potential to generate economic development, reduce inequalities, foster ethical progress, and strengthen democracy, human rights, and the rule of law. The way children are educated shapes the potential for flourishing within any given population, so every decision made in this regard is highly consequential and political.

2. Especially since the COVID-19 pandemic, digital Information and Communication Technologies (ICTs) are increasingly present in the school environment. They are already used in children's admission tests at schools, in how teachers correct homework, in the personalization of learning content across various applications, as well as in school administration and security technologies. The use of learning platforms worldwide, mainly provided by companies from the United States of America (USA), China, and India, is also ever more common. Google Workspace for Education, Class Dojo, Carnegie Learning, IBM's Watson (in partnership with Pearson), Coursera, Blackboard, Udacity and Kahn Academy are just examples of the available diverse range of educational technology (edtech). Additionally, several others are gradually being adopted or are anticipated to be adopted in the near future, such as the use of large language models in adopted Artificial Intelligence (AI) systems, as well as the exploration of extended reality (XR) and the metaverse.

3. The opportunities brought about by edtech are tremendous, as they have the potential to transform education by expanding access to knowledge, improving the learning process, fostering conscious citizenship, enabling people with disabilities to access and enjoy the benefits of technology, and more. Goal 4 of the 2030 United Nations (UN) Agenda for Sustainable Development aims to "ensure inclusive and equitable quality education and promote lifelong learning opportunities for all" (Locatelli, 2018, p. 2). The Qingdao Declaration on ICT in Education of 2015 highlights how technologies can support the Sustainable Development Goals (SDGs) (Qingdao Declaration, 2015: Seize Digital Opportunities, Lead

Education Transformation, 2015). According to the declaration, technology is essential for strengthening education systems, ensuring universal access to education, promoting quality and effective learning, and facilitating equitable and more efficient service provision. More recently, the Beijing Consensus on Artificial Intelligence in Education (2019) recommended that governments and other stakeholders take action in various areas such as planning AI in education policies, AI for education management and delivery, and AI to empower teaching and teachers.

4. More specifically, the first obvious benefit of implementing digital ICTs in education is improving equality and inclusion. They can reduce the costs of accessing education for certain groups, such as those who live in remote areas, do not have access to schools, face learning difficulties, lack time, or have specific disabilities (Good, 2021; UNESCO, 2023b).

5. With the increased availability of information and knowledge online, students can access materials with even better quality than the ones they have access to in their region. Technologies can facilitate including students with special needs, support the diagnosis of disabilities, and adapt content to a way they can enjoy it. Examples include using AI to enable speech to text (and vice versa) or to generate automatic subtitles; supporting the socio-emotional and academic learning of autistic children; helping children with attention deficit hyperactivity disorder (ADHD); and, more importantly, "enabling students with special needs to study in a traditional (and inclusive) learning environment, which also changes peoples' view on disability and special needs" (Vincent-Lancrin, 2021, p. 26)**.**

6. Another promise of edtech relates to the use of early warning systems (EWS) for dropout prevention. An EWS is a tool developed to help identify students at risk of dropping out. Students are considered at risk when red flags, or specific indicators associated with dropout**,** are spotted. Examples include the cost of and structural issues within education, such as teacher quality and curriculum (United Nations Children's Fund (UNICEF), 2018). Technology-based EWS could effectively and promptly assist in addressing these specific needs.

7. Last but not least, edtech is also seen as a way to improve effectiveness and efficiency within education. Some argue that they can improve engagement as a prerequisite for meaningful learning and the development of cognitive and socio-emotional skills. Edtech could help identify engagement proxies (such as interaction patterns and eye, facial and body movements) as well as maintain it through nudging techniques (D'Mello, 2021). Educators'

jobs can get increasingly streamlined with automated systems built for reporting, resource allocation, and credentialing (Baker, 2021; Vincent-Lancrin, 2021)**.** AI systems based on natural language processing can help correct exams or evaluate oral presentations; chatbots can help answer the most frequent students' questions; and predictive analytics promise to predict and assess students' progress throughout their academic life (Smuha, 2023b). Finally, edtech could improve public policies, driving transparent governance and better management of education systems and resources (Chakroun *et al.*, 2022).

8. The transformation of education promised by the benefits described above is, nonetheless, still far from being fully realized. Indeed, the adoption of edtech has brought about significant changes so far, introducing new ways to engage with educational content. The basic skills expected of current students also increasingly include those necessary to navigate the digital environment.

9. However, at this point, these changes can be considered incremental and uneven, with research showing that students can eventually experience more harm than good (Laird; Dwyer; Grant-Chapman, 2023). Their use and impact heavily depend on the socio-economic factors of the community where they are based, as well as the level of preparedness and willingness of the educators who implement them (UNESCO, 2023b, p. 6).

10. Differentiating the potential benefits, i.e., the ones claimed by their developers, and the evidenced benefits, which are supported by robust, independent scientific research on a significant scale is, therefore, key. Although thousands of studies have been carried out on the benefits of edtech, and more specifically on the use of Artificial Intelligence in Education (AIED), there is still little independent evidence of their effectiveness at scale, over time and across contexts (Holmes, 2023; Kucirkova; Brod; Gaab, 2023).

11. We should also consider the broader and often unforeseen side effects of edtech on children's human rights. This includes a significant increase in screen time, the widening of the digital divide between the privileged and underprivileged, the reinforcement of problematic pedagogical practices often focused on behaviorist mechanisms and techniques to capture children's attention, access to inappropriate content, and the rise of mis/disinformation. Historically marginalized communities also suffer disproportionate negative impacts (Laird; Dwyer; Grant-Chapman, 2023).

12. More specifically and important for this thesis, we must consider the effects that edtech has on children's rights to privacy and to the protection of personal data, whether as an end in

themselves or as a means to protect other fundamental rights such as non-discrimination, freedom of expression, personality development, autonomy, and human dignity. Children spend much of their time at school (in person or online) or working on educational activities. Therefore, the digital dossiers created about them while using these technologies have the potential to be highly detailed and comprehensive. This wealth of information can impact not only their performance at school and learning trajectories, but also their opportunities for university admission, entry into the job market, or even access to essential public services.

13. These technologies are also not introduced in a vacuum. The current educational system, whose main structures have changed little over the past centuries, is imbued with pedagogical and methodological discussions that interact with technologies in a unique way. As will be discussed throughout the thesis, important and influential trends in education, such as the measurement movement, align with the datafication processes of some technologies in a way that mutually reinforces each other. Similarly, discussions about the actors influencing educational decisions, which have always existed, intensify with the growth of neoliberalism and the increasing involvement of private actors in education through the provision of technologies.

14. This has intensified a narrative that the education sector is broken and stuck in the past (UNESCO, 2023b; Weller, 2014, p. 119); is lagging behind other sectors in adopting technologies (Allen, 2022; Pedro *et al.*, 2019); is under digitized; and "traditionally laggards when it comes to innovation" (Organization for Economic Cooperation and Development (OECD), 2021, p. 3). This discourse portrays the notion of development and enhancement of the educational framework as inherently reliant on technology. What is more, rather than addressing on the root of the problem, which is often the lack of sufficient financial and human resources, edtech has been seen as a magical way[1] to solve the educational crisis. This perspective has escalated a dangerous discourse of modernization at all costs and of technological solutionism (Morozov, 2014).

15. Discussing children's experience with the digital environment and its impact on their education and broader development is key to understanding the future of individual and collective autonomy, as well as how citizenship is being transformed. If our intention is to maximize the benefits edtech has to offer, it should be assessed and deployed in a critical way,

[1] Sebastian Thrun, co-founder of online learning company Udacity Inc. and Stanford University research professor who helped create Google's self-driving car, once said that "Education is broken. Face it. […] It is so broken at so many ends, it requires a little bit of Silicon Valley magic" (Wolfson, 2013).

focusing on what is scientifically proven, on the educational goals we want to achieve, and on balancing the full array of positive and negative effects on children's human rights.

16. Based on the above, this research acknowledges the enormous potential that edtech can have in effectively transforming education, incorporating greater equity, quality, effectiveness and efficiency. Still, it views the current stage with rationality and scientific spirit, understanding what they can *actually* accomplish and balancing it with the risks they may still pose.

Research question and methodology

17. This section is dedicated to describing the research question that gave rise to this thesis, as well as the path taken to arrive at the outlined outcomes in its conclusion. Section a) will discuss the relevance of this research, why it was carried out, and how it contributes to the current state of the art. Section b) will focus on the research question that arises from the context described so far, as well as the sub-questions that resulted in the development of the respective sections of this thesis. Section c) will delve into the hypothesis formulated to help address the questions posed, serving as a compass to guide the research in a specific direction and methodology. Section d) will describe the scope of the research, and, finally, section e) will concentrate on the methodology used, as well as on the structure of the thesis.

a) Relevance

18. The incorporation of digital technologies in education is speedily expanding. With it, the edtech industry is also on the rise, already contributing around 6% of the global gross domestic product (GDP) (Pangarkar, 2023). The global education technology market is expected to be worth $404 billion by the end of 2025 (HolonIQ Education Intelligence Unit, 2020) and $700 billion by 2028 (Walker, 2023). This represents a significant surge compared to the projected valuation of $76.4 billion for the worldwide education technology market in 2019 (Grand View Research, 2023). In 2021, the online learning platform Coursera, for instance, recorded 20 million new student registrations (Coursera, 2021), and there are at least 30 multi-million-dollar-funded corporations around the world focused on developing AI tools for education (Holmes, 2023, p. 64).

19. It is already a truism that technology is advancing too fast for the Law to keep up with it. The act of regulating presupposes evaluation and public discussion, which takes time and effort that are not proportional to the speed of technological change and innovation. Legal research is crucial to try to bridge this gap by analyzing the state of the art regarding the effectiveness of technologies in relation to what they aim to achieve and how they can affect the legal field. This includes understanding the objectives of education, particularly from a human rights perspective; examining the technologies' side effects, especially concerning children's privacy and data protection; striking a balance to maximize the benefits of technology while minimizing its harmful effects; and, finally, understanding the role of the Law in this equation and the available means to proper regulate technology.

20. To enhance digital readiness in education, the emphasis has been on expanding connectivity, digital infrastructure, and online tools. Nevertheless, aspects such as privacy, data protection, governance, and security have been somewhat neglected (Chakroun *et al.*, 2022). Considering that the global adoption of digital ICT and AI in education is a relatively recent phenomenon, which has intensified with the COVID-19 pandemic, it is necessary to understand whether the current legal framework is sufficient to address the presented challenges. More specifically, we should explore how we can maximize the effects of the available legal tools, such as the Convention on the Rights of the Child (CRC), data protection and procurement frameworks, to handle these challenges without waiting for new laws to be implemented. At the same time, we should map what is out of their scope and assess whether and how the Law should further regulate these issues, if at all.

21. This is only possible by understanding the Law as an applied social science, whose effects on individuals and groups must be grasped empirically and contextually. The cold text of the law tells us little about its real effects on society, and thus a comparative and bottom-up approach to the problem can be beneficial. Despite the existence of research on the risks stemming from specific applications of edtech, there still remains a gap in comprehensive analysis. This thesis therefore contributes to the existing body of knowledge by broadly mapping the risks that edtech can pose to children's rights to privacy and to the protection of personal data in Brazil and the European Union (EU), based on a transdisciplinary literature review and empirical analysis of a case study.

b) Research question(s)

22. The main question that guides this research is: *What are the challenges that edtech presents to children's rights to privacy and to the protection of personal data, and to what extent does the current legal framework in Brazil and Europe address them?*

23. This question can be broken down into several sub-questions, which will ultimately steer the development of the research and the unfolding chapters of the thesis:

i. What can be understood by edtech, and what are its main purposes?

ii. How does edtech, with its logic and design, interact with the concept of education and the long-standing discussions and theories caried out in this sector?

iii. Based on its main uses and technologies encompassed by the concept of edtech, how does it affect children's rights to privacy and to the protection of personal data?

iv. How do the EU and Brazilian legal frameworks currently regulate children's rights to privacy and to the protection of personal data?

v. Drawing on insights provided by the theory of data colonialism, is the current legal framework sufficient to address all the mapped challenges?

c) Hypothesis

24. Due to its comprehensive nature, the concept of edtech encompasses vastly different technologies both in terms of purpose and technical aspects. This results in diverse conditions under which they are used and different risks that could undermine children's rights. However, through the development of a typology, it is possible to identify commonalities among them that would warrant their collective consideration.

25. Considering the existing literature and the theory of data colonialism, the first part of the hypothesis of this research posits that the prevailing business model of digital platforms, characterized by the escalating datafication of human life and social interactions, particularly in the feeding of AI systems, as well as the commodification of data, engender several challenges surrounding the use of edtech concerning children's rights to privacy and the protection of personal data, including the intensification of surveillance, the reinforcement of

historical inequalities, the severe impact on life opportunities, the manipulation of individuals and groups, and ultimately, the erosion of digital sovereignty.

26. Although many of these challenges can already be addressed by the current legal framework, such as through data protection regulation, the latter's primarily procedural focus does not thoroughly considering the purposes for which data can be processed in the first place, and are not completely equipped to deal with the specific challenges posed by AI. Therefore, the second part of the hypothesis to be tested is that the EU and the Brazilian frameworks, including the application of oversight mechanisms, do not address some of these challenges. Because of historical inequalities between the two jurisdictions and the added layers of vulnerability inherent in Brazilian reality, the enforcement of existing rules is further hindered in the latter.

d) Scope of the research

27. **Technical Scope:** The analysis carried out throughout the thesis will be focused on data-driven edtech, encompassing technologies that collect, analyze, and make decisions based on (personal) data that affect people's lives. These activities can be executed through traditional data analysis technologies, using statistical methods and other mathematical techniques to recognize patterns, discover relationships and gain other insights from data. Nonetheless, this has increasingly been done by AI, including symbolic AI techniques or, more commonly (and also more heavily dependent on data), Machine Learning (ML) techniques. The latter will therefore be the main source of challenges to be discussed in Part III of the thesis. Within data-driven edtech, I will present a typology that differentiates between edtech used for *providing education* and for *learning about education* in Chapter 1.

28. **Legal Scope:** The focus of this thesis, concerning legal analysis, is on children's rights to privacy and to the protection of personal data. However, I acknowledge that human rights are indivisible and interdependent. In order to protect these two rights, others must be realized. Similarly, safeguarding the privacy and data of children is essential for the fulfilment of other rights. I therefore adopt a children's rights perspective regarding privacy and data protection rights, aiming to understand this complex framework in a holistic fashion.

29. **Geographical scope:** Technologies are social-technical artifacts that directly interact with the specificities of the communities in which they are embedded. Recognizing the need to analyze this socio-economic context beyond the legal framework, and understanding that the

operations of edtech companies are generally global, this research will focus on two different jurisdictions: the EU and Brazil. As will be later discussed, data protection laws in these two jurisdictions are remarkably similar as a result of the Brussels effect. However, changes in context result in distinct enforcement of these rights and varying effects of technologies within communities. Therefore, rather than a mere legal comparison, which could obscure the concrete application and effects of the Law in society, the aim is to compare socio-economic contexts and how they influence the application of data protection laws. This will be carried out within the context of a case study of Google Workspace for Education, as more thoroughly detailed in Part III of this thesis. The choice to analyze Brazil and the EU stemmed from the geographical location and past experiences of the doctoral candidate. Considering the context of the Joint PhD between the State University of Rio de Janeiro (UERJ) and KU Leuven in which the research was carried out and the fact that these two jurisdiction are part of different spectrums of social reality, the analysis of both situations had the potential to bring a wealth of important insights to the case study. Google Workspace for Education operates globally, yet its social impacts vary significantly across different parts of the world.

e) Methodological approach and thesis structure

30. In order to address the research question and sub-questions presented in Section b) and test the hypothesis outlined in Section c), this thesis employs various complementary and interrelated methods.

31. After this introduction, **Part I** will be developed through a *descriptive approach*, setting the stage for the subsequent analysis. Three chapters will be presented to elucidate the current context in which edtech is developed and deployed.

32. **Chapter 1** will focus on introducing what edtech means. It will offer a historical overview of its evolution to date, aiming to describe not only the journey leading to the technologies currently employed but also how methodologies and theories developed for conceptualizing preceding technologies help us comprehend the functioning and constraints of the current ones. I will additionally present a typology to synthesize and organize the complex landscape surrounding edtech. Although developed only for didactical purposes, this typology will be crucial for understanding the purposes for which these technologies are used and who they support, which directly changes the risks they present to children's rights.

33. **Chapter 2** aims to explore the interaction between the implementation of edtech and longstanding discussions within the field of education. This encompasses the role of the private sector in providing products and services, and, consequently, influencing strategic decisions in education; the phenomenon of "learnification" of education and discussions regarding what is to be "efficient"; the measurement movement in education and its relationship with datafication; as well as the dynamics of platform learning. The importance of this chapter for legal analysis extends beyond identifying the network of actors involved in providing education and their respective interests. It also involves understanding how the integration of edtech into these discussions can amplify specific challenges related to children's privacy and data protection.

34. **Chapter 3** will introduce data colonialism as the theoretical and normative framework adopted by this research, as described by Couldry and Mejias (2019). This chapter will outline the primary components and actors within data colonialism, illustrating its disproportionate impact on certain individuals and communities, particularly children, and examining its effects on both individual and collective autonomy. Together with the legal framework, this theory will serve as a normative lens to evaluate the deployment of edtech and the challenges it poses to children's rights in Part III. It can also thus help assess the sufficiency of the current legal framework to deal with these challenges.

35. **Part II** is focused on *describing and evaluating* how the current legal framework regulates children's rights to privacy and to the protection of personal data.

36. **Chapter 4** will present the literature on the reasons why children require special consideration when it comes to protecting their rights to privacy and to the protection of personal data. Their status as human beings in development and their proportionally larger digital footprint compared to adults will be highlighted as crucial fundamentals for this special treatment. This chapter acknowledges the importance of viewing technologies not only through a lens of risk and protection but also as a means for opportunities and developing children's autonomy. Considering the scope of the thesis, which is focused on identifying the main risks that edtech poses to children's rights to privacy and data protection, the chapter will introduce a risk classification of children's online presence, highlighting how surveillance technologies can significantly impact children's development and learning. However, it also highlights how edtech has a critical role in realizing different human rights, when deployed in a way that respects children's specificities.

37. **Chapter 5** will present the CRC as a fundamental human rights framework adopted by Brazil and the EU, which recognizes children as rights holders and holistically address the specificities mentioned above. This chapter will present the main provisions in the Convention applicable to the scope of this thesis and how some cross-cutting standards (should) influence the interpretation and implementation of the legislative and policy pieces discussed in the following chapters. **Chapters 6 and 7** will respectively describe and evaluate the EU and Brazilian legal frameworks dealing with children's rights to privacy and data protection, as well as applicable policy to edtech.

38. It should be highlighted that this thesis will not adopt a traditional legal comparative methodology, as mentioned above. Comparisons between the EU General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais* - LGPD), in particular, are inevitable due to the considerable similarity between these legal frameworks. However, the thesis' aim is to focus on the social contexts of the application of each law. I will outline some challenges brought by a mere legal transposition of European legislation without necessarily considering Brazilian specificities, especially regarding its institutional design. This will be done in a contextualized manner in Part III of the thesis through a case study, which attempts to discuss how these aspects influence the protection received by data subjects, even with such similar laws being implemented.

39. **Part III** will be formulated based on a *descriptive, evaluative and normative* approach and it has two main focuses. First, **Chapter 8** will map challenging aspects that data-driven edtech raises to children's rights to privacy and to the protection of personal data. I will outline the risks posed by AI systems in general and their intersection with education. Afterwards, I will highlight certain technologies as presented in the developed typology and discuss how particular challenges can be identified in their implementation.

40. The second focus is a case study of the application of Google Workspace for Education in the EU and in Brazil. Google pioneered the development of data-driven business models (DDBM) on the scale that we currently know and Google Workspace for Education is largely adopted worldwide. This model has been widely replicated by other edtech, and even when schools adopt technologies from different companies, Google is still often involved in a broader network of data sharing. Studying Google's dynamics can thus provide a framework to understand other commercial edtech and their impacts on children's rights. Furthermore, in recent years, particularly amid the COVID-19 pandemic, European Data Protection Authorities

(DPAs) have been actively involved in cases related to this technology. This engagement offers valuable insights into its operation and the challenges stemming from its implementation.

41. **Chapter 9** will describe how Google Workspace for Education works, the history of its development, and how it is related with the overarching Google's business model.

42. **Chapter 10** examines its impact on children's privacy and data protection in the EU and in Brazil. First, I describe decisions made by authorities of different EU Member States (MS) that involve the use of Google Workspace for Education by public schools. Considering the auditing and analysis capabilities of certain authorities, especially DPAs, it is possible to have a more in-depth view of the risks, which the mere assessment of Terms of Service (ToS) and Privacy Policies would not provide.

43. The chapter also discusses the implementation of Google Workspace for Education in Brazil. Since the Brazilian DPA has not yet assessed it based on the Brazilian framework, an analysis of the ToS and Privacy Policies applicable to the platform in the country will be conducted. This will be complemented by a literature review on research that have also performed a similar exercise.

44. **Chapter 11** undertakes an analysis of the collected information from both jurisdictions, aiming to understand the systematic functioning of Google Workspace for Education beyond compliance with the GDPR and LGPD, within the context of data colonialism and the application of AI technologies. Initially I will evaluate the similarities, differences, and deficiencies apparent in the current landscape, drawing upon the insights provided in Chapter 10. I will then discuss how data colonialism's main aspects can be identified in the case study. This chapter also assesses the extend to which legal frameworks for personal data protection in the EU and in Brazil deal with such challenges.

45. The thesis will be wrapped up with **concluding remarks, recommendations, and indications for future research**. In addition to summarizing the results of the thesis, this section will present its conclusions, high-level recommendations on how to move forward in relation to the identified challenges, as well as topics for future research.

46. Finally, it is important to mention that this thesis follows the author-date citation style of the Brazilian National Standards Organization (*Associação Brasileira de Normas Técnicas* - ABNT), as adopted by UERJ, the host university.

PART I. SETTING THE SCENE

47. Part I adopts a descriptive approach aimed at laying the context for the legal analysis. To map out the effects that edtech has on children's rights to privacy and to the protection of personal data, it is first necessary to understand what type of technologies are under the scope, what educational context they are inserted into, and which theory will be used to interpret these effects.

48. Chapter 1 will thus provide the history of the development of edtech, as well as a possible definition of it. Reflecting on the past is beneficial not only for understanding our current position and the reasons behind certain phenomena but also for learning from mistakes to prevent their recurrence. Building on this historical background and the literature review, this chapter also introduces a typology of edtech based on their purpose and target audience. This typology will serve as a framework in the final part of this thesis to analyze the risks associated with specific technologies.

49. Chapter 2 acknowledges that edtech is not deployed in a vacuum and that education, in general, and pedagogy, as a specific science, are imbued with centuries-old discussions about how education and learning should be carried out. Technologies are never neutral and will reflect the worldview of their developers, as well as their vision of how education should take place. The risks presented by edtech are therefore also influenced by their interaction with the context in which they are deployed, as well as their leading actors.

50. Finally, Chapter 3 discusses data colonialism as the theoretical and normative framework adopted by this thesis. This theory provides us with important insights to understand risks that may still be present even if the current data protection laws are complied with.

Chapter 1. The use of technology in education

51. The history of edtech is intertwined with the history of humanity's relationship with knowledge. What this timeline includes, therefore, greatly depends on the very definition of education, of technology and, consequently, of edtech.

52. Education is often understood as the discipline "concerned with methods of teaching and learning" or with "the transmission of the values and accumulated knowledge of a society" (Lawson *et al.*, 2023). It can also be seen a process involving "activities aimed at the

development of productive, thoughtful, and responsible persons. These activities result in learning, or stable and persisting changes in what a person knows and can do" (Spector, 2015, n.p.). These two definitions share the idea that students are educated either to acquire knowledge or to develop a particular skill. Even in the second definition, where educational activities include the development of productive, thoughtful, and responsible people, the emphasis is still on what a person can know or do and not necessarily on what they become.

53. With a broader and more critical view, Paulo Freire, a Brazilian pedagogue, understands education as a process of knowledge development, political formation, ethical manifestation, pursuit of beauty, scientific and technical empowerment (Freire, 2001). Freire understood History as a possibility, as something in motion that can actually be changed. This does not deny the role of the conditioning factors to which humanity is subjected. However, by opposing the future as something inexorable, the notion of History as a possibility recognizes the importance of human decisions as acts that imply rupture. It acknowledges the importance of consciousness and subjectivity, of the critical intervention of human beings in the reconstruction of the world (Freire, 2001). Education, therefore, plays a decisive role in the transformative path towards critical individuals and more politicized, democratic, equalitarian and empathetic societies.

54. This broader understanding of the aims of education is aligned with the ones defined in arts. 28 and 29, CRC, as will be discussed in Part II, of this thesis. Focusing on the transformative and multiplier role of education is essential to gauge the power that edtech has in shaping it. If we fail to promote a suitable environment to achieve these goals, we risk hindering the development of both individuals and society as a whole. This already demonstrates the need to treat education as a strategic and inherently public good which demands transparent, democratic and fair decisions.

55. Akin to education, the concept of technology has also been contested throughout history. Saettler (2004, p. 3) understands technology[2] as "a system of practical knowledge not necessarily reflected in things or hardware" (Saettler, 2004, p. 3). In the same vein, for Spector (2015, n.p.), technology would be "the systematic and replicable application of knowledge to achieve a purpose. Some technologies can be seen and touched (e.g., computers), whereas others are in the form of specific ideas and methods (e.g., a sorting algorithm)".

[2] From the Greek form techne, translated as art, craft, or skill plus logos, Greek for word, study or knowledge.

56. On the other hand, Salomon (1984) argues that the use of the word technology to define technical arts themselves more than the *discourse* on the technical arts is recent. According to the author, this happened mainly when these artifacts started to become something other than arts but a scientific endeavor.

57. The author stresses the importance of differentiating *technology* from *technique*. The English language has no real equivalent of the word technique as used in French, German and Slavic languages. In these languages, more than something related to skills or methods, technique refers to all activities associated with things technical. Therefore, he argues that the changes introduced mainly from the XIX century onwards, when science and technical arts became more connected, are fundamental to the very meaning of technology (Salomon, 1984).

58. It is not under the scope of this thesis to dig deeper into this discussion. Indeed, what is commonly called edtech today will more often than not be related to this more refined state of *technique*, as "the application of *scientific knowledge* to the practical aims of human life" (The Editors of Encyclopaedia Britannica, 2022, emphasis added). This is what will then inform the concept of edtech as described below. However, for the purposes of understanding the history of edtech, some educational *techniques* would also be considered to set the scene for the following developments.

59. As becomes clearer with the different views on education and on technology, there is also no single and uncontroversial way of defining edtech, and many of the existing definitions contradict each other (Czerniewicz, 2010). Based on the definition of education by Freire and the broader understanding of technology, edtech will be understood in this thesis as the application of scientific knowledge to support both the acquisition of knowledge and skills, as well as the development of critical, ethical, and socially responsible individuals.

1.1 A brief history of edtech

60. In this section, I will present a brief overview of the historical evolvement of edtech. Looking at the past is an important exercise to gain insights into the trajectory of current edtech, appreciating the challenges, advancements, trends and patterns that influence how we understand the role of edtech in our current society and how they can better serve children and education. However, it is not my intention to tell the story of edtech as something that builds up to the introduction of computers or AI, which are often seen as the pinnacle of this progression.

61. Watters (2019) warns that this kind of thinking runs the risk of suggesting that education has become increasingly and *necessarily* technological over time. It can portray the digital classroom as an inevitable outcome, promoting a vision of teaching and learning that heavily rely on technology (Watters, 2019, parag. 1). The use of technology in education is truly promising and has the potential of realizing several fundamental rights, as emphasized in the introduction. However, as this thesis will argue, there is still a tendency to advocate for the use of technology for its own sake without engaging in a broader discussion about its alignment with predefined pedagogical goals and its necessity and proportionality when its benefits are weighed against its side effects.

62. To view these historical developments in such a teleological manner would prioritize the role of technology at the expense of other social, economic, or political issues that played a significant role. Each technology has its own value and was/is important for its own reason. Unfortunately, it is not feasible to cover all the political, social, and economic aspects of each development. Nonetheless, this disclaimer is necessary for the critique that will follow later in the thesis and for encouraging readers to explore these developments and their implications further through the literature cited in this work.

63. It is also worth noting that while edtech is ubiquitously present in all continents, its development and application have not been uniform. The COVID-19 pandemic has exposed significant disparities in the access to technologies used to maintain learning processes, which are often dictated by technical and financial constraints (UNESCO, 2023a).

64. This overview, therefore, will primarily focus on the moment of the emergence of the respective technologies. This approach is not without its problems, considering that, for the most part, the technologies mentioned below were primarily developed and used in Europe and the USA before spreading to the rest of the world. Thus, the use of some of these technologies in other regions, especially in Brazil, as well as some of the consequences of importing this technology, will be discussed later in this thesis. The history below is also not intended to be exhaustive; rather, its purpose is merely illustrative, highlighting key milestones that influenced the way current edtech is developed and deployed, as well as societal perceptions surrounding them.

65. The use of practical ways to transmit knowledge and to improve learning can be traced back when tribal priests systematized knowledge or when pictographs were used in early cultures. The very development of writing—such as the Sumerian script and the Egyptian

hieroglyphics—can be considered as one important way to facilitate communication and education. Other instruments, such as the abacus[3], analogue computers[4] and the quill pen[5], were also gradually introduced.

66. The invention of the printing press was undoubtedly a watershed in history. It made it possible for previously laboriously handwritten books to be produced quickly and at scale, which increased access to knowledge like never before (Saettler, 2004). With the spread of written knowledge, there was also an expansion of formal education in Europe, which led to the Renaissance and the Enlightenment periods.

67. In 19th-century Europe, improvements in transport infrastructure led to the development of the first distance degree program in the University of London in 1858 (Bates, 2019). In 1873, a network of women teaching other women through the mail was founded by Anna Eliot Ticknor, the Society to Encourage Studies at Home (Briggs, 2014). During this period, technologies such as lantern slides also began to be utilized in the USA, particularly for adult education, thus initiating the visual education movement (Saettler, 2004).

68. At the end of the 19th century and the beginning of the 20th century, the invention of the motion picture profoundly accelerated the use of technologies in education and its effects are still felt today. The great potential that this new technology could have for education was already perceived in the 1910s, both in Europe and in the USA. In 1911, Thomas Edison was one of the pioneers in producing films for the educational setting, having released a series telling the story of the American Revolution (Saettler, 2004).

69. In the New York Dramatic Mirro's issue of July 9, 1913, Edison prophesied that books would become obsolete in schools: "[s]cholars will soon be instructed through the eye. It is possible to teach every branch of human knowledge with the motion picture. Our school system will be completely changed in ten years" (Edison, 1913, n.p., as cited in Saettler, 2004, p. 98). This drastic change was not possible in 10, but certainly in 100 years. A century later, as will be described below, Massive Open Online Courses (MOOCs) would become extremely popular.

---

[3] The abacus is a calculating tool used at least since 480 BC by several cultures such as the Egyptians, the Greeks and Chinese (Briggs, 2014).
[4] Several mechanical analogue computers were developed in ancient times for astronomical calculations such as the astrolabe and the Antikythera mechanism (Briggs, 2014).
[5] The quill pen was usually made from a bird feather and were introduced around 700 AD (Briggs, 2014).

70. At Columbia University, Professor Ben D. Wood, together with University of Chicago Professor Frank Freeman, conducted a study with around 11,000 students involving the use of films in geography and general science classes. The results showed that students who were taught using films scored higher on end-of-unit assessments than those who were taught using printed materials. The study's findings suggested that using teaching films could be a successful way to enhance the effectiveness of traditional pedagogical methods in schools (Watters, 2021, p. 64–65).

71. According to Wood, schools should be more attuned to the individual needs of students. In order to achieve this goal, however, the education system should transition to what he referred to as "mechanical education", which is not to be confused with a mechanistic approach.

> Perhaps this seems counterintuitive: to individualize education, one must automate it. To resist mechanistic education, schools must mechanize. But for education reformers in the early twentieth century (as for those in the early twenty-first), it was a conundrum they managed to justify. Indeed, this contradiction gets at the heart of calls for "personalization" and is central to a vision—then and now—of a modern, high-tech, progressive learning experience (Watters, 2021, p. 68).

72. The 1920s saw the emergence of educational radio (Saettler, 2004). Although its popularity dropped, especially with the rise of television broadcasting in the mid-XX century, it is still important for educational purposes in various parts of the world (see, for example, Damani and Mitchell (2020)). This was an important milestone for the history of edtech, since it marked the introduction of ICT in education (UNESCO, 2023b).

73. It was also in the 1920s that the first paper on and a prototype of an "automatic teacher" was presented by Ohio State University's Professor Sidney Pressey in the joint meeting of the American Psychological Association (APA) and the American Association for the Advancement of Science of 1924 (Watters, 2021, p. 35–36). The machine had various versions, but the most sophisticated one was based on a typewriter. While working on a set of questions on a printed sheet, the student would use the device's keys to choose their answers. The system was designed to immediately inform students whether their selection was correct, and it impeded them from proceeding to the next question until they had it right (Holmes; Bialik; Fadel, 2019). As will be discussed in the last part of this thesis, this strategy is still highly used by current personalized learning technologies.

74. His initial attempts to put the device on the market and later to keep it were not successful for many reasons, but he continued his academic research on the topic. He was one of the first to argue that "[u]nlike the 'mass education' of the radio or the film projector, […]

his Automatic Teacher would foster a more individualized classroom […] and free the teacher from the mechanical tasks" (Watters, 2021, p. 44–45).

75. The first typewriter was developed in 1868 (Cortada, 1993), and in the early 1890s, William A Mowry and Frank Palmer already advocated the use of the machine in secondary schools. However, it was not until 1932 that Professor Ben D. Wood, once again working alongside Professor Frank Freeman, conducted research that demonstrated the benefits of using typewriters in classrooms, including enhanced reading habits among students and an increase in the amount of written work produced. This ground-breaking study paved the way for widespread acceptance of typewriters in the classroom, and subsequent research further confirmed their advantages for learning (Cothran; Mason, 1978).

76. As a consultant to the International Business Machines Corporation (IBM), Professor Wood was also responsible for using machines to analyze test scores. In 1932, an IBM tabulator was adapted to score the Strong Vocational Interest Blank, a test used for student counselling that was previously costly to grade and analyze. A few years earlier, Reynold B. Johnson, had developed his own test scoring machine, the so-called "Markograph" and was afterwards hired by IBM. IBM developed the first commercial test-scoring machine in 1938 (Watters, 2021, p. 72–73).

77. Although IBM's scoring machines were not a commercial success, they influenced the testing industry and the way education was viewed.

> Just as Wood's work with the typewriter industry had likely decreased those companies' interest in manufacturing the machine that Pressey had designed, Wood's work with IBM seemed to convince the company that "mechanical education"—individualized education—was to be achieved through large-scale data analysis and testing machines (Watters, 2021, p. 79).

78. In the 1940s, the invention of the television was seen as a solution to several issues within the educational system, such as teacher shortages and overcrowded classrooms. In the USA, the introduction of classroom-based instructional television in 1947 by the Philadelphia school district marked a ground-breaking initiative and involved broadcasting one educational program per week. During the 1950s, the first educational television programs designed for public broadcasting were developed (Levin; Hines, 2003, p. 264).

79. The City Colleges of Chicago took a pioneering step in 1951 by establishing a comprehensive system for large-scale instructional television programs that offered academic credit. This innovative approach allowed students to earn a degree solely by enrolling in

television courses (The Education Coalition, [*s. d.*], n.p.). In Europe, television was first used in the 1960s for educational purposes (Bates, 2019).

80. In 1953, after visiting his daughter's fourth-grade math class, Harvard psychology professor B. F. Skinner was surprised by the way children were being taught. The students were seated at their desks, solving arithmetic problems displayed on the blackboard. The teacher moved between the rows of desks, observing the students' work and correcting their mistakes. Some students finished quickly and awaited the next set of instructions, while others struggled and were frustrated. After the lesson, the teacher collected the papers to grade and returned them to the class the next day (Watters, 2021, p. 19).

81. This violated the basic principles of Skinner's behaviorist theory of learning and tried to adapt the experiments he has been carrying out with rats and pigeons to people. He tried then to build teaching machines, continuing the work of Sydney Pressy in the 1920s. In one of the models, paper disks containing questions would show up in one window, while the student would write their response on a roll of paper through a second one. The mechanism would automatically hide the student's answer, preventing any alterations and simultaneously unveiling the correct one. This way, Skinner's teaching machine delivered automatic and immediate reinforcement to students (Holmes, 2023, p. 95–96).

82. In regular classrooms with human teachers, they would move too fast for some students and too slow for others. Therefore, Skinner thought that machine instruction would be the solution for students to move at their own pace. This would realize the "industrial revolution in education" and make it more efficient (Skinner, 1958, p. 969). Although some would see this as a way of implementing mass production, Skinner was of the opinion that the machines could rather act as private tutors. His view deserves to be cited in full length:

> (i) There is a constant interchange between program and student. Unlike lectures, textbooks, and the usual audio-visual aids, the machine induces sustained activity. The student is always alert and busy. (ii) Like a good tutor, the machine insists that a given point be thoroughly understood, either frame by frame or set by set, before the student move on. […] (iii) Like a good tutor, the machine presents just that material for which the student is ready. […] (iv) Like a skillful tutor the machine helps the student to come up with the right answer. It does this in part though the orderly construction of the program and in part with techniques of hinting, prompting, suggesting, and so on, derived from an analysis of verbal behavior. (v) Lastly, of course, the machine, like the private tutor, reinforces the student for every correct response, using this immediate feedback not only to shape his behavior most efficiently but to maintain it in strength in a manner which the layman would describe as "holding the student's interest" (Skinner, 1958, p. 971).

83. The resemblance with today's intelligent tutoring systems (ITS) and with the rationale behind edtech is surprising, although not a coincidence. Like teaching machines, current edtech,

especially the ones built for personalized learning, intends to present the content according to each student's level. They use nudges and other psychological mechanisms to guide learning and seek to reinforce certain behaviors to hold students' attention. This shows how much the current technology is still based on behaviorist approaches of learning instead of more progressive ones.

84. Skinner's work has laid the foundation for the functioning of current edtech, especially the ones powered by AI. However, the teaching machines cannot be said to be adaptive, as students would go through the same set of questions and content, although at their own pace. This feature was what Gordon Pask tried to implement also in the early 1950s. SAKI, the self-adjusting keyboard tutor, was created to assist keyboard operators in mastering the use of a card-punching device for data processing. The assigned exercises were tailored according to the learner's unique progress, as indicated by a dynamic probabilistic student model (Holmes; Bialik; Fadel, 2019, p. 98).

85. The rapid development of ICTs in the second half of the 20th century dramatically changed how humanity deals with data and knowledge, bringing new perspectives to the educational sector. The rise of personal computers (PC) in the 1970s and 1980s made this technology more accessible, especially in Europe and the USA. In 1971, Michel S. Hart typed the text of the United States Declaration of Independence and transmitted it to others in the computer network he had access to at the University of Illinois. It was the first document of what would become the Project Gutenberg[6].

86. After the Apple II's release in 1977, the Minnesota Education Computing Consortium procured 500 computers to distribute among schools in the state. In the 1980s, Apple initiated a campaign to promote the usage of their computers in American public schools. They actively lobbied for the passage of a bill in the US Congress and in California to support their cause. In California, a bill was passed granting a 25% tax credit against the state corporate income tax for computer equipment donations to schools. Taking advantage of this incentive, Apple donated a computer to each of the approximately 9000 eligible elementary and secondary schools in California. This significant expansion into California's educational institutions, combined with the launch of the Macintosh in 1984, led to Apple's rapid domination of the education PC market, at least for a certain period (Watters, 2015).

---

[6] Project Gutenberg is the first online library of free eBooks to be ever established (Project Gutenberg, [*s. d.*]).

87. In Finland, the subject of "automated data processing" was introduced in schools. Programming was not being taught to train programmers, but rather to develop student's logic and math skills (Leinonen, [*s. d.*]). However, with all the challenges that computers raised at that moment, teachers who constantly used them in their classrooms were the exception (Corcoran, 2013).

88. At this stage, pedagogical thinking was often based on Computer-based Training (CBT)[7] or Computer-based Learning (CBL)[8], types of Computer-Aided Instruction (CAI), where the interaction would occur between the student and computer drills, micro-worlds and simulations. However, these programs lacked adaptability, which Jaime Carbonell attempted to implement through a system called SCHOLAR in 1970. This is known to be the first implementation of AI in CAI (Holmes; Bialik; Fadel, 2019, p. 100).

89. A second phase of the history of computers in education began in the late 1980s and early 1990s when multimedia computers came to the mass market. Multimedia was seen as a method to cater to the different ways people learn (Leinonen, [*s. d.*]). The advent of the Compact Disc-Read Only Memory (CD-ROM) was probably the first way most people came into contact with educational programs for computers.

90. The popularization of the World Wide Web in the mid-1990s, even with the simple design characteristic of Web 1.0, created many opportunities for education. First, it removed the filter of knowledge publication and for this alone it can be considered the most significant socio-technological change since the invention of the printing press. With the wikis at the end of the 1990s, this process became collaborative, a shared enterprise. Second, it made communication (such as between researchers) easier. Teaching resources also began to be shared, which started the open education movement (Weller, 2020).

91. As with almost anything in this period, learning gained its *e-* form. The concept of e-learning started to spread, and although it initially covered any use of electronic media in

---

[7] CBT is an interactive instructional approach in which the computer, taking the place of an instructor, provides a series of stimuli to the student ranging from questions to be answered to choices or decisions to be made. The CBT then provides feedback based on the student's response (Computer-based training, 2009).

[8] "Computer-Based Learning has emerged in response to Computer-based training (CBT) and as its name it is more focused on Learning. […] The 1980's and 1990's produced a variety of schools that can be put under the umbrella of the label "Computer Based Learning" (CBL). Frequently based on constructivist and cognitivist learning theories, these environments focused on teaching both abstract and domain-specific problem solving. Preferred technologies were micro-worlds (computer environments were [sic] learners could explore and build), simulations (computer environments where learner [sic] can play with parameters of dynamic systems) and hypertext" (Computer-based learning, 2009, n.p.).

learning, its interpretation gradually narrowed down to online learning (Weller, 2020). The hype around e-learning, however, also presented its challenges. With e-learning, the e-learning industry and markets for courses and systems emerged. However, many of these offerings were developed without a thorough prior assessment of their actual need and purpose (Leinonen, [*s. d.*]). As often happens with other edtech, they

> were shown to be designed primarily to prove their success rather than to find solutions to perennial educational problems. The prevailing impulse of these innovations and reforms [was] characterized solely by a desire for improvisation and typically they lacked any sound theoretical or experimental foundation (Saettler, 2004, p. 399).

92. Around 2002, Learning Management Systems (LMS), or Virtual Learning Environments (VLE), became the dominant and most successful edtech. They were created to be the central e-learning technology, and it dismissed the need to use several tools at once, such as bulletin boards for communication, content management systems and web pages (Weller, 2020). In the beginning, LMS were often used as a virtual replica of the physical classroom, where lectures and notes would be uploaded without much experimentation in terms of pedagogy. Its true potential was only realized with time.

93. In terms of terminology, the term VLE has been criticized because of the word "virtual" and of the idea that "learning through such an environment is a poor relation to any learning that takes place in a face-to-face setting" (Weller, 2007). With the intense increase in the number of sensors implemented in physical spaces, the existence of a virtual world was also contested, since it could imply that it is not real or its consequences not as tangible. On the other hand, LMS has also been objected due to the suggestion that it could manage students' learning, which would not be aligned with more exploratory and constructivist pedagogies (Weller, 2007). Ultimately, however, these two terms have been used interchangeably and can be considered synonyms.

94. Around 2007, there was a peak of interest in the so-called online virtual worlds, especially by higher education institutions. The platform Second Life was particularly popular and universities would lease islands to create their own virtual environment through avatars. At the time, it was mainly used for lectures, and it could be integrated with other technologies such as the LMS Moodle (Weller, 2020).

95. Weller (2020) notes that, although the expectations were very high, they did not gain much traction. First, there was a lack of imagination on how to use it beyond lectures. If that was the main goal, regular streaming technology could be used instead. Second, it required

good computer hardware and internet broadband, which was not the case for all students and schools. There was also the problem related to abusive behavior, such as virtual vandalism or classroom interferences. In terms of accessibility, some students were not able to use the online environment due to visual impairments. This is as a prime example of technology being used for its own sake, taking precedence over serving a pedagogical purpose (Weller, 2020). These ideas are currently reflected in the use of the metaverse in education, as will be further discussed below.

96. The rise of online worlds has also emphasized the use of games for educational purposes, as well as the implementation of gamification design patterns in edtech more broadly. Gamification can be understood as a "design strategy used to promote engagement and activity across a wide range of digital products and services" (5Rights Foundation, 2021, p. 34) and is increasingly used in education. Digital badges, for example, became a trend in 2015 and are used to digitally represent skills or experiences acquired by the student (Weller, 2020). With different technologies competing for children's attention and with the increasing implementation of stimuli for completing tasks (highly linked to behaviorist views of education), gamification strategies are increasingly present in edtech.

97. By 2011, with the plethora of services available for learning, a new movement began gaining traction. The collection of the various support tools used by learners and educators came to be known as "Personal Learning Environment (PLE)" and it was seen as a way to enable learners' control and personalization. Instead of a single LMS technology universally used by all, PLEs could be built by learners themselves based on their needs. Initially conceptualized as simple diagrams illustrating the tools individuals employed within their learning contexts, discussions quickly shifted toward the potential integration of data from these diverse platforms (Weller, 2020).

98. Despite various factors leading to the eventual waning of the PLE hype, personalization has remained a coveted goal in education. The SCHOLAR system, as previously described, is considered to be the first ITS, which is the base for the majority of the technologies used for personalized learning today.

99. 2012 was declared by The New York Times as the year of MOOCs (Pappano, 2012). Although the idea of running open courses was not something novel by this time, the convergence of some technologies as well as the sudden popularity of Stanford professor Sebastian Thrun's course on AI attracted all possible headlines (Weller, 2020). Many have

portrayed MOOCs as revolutionary technology, but they did not live up to all expectations. Among the emerged issues were low competition rates, lack of demographic diversity (most participants were already educated) and lack of a sustainable business model. Over time, MOOC providers began integrating e-learning within traditional education systems and underwent changes to their business models.

100. From a strictly educational point of view, MOOCs offered numerous advantages, including the expansion of learning opportunities and open practices (even if this is the case only for enrolling and not for licensing) (Weller, 2020). However, the rise of MOOCs revealed a deeper attitude towards edtech and the narrative created around them played a significant role in their success. The first element of this narrative is the idea that "education is broken". The second is the belief that Silicon Valley technologies were the solution (Weller, 2014). This narrative persists today, as briefly discussed in the introduction, and permeates the deployment of several other edtech. In 2021, the number of students enrolled in MOOCs reached 220 million (Shah, 2021).

101. After the MOOC trend, 2014 was marked by the peak of the discussion on learning analytics and the role of AI in education more broadly. The use of AI in education, with its automation capabilities based on associations, brings about a tremendous shift compared to traditional edtech. It not only captures data but also detects patterns within them and automates decision-making (Cardona; Rodríguez; Ishmael, 2023, p. 1).

102. These features can enhance educational services by improving the adaptivity of learning resources and supporting teachers' roles through automation. For instance, AI systems can draft curriculum and lesson plans, recommend content and help teachers develop tests. Educational chatbots help guide student learning, student admission and learning feedback (Hillman *et al.*, 2023). However, they also raise serious concerns regarding privacy and data protection, due to their need to use large amounts of data, as well as their ethical and pedagogical implications. The automation feature of AI also promotes scalability, which means that the unintended or unexpected consequences can be direr (Cardona; Rodríguez; Ishmael, 2023, p. 3) and individualistic solutions can be shortsighted. Considering that AI capabilities permeate the main edtech adopted nowadays, these risks, mainly those related to children's privacy and data protection, will be unpacked in due time throughout the thesis.

103. Since the early 2000s, biometric technology—used for measuring a person's unique characteristics for identification purposes—has also been gradually introduced in schools

worldwide. These characteristics include fingerprints, iris scans, voice patterns, behavior and more. Such data serve various purposes, such as enhancing school security, facilitating canteen payments, managing library borrowing, controlling door and locker access, enabling photocopying and access to computers etc. (Swist *et al.*, 2022). The use of biometrics in schools sparks a debate not only concerning the challenges posed by AI and datafication, but also regarding the necessity and proportionality of using very intrusive and surveillance technologies in education, especially when other forms of identification could suffice for the school's intended purposes (King; Persoon, 2022).

104. Around the mid to late 2010s, XR technologies became more accessible and affordable, thus being increasingly used for educational purposes. XR is a multimodal technology, which enables the merging of physical and digital realities. It includes augmented reality (AR), virtual reality (VR) and mixed reality (MR) (Cortesi *et al.*, 2021, p. 6).

105. The applicability of XR in education is still under-researched, but, according to Cortesi *et al.* (2021, p. 9–10), preliminary evidence suggests that XR could be potentially used in three main areas. First, XR technologies offer potential for skill-based learning, particularly in learning foreign languages, as immersion has shown to be beneficial for it. Second, XR can significantly broaden the range of hands-on learning experiences available to students, such as virtual journeys inside the human body. Lastly, XR provides new functionalities and opportunities for learners to engage in new ways that were previously not possible with other technological tools. It could be used, for example, in architecture classes to simulate designs.

106. Seen as the culmination or realization of the full potential of XR, as well as a way to solve some of the issues brought about by the COVID-19 pandemic, the metaverse is perceived as a technology that holds significant potential for education. Although the first attempts to introduce "virtual worlds" in education did not succeed around 2007, the metaverse discussions came back with a vengeance after more than a decade, with even the company Facebook changing its name to "Meta" to mark this "new phase" of the internet—and also for rebranding purposes due to the controversies associated with its previous name (Isaac, 2021). Even nowadays, however, it can be said that society is still not technologically nor culturally ready for the metaverse. With the rising popularity of games such as Roblox, Minecraft and Pokemon Go, what we witness is a plurality of online worlds within a multiverse (Peckham, 2020) that represents the transition to the new digital frontier.

107. In education, metaverse-based learning promises to be more than the combination of in-person learning and screen-based remote learning. The main idea is to compensate for the limitations of both models (Zhang *et al.*, 2022), blending the analogue, online and augmented reality together for a seamless transition. However, the current state of the "multiverse" is still in the hands of a few companies. If education is to somehow profit from this new technology, it is crucial to start a discussion on public-service media and non-commercial zones in the metaverse, where under-served ideas, information and communities can flourish (Kleeman, 2021).

108. In 2020, the COVID-19 pandemic disrupted education around the world and every social interaction became digital by default. As described in this history, (digital) ICT have always played an important role in education, but the pandemic accelerated their implementation overnight. It indeed introduced new ways of learning, but also exacerbated existing inequalities, which prevented many children from fulfilling their right to education. Even when technology was easily accessible, technology-centered methods often resulted in low engagement and poor achievement (UNESCO, 2023a, 2023b, p. 12). It also aggravated the risks to children's right to privacy and data protection, as they would use the digital environment not only for learning, but also for playing, and socially interacting.

109. With the limited historical distance currently available, we can view the COVID-19 pandemic as a prime illustration of the risks of technological solutionism and "challenge the assertion that educational technology investment necessarily strengthens education system resilience, and […] that expenditure on education technology should necessarily scale up" (UNESCO, 2023b, p. 12).

110. At the end of 2022 and beginning of 2023, with the launch of ChatGPT, generative AI systems became extremely popular and have once again sparked discussions on the role of AI not only in education, but in society as a whole (Center for Democracy & Technology (CDT), 2023). The very concept of generative AI is still disputed, but one way of defining it is "a technology that (i) leverages deep learning models to (ii) generate human-like content (e.g., images, words) in response to (iii) complex and varied prompts (e.g., languages, instructions, questions)" (Lim *et al.*, 2023, p. 2). As a relatively new technology, the challenges and opportunities of its use are still being mapped, but attention has been especially given to discussions like plagiarism, the relevance and role of assessments, limitations in relation to current data, the spread of misinformation, and new skills that students and teachers will need

to develop (Center for Democracy & Technology (CDT), 2023; Lim *et al.*, 2023; UNESCO, 2023b).

111. Looking ahead towards the future of edtech, in a rapidly evolving world, new technologies emerge at an ever-accelerating pace, and AI systems capabilities seem to be developing on a monthly basis. This emphasizes the need not only to understand the operation of each of these emerging technologies but also to determine what kind of education we envision and what schools should offer to enable students to navigate a future in which humans and machines will be intricately interconnected. Understanding education as a promoter of the vision of history as possibility, more important than ever, "[e]ducation systems need to return agency to learners and remind young people that we remain at the helm of technology. There is no predetermined course" (Giannini, 2023, p. 4).

1.2 Edtech typology

112. As the brief history outlined above demonstrates, a wide range of technologies has been applied to education. For the most part, they were not initially designed for this specific purpose, which gives rise to particular challenges related to children's human rights. To systematize the discussion and gain a better understanding of edtech's various applications, this section aims to present a possible typology of edtech. This typology will serve as the foundation for explaining the scope of this thesis and determining the technologies that will undergo a legal analysis.

113. This typology was developed through the clustering and adaptation of previous research, as in Fedders (2019), Holmes *et al.* (2019), Pangrazio, Selwyn and Cumbo (2022), and Holmes *et al.* (2022). Since the central topic of this thesis is understanding the risks associated with children's rights to privacy and to the protection of personal data, the typology will focus on digital ICT. ICT are understood as

> a diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players, and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.) (UNESCO Institute for Statistics (UIS), 2009, p. 120).

114. More specifically, this thesis will concentrate on data-driven digital ICT, which encompasses technologies that collect, analyze, and make decisions based on data. These processes can be carried out by traditional data analysis technologies (which heavily rely on humans), using statistical methods and other mathematical techniques to identify patterns,

discover relationships and gain insights from data. However, more often than not, this has been done by AI, including symbolic AI techniques or, more commonly (and also more heavily dependent on data), ML techniques.

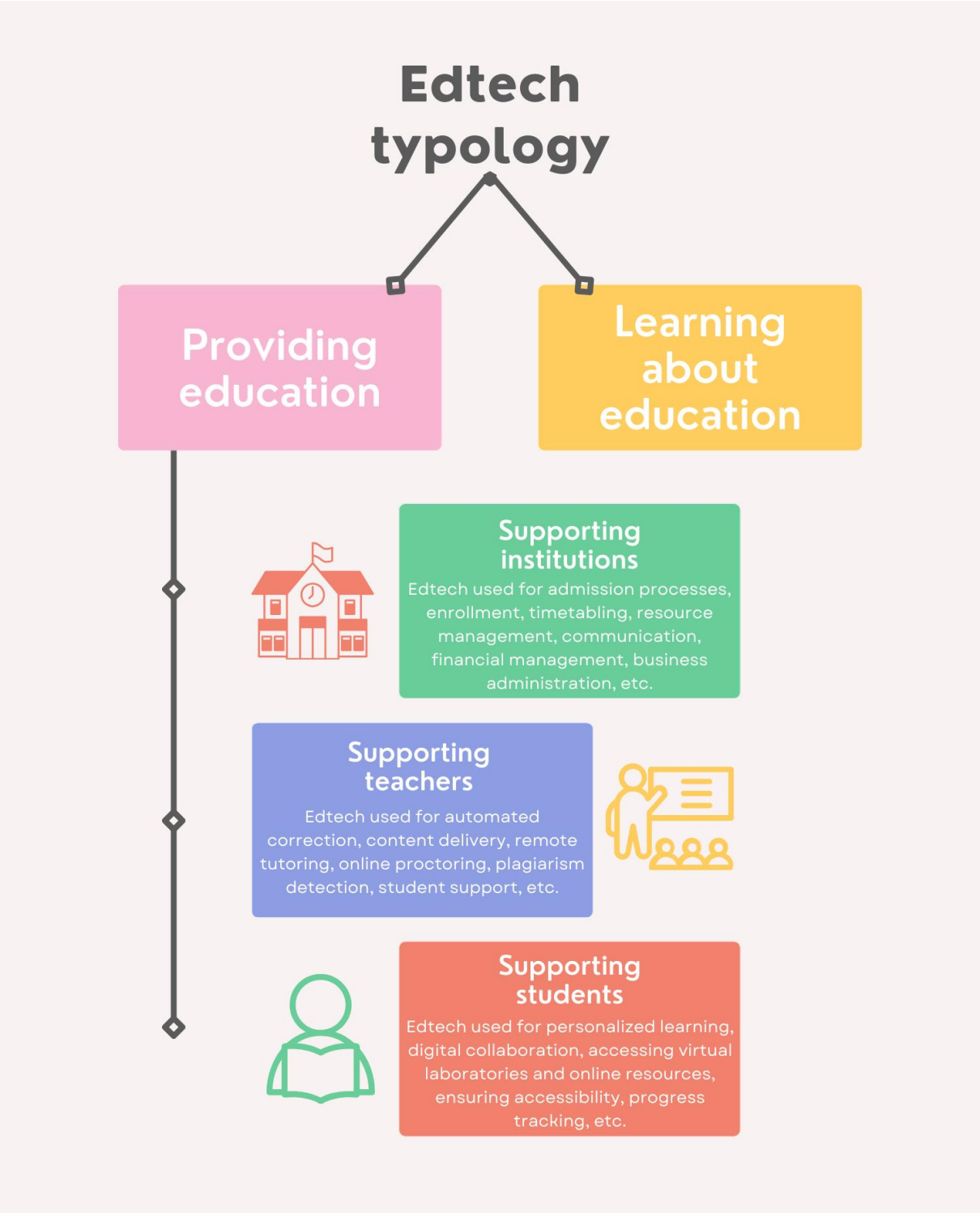
115. Defining AI is a very challenging task and there is no single definition that is universally accepted. For the purposes of this thesis, I will apply the definition provided by UNICEF. According to UNICEF (2021, p. 16), AI are

> machine-based systems that can, given a set of human-defined objectives, make predictions, recommendations, or decisions that influence real or virtual environments. AI systems interact with us and act on our environment, either directly or indirectly. Often, they appear to operate autonomously, and can adapt their behavior by learning about the context.

116. This is a very interesting and functional definition. It incorporates various types of AI, and has a critical view of the role that humans play in their development and utilization (they depend on "human-defined objectives" and only "appear to operate autonomously"). However, this definition also has its drawbacks. One example is the application of the notion of learning to AI systems, which could be understood as something inherently human, dependent on agency and consciousness (Holmes *et al.*, 2022, p. 16). What machine learning algorithms actually do is essentially recognize patterns in the wealth of data they are fed with (Solove, 2024).

117. Based on these initial definitions, the typology can be presented. It is important to note, however, that the boundaries between each category are not always clear and the same technology can be used for different purposes and in different contexts. Especially when they are supposed to be a central hub or LMS, they will also often provide many options and possibilities to schools, educators and students, enabling it to feature in more than one category. The function of the typology is, therefore, to assist us in navigating this complex environment with a significant amount of available technology. Figure 1 provides a visualization of the typology.

Figure 1 - Edtech typology



118. The primary distinction that should be made is between the use of edtech for *providing education* and for *learning about education*. When it comes to *providing education*, technologies can be used, first, to support educational institutions. This includes supporting admission processes, managing student's and school's data, timetabling, managing resources

management, as well as facilitating communication among the school staff, students and parents/legal guardians. This encompasses processing data such as enrolment, attendance, grades, schedules, academic records, contact details, social media, human resources, business data and finances. Schools often use one or more platforms to help them manage these data. If understood more broadly, this category could also include parallel activities that use technology to support the institution. An example would be school security—whether physical or online—by applying video cameras (including the ones powered with facial recognition), iris detector, metal detector, turnstiles, etc.

119. Second, technology plays a crucial role in supporting teaching and learning. This includes a wide range of tools such as LMS, document creation applications, e-textbooks, online tutoring, e-proctoring systems, educational games, chatbots, and automated writing evaluation systems. These technologies can be more focused on students themselves, by automating teacher functions and promoting independent learning. They include personalized learning technologies, virtual laboratories, online resources, progress tracking tools, educational games, and chatbots. On the other hand, they can be designed to directly assist teachers by streamlining and automating tasks, such as automated correction, content delivery, remote tutoring, online proctoring, plagiarism detection, student support etc.

120. Most AI research in education has been developed with a focus on supporting students, often by taking over teacher-related tasks. In contrast, limited research has been conducted on AI systems designed explicitly to aid teachers instead of replacing them. Frequently, designers think of teachers only at the end of the process by adding, for example, a dashboard to the application (Miao *et al.*, 2021). However, the examples above highlight the flexible boundary between technologies that focus on students and the ones that focus on teachers (Holmes; Bialik; Fadel, 2019, p. 21).

121. Edtech could also be used for *learning about education*, commonly known as learning analytics or educational data mining within the AI field. This meta level encompasses collecting, analyzing, and interpreting data from edtech to understand and optimize learning and learning environments. In other words, the data collected during interactions between students, educators and the edtech platform is not only restricted to the initial purposes of the application but serves as a basis for uncovering patterns of how the learning process takes place. This generates new data that can be, eventually, fed back into the system to improve the algorithm or used for other purposes. This will be better detailed in the last part of the thesis.

122. Before moving to the second chapter, I would like to highlight that the above typology is just one way to cluster educational technologies and can certainly be complemented by other ones focusing on different aspects. It was based on who/what the technology supports, as well as their purposes, but it is also possible to group edtech based on the means through which it is presented to these stakeholders, for instance. The table below shows, within the global market share of edtech, examples of different ways edtech presents itself to the public, either as hardware, software or a service.

Table 1 - Examples of EdTech "products", with % Global Market share (2019)

EdTech Hardware (9%)	**EdTech Software (49%)**	**EdTech Services (42%)**
Classroom Technology and Institutional Devices, including VR, XR, head-sets and other simulation devices.	Marketplaces, Peer to Peer Learning, Coaching and Mentoring Networks, Apps, Cloud-based management systems and tools.	All online forms of Primary and secondary education, higher education, tutoring and test preparation, online program managers and Bootcamps, as well as digital internships, apprenticeships and mentoring.

Source : Adapted from Vicentini *et al.* (2022, p. 16)

Interim conclusion

123. When tracing the historical evolution of edtech, we can perceive how diverse and rich its different applications are. We must look at this past not merely as steps leading us to the use of computers and AI in education, but as decisions made by humans that provide insights into how we can understand and regulate current technologies. Many of these technologies were not designed with education or children in mind, which can pose extra challenges to children's rights.

124. As we will see in the upcoming chapters, the education measurement movement, along with behaviorism, which played significant roles throughout the 20th century and shaped the development of early teaching machines, continue to influence current edtech. Therefore, reflecting on the past and the technologies that preceded those we use today also helps us understand enduring patterns and learn from previous experiences.

125. Setting the stage for the legal analysis, I have also introduced a typology of edtech that guides us through the complexity and great amount of edtech currently available to educators.

As in any categorization of complex phenomena of reality, the boundaries between the categories are blurred. Nevertheless, it can still be workable and helpful in identifying and systematizing the impacts that technologies have on the privacy and data protection of children. This typology will be used in the final part of the thesis when risks related to edtech to these rights will be mapped.

Chapter 2. Exploring the interplay between edtech and longstanding discussions in education

126. The proliferation of edtech, especially the introduction of digital ICT in education, has sparked a dynamic interaction between educational developments and the imperatives and constraints introduced by technology. On the one hand, edtech is imbued with specific design features that either enhance or limit certain actions and pedagogical methodologies. On the other hand, they were not introduced in a vacuum nor applied to blank slates, as education was already undergoing significant changes that benefit or face challenges in adapting to technology. As previously discussed, education is an inherently political and contested domain that encompasses various strands of theory and practice, each interacting with technology in unique ways.

127. This chapter will thus seek to present some of the main issues that arise from this mtual influence. This includes enduring questions such as the role of private actors in education, the demand for "efficiency," and the learnification of education phenomenon, as well as more contemporary issues, such as the concept of platform learning. Each of them represents a crucial dimension shaping the present and future trajectory of education, raising significant issues about its nature, its role in society and how technology interferes with it. This chapter is important for gaining a broader and more holistic understanding of the risks that technologies can pose to children's privacy and data protection. Some of the trends analyzed here may either curb or encourage certain technological features, affecting these rights to varying degrees.

2.1 Public and private values in education

128. Public institutions are foundations of western societies and some sectors, such as education, are considered public or common goods (UNESCO, 2015), essential for the maintenance of the rule of law, democracy, and human rights. Education is crucial to equip individuals to make informed decisions within a community, enable civic participation; foster tolerance and diversity, as well as promote social and economic development.

129. Public education can actually be considered as a matter of international human rights law. The structure of the rights within the CRC and the International Covenant on Economic, Social and Cultural Rights (ICESCR) is such that they first lay down the right to education (as well as the general principles that should be sought in order to fulfil it), only then to recognize

a right for individuals to establish and attend schools other than public ones. The scheme and the wording of these provisions would prioritize education provided by states as the "norm" (Mowbray, 2021).

130. We can also argue that public education is the best form of democratic education. Heimans *et al.* (2022, p. 71) is of the view that "what is 'public' about public education emerges from when democracy is put into practice *in* education". Democracy here is focused not only on the system's features (such as voting, political representation etc.), but on democratic acts or moments. When people engage in these acts and moments and become part of them, especially those who were previously excluded from the sense-making process, it can be said that education "becomes public" (Heimans; Singh; Kwok, 2022). According to the authors, this kind of education would be at odds with efforts of standardization and the perception of education as a product that could be exchanged in the market.

131. However, with the globally growth of neoliberal policies in the 1980s, the public sector started to be depicted as unproductive in comparison with the private sector, leading to the worldwide implementation of policies limiting public expenditure. This phenomenon has fostered the *marketization* of education, i.e., the "creation of a series of policy logics that aim to create quasi-markets in education" (Hogan; Thompson, 2021, p. 3). This was especially reinforced by the education sector strategies encouraged by the World Bank in developing countries (Singh, 2015a).

132. This means that private actors are increasingly involved in a service that was once mainly provided by the state. While the relationship between public and private entities in education has always existed (consider, for instance, the commercialization of textbooks), this has intensified (Hogan; Thompson, 2021), resulting in an environment characterized by "power-sharing, negotiation and competition, where decisions are made through a complex web of network interactions" (Castells, 2010, as cited in Hogan; Thompson, 2021, p. 3). It also implies that the service is more focused on individual needs, rather than on the common good, potentially fostering discrimination, and hampering equality of opportunities and social justice (Singh, 2015a).

133. The marketization of education can be realized in two forms: privatization and commercialization.

> Privatization is the development of quasi-markets through institutional and policy structures that privilege parental choice, school autonomy and venture philanthropy, often with the state regulating for public accountability. It happens *to* schools. [… On the other hand], [c]ommercialization is the creation, marketing and sale of education

> goods and services for commercial gain. It happens *in* schools. […] While privatization is about the logics of who conducts education, commercialization is about how actors profit from the "commodification" of education (Hogan; Thompson, 2021, p. 3, emphasis in the original).

134. The school influenced by neoliberal policies is then related to understanding education as an essentially private good, whose value is, above all, economic. According to this narrative, education should not necessarily be provided by society, or the government, but should be mainly the product of the investment of individuals. The notion of the full autonomy of individuals with no strings attached, except those they themselves recognize by their own will, corresponds to institutions focused on serving particular interests, transforming citizens into clients (Laval, 2019, p. 17).

135. The reduced involvement of the government, the marketization phenomenon, and the responsibilisation of individuals through economics compel people to make risky choices about every aspect of their lives, including education. Peters (2005, p. 131) explains that "'[c]hoice' assumes a much wider role under neoliberalism: it is not simply 'consumer sovereignty' but rather a moralization and responsibilisation, a regulated transfer of choice-making responsibility from the state to the individual in the social market". If individuals are to bear the responsibility and possibly the costs of education, that also means that providing several market options would be the best strategy to improve competition and diversification in the service provided (Lubienski, 2021, p. 22).

136. This not only places the burden on individuals, who do not necessarily have all the information and bargaining power to make a decision suited to their best interests, but is also corrosive to democracy. A "consumer-based public sector is limited in its ability to address the perverse effects of choices and to build stable and reliable institutions" (Needham, 2003, as cited in Peters, 2005, p. 135–136). If, on the other hand, the provision of education is focused on its collective benefits, then the emphasis should be on "issues of access and adequacy, equity of outcomes and guaranteeing that all students have quality schools—issues often better addressed by public governance or direct state provision" (Lubienski, 2021, p. 22).

137. The dynamics of the private sector are introduced in the public sector primarily under the efficiency argument, which will be further elucidated in Section 2.3. This is brought about by reducing public investment in education: more needs to be done with a smaller budget, and management techniques that have already been put to the test in the private sector start to be incorporated (Laval, 2019, p. 193). When it comes to edtech, the role that private actors have on taking important decisions in education also increases, ranging from determining (part of)

the content that is learned, to defining pedagogical strategies and interpretating a child's educational development (Knox, 2020).

138. Edtech wields immense influence over contemporary childhood education, shaping what can and cannot exist, setting priorities, and fundamentally defining its nature based on the investors backing edtech companies. Edtech made education *investable*, which means that more than financial decisions, investors make political decisions that affect the whole society (Komljenovic *et al.*, 2023). As one edtech investor puts it, the most difficult part in investing in innovation is "[w]hich new ideas will work? Which new ideas will be purchased—at what unit price and what gross margin? Which new ideas will scale and deliver consistent and increasing revenue, ROI [Return of Investment] and profitability? […]" (Palmer, 2022, n.p.).

2.1.1 The role of philanthropy in education

139. The role of philanthropy also contributes to the privatization and commercialization phenomena. This is of course not a new event, but "the new generation of impact or 'venture philanthropy' often treats giving as an investment that needs to be strategically managed for maximum effectiveness and return" (Saltman, 2010, as cited in Lubienski, 2021, p. 23).

140. Important examples include the Gates Foundation, Dell Foundation and Chan-Zuckerberg Initiative, all of them related to technology companies. Although they are very much relevant in the USA, they already have a lot of influence in the whole world. These institutions embrace varied agendas, but they converge in transforming schools through top-down market models and business approaches, funding institutions and individuals, and defending advocacy strategies in public policy (Lubienski, 2021, p. 24).

141. The emphasis on individual purposes present in philanthropist agendas has severe implications for the governance of education, as the methodologies and remedies used to tackle educational problems will be defined by their interests. After analyzing the "social divisions" [9] within some big tech companies, Magalhães and Couldry (2021) argue that these companies understand social good as being datafied, probabilistic and profitable.

142. By datafied, the authors mean that "social good is generally taken as proportional to and made comprehensible by the quantity, type, and granularity of the data that can be gathered"

[9] By this, the authors mean "more or less organized sectors within Google, Facebook, Amazon, Microsoft, and IBM that define themselves as geared toward helping (typically, vulnerable) people, not profit" (Magalhães; Couldry, 2021, p. 347).

(Magalhães; Couldry, 2021, p. 349). The lack of data is generally seen as a barrier that impedes social good to be realized and the investment and tools provided by big tech as the solution. This is also related to the fact that data about humanity in general is increasingly held in private hands.

143. The datafication of social good leads to the idea of probabilistic good, as the attempt to make sense of data is related to a language of probability. The problem with this approach is that "the association between (probably) doing good and (necessarily) allowing some harm to happen flows automatically from the probabilistic notion of algorithmic knowledge on which proponents of datafied social good choose to rely, as their model for producing social knowledge" (Magalhães; Couldry, 2021, p. 352).

144. Finally, the projects conducted by these social divisions seem to be inseparable from profit generation, as datafication can hardly be separated from commodification (Dijck; Poell; Waal, 2018, p. 121). This happens not only because of their role in big tech's marketing strategies, but also because they are entangled with their commercial products (Magalhães; Couldry, 2021). As will be further discussed in Part III of this thesis, Google Workspace for Education serves as a prime example of this model. Although mostly offered at no cost, it concurrently collects vast amounts of data from students, which may potentially be leveraged for commercial purposes.

145. This kind of philanthropy is often driven by the idea of disrupting sectors, such as education, but it also "tends not to act in ways that are counter to the interests of the wealthy, nor to 'disrupt' the systems or exploitative practices that produced the vast fortunes that these philanthropists now leverage" (Lubienski, 2021, p. 30). It also raises the question of the origin of the money employed by these organizations, as they are often linked to predatory business practices (Lubienski, 2021).

146. The digital transformation in public sectors such as education (partially) funded by the private sector is often seen as very attractive and benign (Alston, 2019, p. 4). However, beyond the challenge of estimating the effects of this influence on education[10], if imbued with strong individualistic and private values, it can also be viewed as a "Trojan Horse for neoliberal hostility towards welfare and regulation", as described by the former UN Special Rapporteur on extreme poverty and human rights, Philip Alston (2019, p. 12). This has a significant impact

[10] See, for example, Strauss (2013) and Hess (2020).

on countries that do not have large-scale data actors, robust systems for data processing, and have limited connectivity infrastructure (Magalhães; Couldry, 2021, p. 346).

2.2 The "learnification" of education

147. According to Biesta (2010), the last decades have seen the intensification of a phenomenon called the *learnification* of education. This means that the discourse around education has been translated into a discourse of learning, i.e., a narrative that focuses solely on the knowledge and skills that should be acquired by individuals. Teaching is seen as an activity that supports or facilitates learning (Biesta, 2016a, p. 15).

148. This results from a confluence of events rather than the intended outcome of a particular agenda. The author highlights four main trends contributing to it: a) emerging theories of learning, especially constructivist and sociocultural theories, which challenge the idea that learning is a passive exercise and advocate for the active construction of knowledge by learners; b) postmodernism, which understands education as a project of modernity, intimately connected with the Enlightenment. It casts doubt on the idea that education can emancipate students through rationality and critical thinking; c) the silent explosion of adult learning, and the fact that people spend increasingly amounts of time and resources on learning both withing and outside established educational institutions; and d) the erosion of the Welfare State; While neoliberalism's market-oriented ideology has not entirely supplanted the principles of the Welfare State, such as universal education, the dynamics of citizen-government relations have shifted. Instead of a political relationship, it is increasingly an economic relationship, where the state is seen as a provider of public services and the taxpayer as a consumer (Biesta, 2016a, p. 17–19)**.**

149. The main issue related to this language is that it, deliberately or not, promotes the idea of education as an economic transaction, where the learner has needs that the educator should fulfil. Ultimately, education becomes a "thing", a commodity that can be consumed by the learner (Biesta, 2016a, p. 19–20), which is related to the issue of private actors in education as discussed above.

> This is the logic that lies behind the idea that educational institutions and individual educators should be flexible, that they should respond to the needs of the learners, that they should give their learners value for money, and perhaps even that they should operate on the principle that the learner/customer is always right (Biesta, 2016a, p. 20).

150. It assumes that children and their parents or legal guardians know exactly and in detail what they want from school. This assumption fails to consider that one of the primary objectives of pursuing education is to determine one's actual needs, and this process heavily relies on the involvement of educational professionals with the necessary expertise (Biesta, 2005, p. 59). That is exactly the difference between a market model and a professional model, which lies in the latter's emphasis on producers not just servicing a need, but also helping define it (Feinberg, 2001, p. 403, as cited in Biesta, 2005, p. 59).

151. The learnification phenomenon is also aligned with understanding education as the provision of human capital for the economy (Holmes *et al.*, 2022, p. 27). This human capital should be qualified and skilled and, therefore, the focus of education should be on the content that children are receiving.

152. It is important to highlight that this new language is not problematic *per se* and can even empower individuals to take control of their educational agendas. It could also help redress imbalances created by inflexible and provider-led situations, excluding many from educational opportunities (Biesta, 2016a). However, the language we use to describe the world directly influences reality and set the boundaries of what is possible to be said, to know, to be thought and, ultimately, to be done (Biesta, 2005, p. 54).

153. Framing education as purely learning reduces its scope and reach. It focuses only on the qualification aspect of education (related to acquiring knowledge, skills, values etc.), and sidelines the aspects of socialization ("the ways in which, through education, we become part of existing traditions and ways of doing and being") and of subjectification (related to the subjectivity or "subject-ness" of the educated, raising questions related to emancipation and freedom) (Biesta, 2016b, p. 4). The "learnification model is predicated on the real-time, short-term process of learning, while education involves a simultaneous nourishing of intellectual, social, technical, and cognitive skills and involves a longer trajectory over a period of years" (Dijck; Poell; Waal, 2018, p. 124).

154. If the problems stem from inequality and limited access to education, the priority should be addressing the root cause, rather than confining education solely to learning outcomes. We should be focusing on making education, broadly understood, more human and democratic, ensuring that all individuals, including children, actively participate in decisions that impact them. Moreover, education should not only be seen as an individual path or preference, but also as a way for students to become citizens and active political actors.

2.3 Learning, calculation and efficiency

155. The narrow focus on learning, as explained above, is open-ended in relation to the objectives of education. Judgements in education should, however, not only be related to what is possible (factual judgement), but also what is desirable (value judgement) (Biesta, 2010, p. 37). Learnification deflates a collective and democratic discussion about the reasons and ends of education beyond individual preferences, diverting attention to procedural aspects. Consequently, questions tend to gravitate towards technicalities and efficiency.

156. A framework that is only focused on the means is never neutral. The efficiency of teaching in the way it develops in neoliberalism tends to be confused with economic efficiency, which consists of maximizing countable results (Laval, 2019, p. 213). The idea of effective intervention (a causal model between the intervention and the results), that was first developed in medicine, comes from a particular understanding of professional practice that is not necessarily well translated to education (Biesta, 2010).

157. Education, however, is not a physical interaction, but rather a symbolic or symbolically mediated interaction. “If teaching is to have any effect on learning, it is because of the fact that students interpret and try to make sense of what they are being taught. It is only through processes of (mutual) interpretation that education is possible” (Biesta, 2010, p. 34). What teachers do (and here it is also possible to include any other input that the student receive) should be than seen not as the cause of learning, but as an chances “for students to respond and, through their response, to learn something from these opportunities” (Biesta, 2010, p. 35).

158. The demand for efficiency is intrinsically related to the measurement of education and, consequently, to datafication (Barassi, 2020, p. 72). The rise of the measurement culture in education dates from the 20th century, when large-scale assessments that trace performance and growth even across borders started being applied to drive evidence-based decision-making (Pangrazio *et al.*, 2022, p. 259–260). In 1904, one of the main proponents of the idea of measuring education was the American psychologist Thorndike, who believed that units of measurement should be devised, tested and standardized in education so the latter could yield the true benefits of quantitative science (Lawn, 2013, p. 110).

159. This process was extremely important so decisions in the educational realm started to be informed by factual data, rather than by mere opinions of what education should be. However, the excitement with the abundance of information has also resulted in an exacerbated

reliance on factual data (Laet *et al.*, 2018). Measuring not only refers to a new way of describing education, but a new definition of education and the relations within it (Lawn, 2013, p. 110). With the measuring movement, not only students are analyzed; schools are also assessed in order to check whether they meet national goals and have their data scores ranked against each other (Barassi, 2020, p. 74). Children become proxies for school performance, while schools become data centers (Williamson, as cited in Barassi, 2020, p. 75)**.**

160. Computing language helps compartmentalizing and calculating learning and achievements. It reframes and explains educational dynamics, proposing that education can be programed, executed and standardized. More than that, it starts to delineate what counts as knowledge or not.

> [P]eople begin to think that socio-cultural processes could be engineered, streamlined and automated (i.e. orchestrated) to enhance performance and efficiency. In some cases this becomes more than a simple belief, as it begins to constrain practices by imposing a technocratic ideal of how education should be run (Perrotta; Evans, 2013, p. 522).

161. Quantitative data concerning educational outcomes is undeniably useful. However, a genuinely scientific spirit should question the limits of these assessments, the uses that can be made of them and the practical consequences they can have, especially in the pedagogical field (Laval, 2019, p. 214). More than questioning if one is measuring what they want to measure, the problem lies in the normative validity of the measurement. That is related to the question

> whether we are indeed measuring what we value, or whether we are just measuring what we can easily measure and thus end up valuing what we (can) measure. The rise of a culture of performativity in education—a culture in which means become ends in themselves so that targets and indicators of quality become mistaken for quality itself—has been one of the main drivers of an approach to measurement in which normative validity is being replaced by technical validity (Biesta, 2010, p. 13).

162. This is related to what Laval (2019, p. 16) calls the cult of "innovation" for the sake of "innovation", which is dissociated from clear political implications. The discussions about edtech should then be focused not on the technology itself, but on the educational challenges we as a society would like to tackle, such as equity and inclusion, as well as education's quality (UNESCO, 2023b, p. 7). Efficiency and the tools we choose to use are also a very important part of the discussion, but they should be focused on *supporting* the achievement of these broader goals.

2.4 Platform learning

163. The way the digital economy is currently constructed heavily relies on platforms and they are one of the main data infrastructures present in schools. Platforms are a "programmable digital architecture designed to organize interactions between users [… and are] geared toward the systematic collection, algorithmic processing, circulation, and monetization of user data" (Dijck; Poell; Waal, 2018, p. 4). They are increasingly the way through which education takes place in the digital environment, especially from 2010 onwards (Rivas, 2021).

164. It is important to remember that a platform is always a means to something else. While platforms are often assessed based on their functionality, such as the delivery of goods and services, it is crucial to examine the manner in which they operate, specifically how they facilitate interactions between users, service providers, and other technical systems (Nichols; Garcia, 2022, p. 213).

165. Van Dijck (2013) understands platforms as a metaphorical construct with technological, social, economic and political dimensions. These dimensions coexist and influence one another, meaning that all of them should be assessed when deciding if and which platform will be used within an educational setting. Platforms should also not be understood as static tools, but as having a living and dynamic nature, which the author compares to a tree. They are constantly evolving and shaping their environment and they are part of a larger global connective network (Dijck, 2021, p. 2805).

166. Whitin the school environment, platforms significantly shape students' and teachers' social experiences, as well as how data are processed within its architecture. They differ from previous software solutions in that they not only provide services to their users, but also collect data from these interactions, which their owners can sell or use for product development (Nichols; Garcia, 2022, p. 210). The interfaces users interact with change in real time based on these data and it learns from users' behavior, which makes them unique to each user (Susser; Roessler; Nissenbaum, 2019, p. 7). In this sense, while education datafication provides platforms with the data for analytics, platforms are essential for collecting, structuring and representing them (Pangrazio; Selwyin; Cumbo, 2022, p. 2).

167. As an entry point for making sense of data, platforms "help concretize otherwise abstract data processes by locating them in particular socio-technical and political-economic relations" (Pangrazio *et al.*, 2022, p. 261). Being rooted in the *learnification* narrative, they are "imagined

as a customizable on-demand service as learners interact with platforms like users interact with Netflix, Facebook, Amazon, and iTunes" (Means, 2018, p. 329). In fact, to become "the Netflix of Education" was exactly Pearson's (a British multinational publishing and education company) goal (High, 2018).

168. When this model is applied to education, it "reflects a belief in learning as a prescriptive process, rooted in efficiency and calculation, and powered by artificial intelligence, mobile apps, cloud services, and data processing" (Means, 2018, p. 329). Thus, they are the perfect way to implement the efficiency and evaluation culture described in the previous subsections and their design is often shaped to transform social interactions into data and quantifiable knowledge.

169. It is important to consider that over time, humans often become accustomed to using technology, focusing primarily on the tasks it facilitates rather than on the technological means itself. Consequently, because technological tools can fade into the background, their influence might go unnoticed, potentially allowing for hidden and manipulative practices to persist (Susser; Roessler; Nissenbaum, 2019, p. 7). Therefore, learning powered by platforms can uproot or bypass the core values of publicly funded education, such as a knowledge-based curriculum, teacher autonomy, affordability, and education as a means for socioeconomic equality (Dijck; Poell; Waal, 2018, p. 118).

170. The main platform usually used within the school is the LMS, and it is part of the broader data infrastructure, which also includes human and material infrastructure such as cables, routers and servers (Pangrazio; Selwyin; Cumbo, 2022, p. 4). LMS are designed to provide a centralized platform for managing and delivering educational content, activities, and assessments. They usually support a wide variety of teaching and learning modalities and integrate with other more specific applications. This implies that the possible activities that can be carried out within a LMS are diverse, encompassing content management, communication, discussion forums, online quizzes, and assignment submission. This also means that they can serve as central hubs for data collection. This underscores the significance of examining Google Workspace for Education as an LMS in Part III, as it provides interesting insights into the challenges related to children's rights to privacy and to the protection of personal data while using edtech.

Interim conclusion

171. This chapter aimed at unraveling the complexities arising from the intersection of long-standing questions within education and the influence of edtech, with their inherent promises and limitations. I have argued that public education is the best way not only to implement, but also to promote democracy in our society, as well as to nurture critical and informed citizens. When education is treated as a private good and citizens are cast merely as consumers, the focus narrows down to individualized needs, overshadowing its broader societal role and neglecting other collective values. I have also discussed how neoliberal educational policies are one of the reasons behind the phenomenon of "learnification" of education, prioritizing individual knowledge and skill acquisition. While this shift can empower individuals in their educational agendas, it risks minimizing the significance of education, overlooking crucial aspects of socialization and personal development.

172. Understanding education solely as learning also seems appealing as it reduces its qualitative aspects. The more quantifiable education is, the easier it is to measure it and, therefore, focus on efficiency. The growing emphasis on efficiency tends to prioritize its economic aspect over the symbolic interactions fundamental to the educational process. Despite this measurement culture having roots in the early 20th century, the advent of data-driven digital ICT has intensified this trend through datafication.

173. The use of edtech interacts with these trends by facilitating the involvement of private actors in education, given the increasing use of technology in the field, and by enabling interaction among students, educators, and companies within platforms. The implementation of platforms aligns with the trend of the learnification of education and the measurement movement, which remains strongly present today. They facilitate user interactions and data collection, having progressively become the primary mode of education delivery. They are more than mere functional tools; their dynamic nature shapes social, economic, and political dimensions and reflect an efficiency-driven, data-centric narrative, akin to consumer platforms like Netflix. This model risks undermining core educational values and reinforcing inequalities.

174. In light of these developments, technology should be seen as a valuable tool in education, with the potential of enhancing learning and even other aspects of education such as socialization and subjectification. However, the focus should not be on innovation for its own sake but rather on leveraging technology as part of a comprehensive strategy aimed at achieving educational goals like equity, inclusion, educational quality, and children's best interests.

Chapter 3. Data Colonialism as a theoretical and normative framework

175. Within legal scholarship, research frequently entails a summary of the current state of positive law, combining reference to legal sources, such as legislation and cases, with the analytical doctrine. However, less frequently identified is the explanation of how researchers, through this review of the current state of the art, reach conclusions and normative claims (Taekema, 2018). A theoretical framework becomes essential to shed light on the lens that the researcher adopts to see the social reality. It not only enhances transparency but also aids the reader in understanding the reasoning that leads the researcher to their conclusions, making research reproducible.

176. Considering that the majority of legal research is not only descriptive or explanatory but also normative, the theory also needs to serve as a normative framework. It provides the link to prior research and the foundation for an evaluation of the current affairs and/or proposing a solution (Taekema, 2018).

177. Therefore, as a theoretical and normative framework, this research adopts data colonialism, as described by Couldry and Mejias (2019). This normative framework will help evaluate the current state of positive law to answer the research question in the last part of this thesis. This chapter unpacks this framework and complements it with a broader literature on datafication and data colonialism that can help clarify some of the concepts developed in the book. Apart from explaining what data colonialism is, its main components, and the actors involved, I will also focus on how it disproportionally affects some people and communities, as well as how it is rooted in very specific business models. Finally, I will discuss the implications of data colonialism on human autonomy.

3.1 The concept of data colonialism

178. The concept of data colonialism, as developed by Couldry and Mejias (2019, p. xiii, xix), refers to an emerging order of appropriation of human life through data. The authors do not use the term colonialism as a metaphor, but as a concept that encompasses significant evolutionary stages throughout human history, with a particular focus on the context of capitalism. It does not mean, though, that there is a one-to-one correspondence between what is happening within data colonialism and the highly violent activities of historical colonialism.

179. This is because colonialism's core is not understood as a particular method since they can be complex and varied (including not only physical violence but also symbolic forms of violence through legal, social and technological constructs). It is actually understood as a universalist view of the world's economic and cognitive resources (Couldry; Mejias, 2023, p. 794). While historical colonialism was focused mainly on natural resources and human labor, data colonialism adds a layer of human relations captured through data.

180. The data colonialism theory refers to the exploitation of human life and social relationships by a few entities through datafication and data commodification. It stresses that data do not naturally exist by themselves as if they were a natural resource. People do not "leave behind" digital traces or footprints as they wander around the digital realm; rather it is technology that facilitates the collection of these data. Data are always the outcome of an abstraction process, which transforms the whole of social life and meaning into something that can be counted. If it cannot be measured and counted, it does not exist (Mejias; Couldry, 2019, p. 3–4). It thus implies selection and transformation of reality which can be said to be a biased way to interpret and represent the world.

181. The datafication of human relations leads to the progressive reconfiguration of larger parts of the social domain, in ways that position technology companies as privileged providers not only of social solutions, but also of social knowledge (Magalhães; Couldry, 2021, p. 354). This is possible due to *data relations*, which is a new type of social form. They ensure that the collection of personal data and their storage give rise to a new type of knowledge about the social world: the so-called *social caching* (Couldry; Mejias, 2019, p. xiii). In many cases, this is a relation that has to be built to implement the data flow since data extractability only exists because it is socially constructed (Couldry; Mejias, 2019, p. 27).

182. Important for this thesis is the fact that targeting vulnerable social groups is considered by the authors to be an important part of data colonialism (Couldry and Mejias, 2019, p. 67–68, 148–149). Although every person's data would contribute as an input to data colonialism, some people at the margins of the social and economic order would pay a higher price. This includes not only people within the Global South, for example, but also children and other vulnerable data subjects even within the Global North.

3.2 Main components of data colonialism

183. In order to better understand the idea of data colonialism, the authors propose four main components that can be identified in both data colonialism and historical colonialism (and for that very reason, it is possible to recognize the historical continuity between one and the other). It is important to note, however, that the world has undergone fundamental changes over the past centuries, which provided data colonialism with some particularities. Without globalization, financialization, the acceleration of capital flows, as well as the huge development of communication infrastructures, the current way of processing data would not be possible (Couldry & Mejias, 2019, pp. xii, xix).

184. This highlights the relationship between the development of industrial capitalism and data colonialism. Couldry and Mejias (2019, p. xix) argue that the latter is driven by the imperatives of the first, which includes the logic of accumulation, profit maximization, competition, labor productivity through the technological elaboration of production, as well as growth through the reinvestment of surplus (Zuboff, 2019).

185. On the other hand, "capitalism itself emerged on the basis of colonialism's detailed histories, in particular the European colonial power's vast aggregation of global resources that fueled industrial capitalism"[11] (Couldry; Mejias, 2023, p. 787). Data colonialism is then the link that emphasizes how the relations between colonialism and capitalism are contemporary and evolving. This correlation is exacerbated by the current convergence of economic power (generating value) and cognitive power (generating knowledge) since data colonialism is appropriating the very resources for knowing the world (Couldry & Mejias, 2019, xii).

186. The first component is the *appropriation of resources*. Whereas historical colonialism was embedded in the *terra nullius* legal doctrine (the idea that some lands belonged to no one), in data colonialism, data are assumed to be there for the taking as a freely available resource (Cohen, 2019, p. 48; Couldry; Mejias, 2019, p. 88). Datafication is key for the processes of

[11] Neocolonial legacy still shapes capitalism's development, as can be exemplified by Facebook's Free Basics program (Facebook, [*s. d.*]). Cohen (Cohen, 2019, p. 59) describes the patterns in exploration and colonization of the public domain in two steps: "initial extensions of surveillance via a two-pronged strategy of policing and development, followed by a step back as the data harvests are consolidated and absorbed". However, more than facilitated by historical colonialism's current influence on societal and economic relations, extracting value through data would be a new form of resource appropriation, starting a "new stage of colonialism that lays the foundations for new developments in capitalism" (Couldry; Mejias, 2023, p. 788). Understanding this new form of life appropriation for profit only under capitalism, as does Zuboff (2019), for example, misses the point of the "Big Data rhetoric which insist [sic] that only through maximal collection and concentration of data can the world be developed, understood, governed, and saved" (Couldry; Mejias, 2023, p. 796).

commodification and privatization of data, which means that data (and, more specifically, big data) are being produced not only with its use in mind but also with the explicit purpose of market exchange (Couldry; Mejias, 2019; Thatcher *et al.*, 2016).

187. The second component is the *unequal social and economic relations* that secure resource appropriation. The historical colonialism framework included moral or legal norms that would allow forced labor, for example. Within data colonialism, what the authors call "data relations" makes the appropriation of human beings' data seem normal and it is generally enforced by the technology design itself, as well as legal frameworks (Couldry; Mejias, 2019).

188. These data relations, especially between the colonizing agents and data subjects, are asymmetrical due to how obscure the transformation from individual data points to big data is (Thatcher; O'Sullivan; Mahmoudi, 2016). They provide corporations with a privileged overview of social relations, which is incredibly powerful. States are ever more dependent on this knowledge, reversing the longstanding flow of knowledge transfer (Couldry; Mejias, 2019, p. 13).

189. The third component is the massively *unequal global distribution of the benefits of resource appropriation*. While historical colonialism would concentrate wealth in colonizing nations, data colonialism favors the concentration of wealth in the hands of the colonizing agents (Couldry; Mejias, 2019).

190. As explained above, the control of data collection processes provides a special power to those who own the hardware and software that process them. As it stands, the "data economy" tends to be monopolistic, reinforcing other asymmetric balances of power (Cheng, 2020). This monopolization is not only restricted to services; being also present in the production of devices through which people connect to the infrastructures of data collection, in the computer capacity, production of content, and content delivery (Couldry; Mejias, 2019).

191. Finally, the fourth component is the spread of *ideologies that help make sense of the new order*. Within the historical colonialism framework, it was common to reframe "colonial appropriation as the release of 'natural' resources, the government of 'inferior' peoples, and the bringing of 'civilization' to the world" (Couldry & Mejias, 2019, p. 4).

192. Data colonialism, on the other hand, is embedded in several ideologies, such as, for example, the ideology of connection, which naturalizes the connection between people, objects and processes through computer-based infrastructures. "Connection is, of course, a basic human value, but the requirement to connect here and now—connect to this particular deeply unequal

infrastructure—means submission to very particular conditions and terms of power" (Couldry; Mejias, 2019, p. 16).

193. The authors also mention the ideology of datafication—which perceives that all aspects of human life can and should be transformed into data—and the ideology of personalization—which makes surveillance attractive. In a similar vein, Van Dijck (2014, p. 198) describes *dataism* as the "belief in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies".

194. Regardless of the various ways and levels of granularity in which these ideologies can be described, they have in common that they are all related to an overarching myth that

> technology, especially digital technology, is powerful, benign, and irresistible. There is no point whatsoever in opposing the Next Internet because the Cloud, Big Data, and the Internet of Things are too strong to overcome. Moreover, because it is a force for good, perhaps a major step along our evolutionary journey, it makes no sense to oppose them. The only reasonable choice is to yield to our digital future and embrace it enthusiastically (Mosco, 2017, p. 122).

195. This mainly occurs because of the asymmetrical extraction of value through datafication, which assumes that quantification and surveillance of all aspects of human life are natural and desired by all members of society (Thatcher; O'Sullivan; Mahmoudi, 2016, p. 991). This myth empowers technologies and can undermine human autonomy.

3.3 Colonizing agents

196. The network of actors participating in data colonialism is a complex one. The result of data colonialism, i.e., what the authors call the "cloud empire", is being implemented and extended primarily by the "social quantification sector", the industry sector devoted to the development of the infrastructure required for data collection (Couldry & Mejias, 2019, p. xiii).

197. The social quantification sector is composed not only of the most obvious players, such as the Big 5 (Amazon, Apple, Google, Facebook and Microsoft). It also includes smart appliances manufacturers, developers of digital environments, data brokers, financial companies, and data-driven platforms (such as Netflix, Spotify, Airbnb and Uber) (Couldry & Mejias, 2019, p. xiv).

198. Although not at the center of the data colonialism process, other businesses were also transformed to accommodate data colonialism into society's life. Ordinary businesses increasingly not only collect data for their internal purposes, often sharing them with other

actors, but also depend on the social quantification sector for services such as targeting advertisement and data storage (Couldry & Mejias, 2019, p. xv).

199. At the same time, the activities of the social quantification sector do not flourish without the active participation of states, which allows (or at least do not regulate) certain social relations. Knowing the social world in depth was previously just a prerogative of the State. Currently, it is the large technology companies that have this privilege, and states have become progressively dependent on them.

3.4 Data Commodification

200. One of the main conditions for the existence of data colonialism is understanding data as a commodity, i.e., something that can be traded in the market. Once collected and analyzed, data can be sold as a product or service in the digital economy. It does not mean that an ownership right is required. The data flow paradigm which reinforces commodification can be identified even when the legal framework recognizes *data access obligations* as an exception of *de facto* ownership (Ducuing, 2020).

201. The dominant conservative economics view of data is that it is a club good. Based on a way of classifying goods in neo-classical economics, this means that it is non-rival, i.e., its consumption by one individual would not prevent others from consuming it, as well as excludable, i.e., that its consumption could be prevented by organizational, technical or legal mechanisms (Purtova & Maanen, 2023).

202. The logic behind this classification is aimed ensuring that there is an adequate quantity and quality of data available in the market. Therefore, the focus shifts to data, itself as a resource and as an object of governance, to create incentives for their production and availability. However, if the purpose is to achieve other societal goals, even with the aid of data, like privacy, democracy, and sustainability, these goods are the ones that need to be conceptualized (Purtova & Maanen, 2023, pp. 21, 50).

203. An important problem with this approach, as described by Purtova and Maanen (2023), is its performative effect, as this view alters the very way humans interact with and value not only goods but also other people. The “market” becomes the standard against which these relationships and society as a whole are evaluated. This treatment of data as a commodity has

direct or indirect consequences, reinforcing harmful practices such as surveillance, creating problematic dependencies, and exploiting those involved in data production.

204. Moreover, adopting the neo-classical economic vocabulary may lead to market principles infiltrating non-market areas of life where exchange and commodification are not suitable, such as in family and community relationships (Purtova & Maanen, 2023, pp. 51–52). As the emphasis shifts towards collecting and producing increasingly more data, human life and social relations begin to be shaped to enable it. More broadly, understanding data as a commodity and the market as the standard for human relationships directly affects our individual and societal autonomy, ultimately calling into question our humanity and dignity.

3.5 Data colonialism and its incursion into autonomy

205. As explained above, this new data-mediated social configuration brings serious consequences for human autonomy. First, Couldry and Mejias (2019, p. 157) argue that autonomy is being harmed by the mere fact that data are being mandatorily collected as a requirement of daily life. Data colonialism not only potentially but in principle and by design affects the self's sphere of action because of its ubiquity. Every social relation is increasingly being datafied and embedded in data-driven technologies, which makes it very difficult for individuals to opt out, especially when it comes to essential services like education. And that is why one can speak of an increasingly extensive state of surveillance. Even if technologies are not being used for this immediate purpose (such as security cameras or behavior monitoring), individual and collective life is increasingly tracked in a disguised manner, thereby fostering a new layer of surveillance. This pervasive monitoring engenders a chilling effect, altering people's behavior as they are constantly observed.

206. Autonomy is also affected by the attempt to predict human behavior based on past behavior, which can restrict people's exposure to diverse perspectives, ideas, and opportunities, thereby limiting their possibility of exploring new and unanticipated paths. Data start to speak on people's behalf, which could also lead to violations of equity and non-discrimination.

207. Manipulation is also a very often outcome of commodification and DDBM, which implies that people's ability to make choices is compromised. Susser, Roessler and Nissembaum (2019, p. 4) argue that a critical aspect of manipulation is that it is a hidden practice. Manipulating someone would mean "intentionally and covertly influencing their decision-making by targeting and exploiting their decision-making vulnerabilities". This could

happen not only through deception but also by leveraging people's cognitive biases to influence the trajectory of decision-making (Susser; Roessler; Nissenbaum, 2019, p. 5). Through manipulation, autonomy is hampered in two main ways. First, it leads people to act towards ends they have not chosen. Second, their actions will be taken based on reasons that may not be their own.

208. People's digital profiles provide enough information for companies engaging in behavioral targeting to know precisely when to intervene to reach their goals most effectively. More than that, it enables the detection of specific vulnerabilities beyond the ones common to all human beings (such as related to unbounded rationality) (Susser; Roessler; Nissenbaum, 2019, p. 6)). Here, it is important to understand manipulation as a spectrum, as some practices can be more manipulative than others. In case of children, for example, the threshold for defining what is manipulative or not should be higher, as they are still developing their own discernment.

209. More generally, autonomy deeply impacts the educational experience, as it plays a pivotal role in fostering a dynamic and enriching learning environment, igniting students' intrinsic motivation and engagement. It fosters independence and self-confidence, empowering learners to take ownership of their educational goals and to take a broader part in society as a whole.

210. Given that autonomy is closely tied to safeguarding one's interests, it is logical to assume that eroding people's autonomy can lead to a reduction in pursuing them. As datafication continues to permeate every aspect of human life, there is a growing concern that we may progressively "unlearn" how to be autonomous (Couldry; Mejias, 2019, p. 173). In the case of children, they can grow up in a world where being autonomous is not even a possibility in the first place. Children are highly susceptible to manipulation (Giannini, 2023, p. 5) and these practices can affect the very development of children's autonomy and, consequently, how they value their own and other's privacy.

211. Finally, eroding autonomy also means eroding democracy and public institutions, as "it is only because we believe individuals can make meaningful independent decisions that we value institutions designed to register and reflect them" (Susser; Roessler; Nissenbaum, 2019, p. 11). Autonomy is at the core of liberal democratic societies, and it is only because individuals could potentially govern themselves that collective and democratic decisions can be made. The

incursion into democracy is deepened by the power asymmetry resulting from harvesting vast amounts of data and the fact that social knowledge is in the hands of only a few actors.

Interim conclusion

212. This chapter aimed to present the theory of data colonialism as a normative theory that will be used to evaluate the implications that current edtech have on children's rights to privacy and to the protection of personal data, as well as the extend to which the current legal framework deals with them. By appropriating human life and social relations and converting them into data, data colonialism can impact almost all of our actions and inner thoughts as they increasingly take place in the digital environment. This is not necessarily because we share them but because the infrastructure to collect observed and inferred data is becoming ever more ubiquitous and invasive, leading to an intricated, surveilled digital environment.

213. We have seen that historical colonialism and data colonialism share four key aspects: the appropriation of resources, unequal social and economic relations, unequal global distribution of the benefits of resource appropriation, and ideologies that help us make sense of the new order. Although discussed separately, these aspects are directly linked to one another. In order to appropriate data, the Cloud Empire needs to implement or make use of already existing unequal data relations. These relations are extremely asymmetrical due to (i) the opacity of the operations made with personal data, (ii) the overview of the social world that these companies have as a consequence, which is extremely powerful, and (iii) the fact that they are built on top of historical asymmetries, often as a product of historical colonialism. This exacerbates the global distribution of wealth and can only be justified by very specific narratives of datafication, connection, and techno-solutionism.

214. The Cloud Empire, implemented and extended by many players but primarily by the social quantification sector, directly benefits from the collusion or lack of states' action, which do not always act by the will of their people. This has caused the balance of knowledge to tip towards the side of a few technology companies, helped by a network of many other actors, generating a severe asymmetry of power that threatens our autonomy as individuals and as a collective.

215. The theory of data colonialism serves as a valuable framework for comprehending challenges associated with children's rights to privacy and to the protection of personal data in the digital realm, particularly with the use of edtech. Nevertheless, the solutions to these issues

are not readily apparent. Some ways to resist it will be briefly outlined in the conclusion of this thesis, encompassing the review of business models, the investment in sovereign and open source technology, the prohibition of data use for commercial purposes conflicting with educational objectives, the enforcement of protection by design standards, among others. However, promoting democratic and decolonial solutions presupposes that the process is as crucial as the content. Any attempt to oppose this order must be global in its *framing* (Couldry; Mejias, 2023, p. 793, 797), but the actual activities carried out must always consider the local specificities, including the community in imagining and designing them.

PART II. LEGAL FRAMEWORK ON CHILDREN'S PRIVACY AND DATA PROTECTION

216. Part II will describe and evaluate the current legal framework applicable to children's rights to privacy and to the protection of personal data in the EU and in Brazil. More specifically, I will focus on the rights enshrined in the CRC (Chapter 5), as well as on the GDPR (Chapter 6) and the LGPD (Chapter 7). Additionally, I will briefly present how AI is currently being specifically regulated in both jurisdictions, especially when it comes to data governance.

217. Before delving into these topics, however, I will discuss why children need special treatment by recognizing them as a subject of rights and adopting a children's rights perspective on privacy and data protection. This entails recognizing and prioritizing children's specificities while protecting and promoting these rights, as well as viewing their fundamental rights as indissociably connected to one another. Therefore, when one right is violated or realized, others are also affected. More specifically, the rights to privacy and to the protection of personal data are certainly an end in themselves but also importantly a means to realize other rights, such as the right to education. Only through this holistic view will we be able to properly allow children to grow autonomously and to their full potential as an individual and as a member of a larger collective.

Chapter 4. Why children need special privacy and data protection rights

218. The creation of a dedicated set of rights specifically tailored to children was not without its controversies, as some still argue that human rights codes already encompass all individuals, regardless of age. However, precisely because children are inherently less mature, more vulnerable, and in need of care and protection, their rights are frequently ignored, denied or abused, which demands a special treatment (Livingstone; O'Neill, 2014).

219. The CRC, as will be better discussed in Chapter 6, focuses on ensuring children are protected from harm, but also intends to foster the opportunities that can help children develop through provision and participation rights. Risks and opportunities, especially in the digital environment, are often linked—"the more one enables provision and participation, the more the need for protection; similarly, the more one seeks to protect, the more one risks undermining participation" (Livingstone; O'Neill, 2014, p. 28).

220. As a provision right, the right to education fosters children's development to their full potential and can be supported through edtech. As previously outlined in the introduction to this thesis, edtech offers numerous opportunities for learning, acquiring information, developing social, digital, and personal skills, as well as enhancing physical and mental abilities. This can prepare children for responsible life in a free society, as demanded by art. 29, CRC (Livingstone; O'Neill, 2014, p. 26). At the same time, the opportunities provided by edtech can create risks to children's rights, especially the rights to privacy and data protection, which is the direct focus of this thesis.

221. This chapter aims to highlight the unique characteristics of children that demand a special treatment in the digital environment. Section 4.1 will begin by discussing two main reasons why children deserve special treatment in this realm, namely their condition of human beings in development, which adds to them an extra layer of vulnerability, and their proportionally larger digital footprint when compared to adults. Section 4.2 will then outline a risk classification of children's online presence, which includes three main dimensions of privacy developed by Livingstone, Stoilova and Nandagiri (2018): interpersonal, institutional, and commercial. Finally, Section 4.3 underlines how surveillance technologies can significantly influence children's trust and development, impacting their ability to make independent decisions and fostering an environment that hinders their creativity and critical thinking.

222. Overall, the chapter underscores the need for a delicate balance between protection and autonomy, risks and opportunities, to ensure the holistic development of children in the digital era and, consequently, the exercise of their rights to education, privacy and data protection in their full potential.

4.1 Why do children's data require special treatment?

4.1.1 Childhood as an extra layer of vulnerability

223. Malgieri and Niklas (2020) conducted a thorough literature review on human vulnerability and propose a new vulnerability-aware interpretation of the rights to privacy and to data protection.

224. The authors show that discussions on vulnerability are traditionally focused on two dichotomies. One of them revolves around the particular and universal aspects of vulnerability. Vulnerability can be understood as a particular characteristic of a group or individual (such as

children, people with disabilities, racial minorities, etc.). On the other hand, some theorists argue that this may lead to stigmatization and defend that vulnerability is a universal human condition—an approach criticized by some, as it tends to overlook structural issues experienced by specific groups or individuals (Malgieri; Niklas, 2020, p. 3).

225. Another important dichotomy is related to the consequences of being vulnerable. One of the approaches focuses on the harms and ways to eliminate them. Another is centered on the individual capacity to overcome this vulnerability through decisional and procedural safeguards in the decision-making process, such as consent (Malgieri; Niklas, 2020, p. 3–4).

226. Based on these dichotomies, the authors advocate that the best way to deal with vulnerability in general, and within privacy and data protection discussions in particular, is the layered approach developed by Luna (2009). She proposes that vulnerability should be understood dynamically and relationally (between the person or group and the circumstances) through layers (Luna, 2009). This notion obliges us to unravel the intricate layers and understand the intersectionality of different issues related to the context. A person's age, if they are a child for instance, can already be considered a layer of vulnerability. Additionally, we must also consider other aspects such as the specific age (due to the evolving capacities of the child), gender, race, country, nationality, health conditions, etc.

227. The extra layer of vulnerability children have is related to the fact that they are still developing physically, mentally, emotionally and spiritually. This means that they still depend, to a varying extent, on other people for protection, provision and decision-making (Sandberg, 2015, p. 222). Children's vulnerability can then be biological or socially constructed. Meyer (2007, p. 90) indicates that children can be

> physically vulnerable (e.g. their bodies are smaller and weaker), socially vulnerable (e.g. they lack certain social skills) and structurally vulnerable (e.g. there are asymmetrical power relations between children and adults). Social and physical vulnerability are usually thought of as "innate" characteristics of the individual child and denote a lack of personal competence or strength. In contrast to this, structural vulnerability—as a lack of power—is a product of society.

228. The Committee on the Rights of the Child[12] also recognizes this horizontal vulnerability of children and specifies that

> [a]t a universal level all children aged 0-18 years are considered vulnerable until the completion of their neural, psychological, social and physical growth and development. Babies and young children are at higher risk due to the immaturity of

[12] The Committee on the Rights of the Child is the body of 18 independent experts that monitors the implementation of the CRC, as well as of its additional protocols. It also has a more "legislative" role, providing commentary on the interpretation of the Convention (United Nations Human Rights Treaty Bodies, [*s. d.*]).

> their developing brain and their complete dependency on adults […] (Committee on the Rights of the Child, 2011, parag. 72(f)).

229. More specifically, the CRC states that some children deserve special attention, such as within the context of art. 23 on children with disabilities and art. 22 on asylum-seeking children. In its comments and jurisprudence, the Committee on the Rights of the Child also emphasizes the existence of subgroups of children with specific characteristics that require further protection (Sandberg, 2015). This aligns with Luna's layered approach mentioned above and also with the principle of non-discrimination enshrined in art. 2, CRC.

230. Children's vulnerability should not be interpreted in a paternalistic way, though, focusing on protection at all costs since it can stigmatize and hinder children's development. As a framework designed to address the specific vulnerabilities of children, the CRC (see *infra* Chapter 5) was established with a central emphasis on recognizing children as rights-holders, acknowledging their diverse capabilities and evolving capacities, and striving to strike a balance between various human rights in different circumstances. Recognizing children's vulnerabilities means, therefore, that they deserve a specific set of rights, including protection, provision and participation rights.

231. More specifically, in the data protection realm, data processing implications are already difficult for adults to understand, let alone for children. They are less experienced, especially in relation to possible risks and harms, and can be easily manipulated (Malgieri; Niklas, 2020, p. 5). For this reason, their agency is limited and others frequently take decisions related to their data on their behalf. There is also "a particular gravity to violations of children's rights because they often have severe and long-lasting impact on child development" (Committee on the Rights of the Child, 2013b, parag. 24). Finally, they have fewer means for challenging the inferences and decisions made for them.

232. This links to the distinction between vulnerability risks related to data processing and the ones related to the outcomes of this processing (Malgieri; Niklas, 2020). Regarding the first one, risks can arise in terms of understanding information about data, what can hamper, for instance freely consenting when necessary, as well as effectively exercising data protection rights. From the second perspective, vulnerability is manifested through specific harms that children may be exposed to as a *result* of the processing of their data. Both of these sources of vulnerabilities will be developed further throughout the thesis.

4.1.2 A proportionally larger digital footprint

233. Apart from having an extra layer of vulnerability compared to adults, another aspect that demands a different approach in relation to children's privacy and data protection is their "digital footprint" being proportionally larger than adults'. Children are being datafied before they are even born through, for example, parent's searches on the internet, online purchases, ultrasound images publications on social media, and the use of pregnancy apps. Corporations have early access to important and sensitive data such as "conception date, weight, number of kicks in the womb, possible names, cultural background, heart rate, diet before conception, parents' thoughts, family ties, family medical history, complications during pregnancy" among others (Barassi, 2020, p. 35).

234. After birth, the baby's life continues to be tracked through growth-monitoring apps, wearables, smart toys, governmental apps and other data-driven technologies. Through smart assistants in the homes, as well as the children's use of parents' devices, children also have their data collected through technologies that are not necessarily appropriate to their needs. As mentioned earlier, the boundaries between individual and group data in data mining processes can be ambiguous. Therefore, children may also be profiled based on the behavior of their parents and the broader family.

235. This means that, unlike previous generations, children have all aspects of their lives turned into data points early on. Each year, a child will have more data collected about them throughout their life compared to a similar child born in previous years (Young; Verhulst, 2020). The older the child, the more they engage themselves in these practices, "but many other actors do so on their behalf, including not only their parents and other caregivers and family members, friends, teachers and healthcare providers but also commercial entities seeking to capitalize on and profit from children's personal information" (Lupton; Williamson, 2017, p. 781).

236. Throughout history, children have, in fact, been subjected to surveillance as a means to enhance their well-being, foster their growth and educational development, and shape them into responsible members of society (Lupton; Williamson, 2017). With the rise of sharenting, parents have been constantly blamed for children's digital presence. Indeed, this is a very problematic phenomenon of our current reality and cultural changes are needed to strike a proper balance between children's rights and their parents'. However, it is essential to recognize that the vast majority of the data points collected from children do not necessarily originate

from their parents' practices. Companies' interests play a significant role in encouraging and facilitating such data collection through technology's design, the sale of wearables, connected toys, and other means.

237. Surveillance technologies are marketed primarily by highlighting the potential risks that children could face, taking advantage of parental worries and making intimate surveillance seem like an essential part of responsible caregiving. It is portrayed as a crucial aspect of being a parent and aligning with the social expectations and norms that new parents are expected to follow or adopt (Mascheroni, 2020, p. 805).

238. It is also important to highlight that tracking a family's life is emotionally relevant to parents as it helps them to experience important moments, such as when family photos are taken. Family data tells a story that people like to share, and this has been done even before digital technologies (such as when parents journaled about a baby's development, tracked their growth and took analogue photos) (Barassi, 2020). As this thesis will show, a closer look needs to be taken technologies' data governance and business models in order to collectively solve a problem that cannot be tackled individually.

239. This is clearly shown by Vertesi (2014), who went through a self-experiment in which she tried to hide her pregnancy, which proved to be a challenging task. She had to refrain from explicitly sharing it on social media (and also ensure that no one who knew her did) and from using pregnancy apps. She also had to use a private browser to look up baby names, as well as buy all pregnancy and baby-related items with cash. The attempt to "opt out" not only made her look rude to family and friends when they tried to bring up the topic online, but also like a criminal. She describes a situation where she had to purchase a large amount of gift cards with cash to buy a stroller online and the store displayed a notice indicating that it could limit the daily amount of prepaid card purchases and report excessive transactions to the authorities (Vertesi, 2014).

240. As a collective concern, the datafication of children's lives poses significant challenges, primarily due to the uncertainties surrounding its future implications. While some of the effects on human rights, particularly in relation to children's equitable access to education, employment, credit, and public services, are already discernible, the long-term cumulative effects of datafication remain unseen. Children's vulnerability obliges us to think about the long-term impacts of technologies and the society we are building by datafying citizens from childhood.

4.2 Privacy and data protection as a cross-cutting dimension of risks to children's online presence

241. Children are increasingly part of the digital environment, already accounting for one-third of all internet users (UNICEF, 2017). This participation holds significant importance in navigating today's society and fostering children's development. It provides them with opportunities such as staying in touch with friends and family, engaging in play, accessing information and education, and participating in democratic discussions. Children themselves, while consulted for the drafting of the Committee on the Rights of the Child's General Comment No. 25, acknowledged that digital technologies are vital for their current lives and future (Committee on the Rights of the Child, 2021).

242. More than a way to enhance fundamental rights, digital technologies are increasingly the gateway for their realization, and children often have no choice whether they would like to use them or not for the most different purposes. Parents, educators, governments, and companies predominantly make these decisions on their behalf. In this sense, opportunities brought about by digital technologies need to be carefully balanced with the risks they pose to children's rights, as they have reduced agency to exercise them and demand their realization. The dynamic and ever-changing nature of the digital environment also means that risks are continuously evolving. As a consequence, children often find themselves encountering emerging risks long before adults are able to adequately tackle them (Siibak; Mascheroni, 2021).

243. It is also important to reinforce that fundamental rights are indivisible and interconnected. This means that the realization or infringement of one right automatically affects others. For instance, if steps are taken to protect children from potential online harm without concurrently considering their right to freedom of expression, the protective measures may excessively limit that freedom (Livingstone; Lievens; Carr, 2020). Therefore, in this session, a risk classification for children's online activities will be presented that takes into consideration different types and dimensions of risks.

244. Drawing from the online risk classification put forth by EU Kids Online in 2009 and an extensive literature review of similar initiatives, the CO:RE project introduces the 4Cs framework for understanding online risks children face. The 4Cs are content, contact, conduct and contract risks (Livingstone; Stoilova, 2021, p. 11):

> Content risks: The child engages with or is exposed to potentially harmful content. This can be violent, gory content, hateful or extremist content, as well as pornographic or sexualised content that may be illegal or harmful, including by being age-inappropriate. Content online may be mass-produced or user-generated (including by the child), and it may be shared widely or not.
>
> Contact risks: The child experiences or is targeted by contact in a potentially harmful adult-initiated interaction, and the adult may be known to the child or not. This can be related to harassment (including sexual), stalking, hateful behavior, sexual grooming, sextortion or the generation of sharing of child sexual abuse material.
>
> Conduct risks: The child witnesses, participates in or is a victim of potentially harmful conduct such as bullying, hateful peer activity, trolling, sexual messages, pressures or harassment, or is exposed to potentially harmful user communities (e.g. self-harm or eating disorders). Typically conduct risks arise from interactions among peers, although not necessarily of equal status.
>
> Contract risks: The child is party to and/or exploited by potentially harmful contractor commercial interests (gambling, exploitative or age-inappropriate marketing, etc.). This can be mediated by the automated (algorithmic) processing of data. This includes risks linked to ill-designed or insecure digital services that leave the child open to identity theft, fraud or scams. It also includes contracts made between other parties involving a child (trafficking, streaming child sexual abuse).

245. Each type of risk is divided into three dimensions in relation to its nature: aggressive, sexual and values. Additionally, apart from the 4Cs, the classification recognizes that some of the mapped risks are related to most or all the four categories, so they were considered cross-cutting risks (these include online risks related to privacy, physical or mental health, inequalities or discrimination), as depicted in the table below:

Figure 2 - The CO:RE classification of online risks to children

	Content Child engages with or is exposed to potentially harmful content	**Contact** Child experiences or is targeted by potentially harmful *adult* contact	**Conduct** Child witnesses, participates in or is a victim of potentially harmful *peer* conduct	**Contract** Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	**Privacy violations** (interpersonal, institutional, commercial) **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) **Inequalities and discrimination** (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

Source: Livingstone & Stoilova (2021, p. 12)

246. The risks related to privacy are considered cross-cutting risks and they can be described in three main dimensions: interpersonal, institutional, and commercial. This framework was initially developed by Livingstone, Stoilova and Nandagiri (2018) based on Nisenbaum's theory of privacy as contextual integrity. It is important to mention that Nissenbaum's theory frames privacy in a broad way, including informational privacy, which would also be aligned with the right to the protection of personal data, as understood in the EU and Brazilian legal frameworks. The authors propose this division focusing on the importance of relationships and contexts in which children act for determining privacy risks, as well as on how children understand the implications for their privacy.

247. Interpersonal privacy is undoubtedly the aspect that children and their parents most focus their attention on, and it refers to the relationships between an individual and other individuals or groups. The decisions taken in the digital environment related to this domain are heavily influenced by how children perceive each context, what is the audience they interact with, and how they balance privacy with other wishes such as participation, self-expression and belonging (Livingstone; Stoilova; Nandagiri, 2018, p. 13)

248. Institutional privacy is related to public or third-sector (not-for-profit) organizations and how they handle children's data. Through exchanges with research participants, as well as a literature review, Livingstone, Stoilova and Nandagiri (2018, p. 13) identified that the collection of data by these entities is often perceived as legitimate, and people do not express concern about the purpose of data collection or the potential long-term consequences of data processing. However, the involvement of governments and other entities in creating children's digital footprints, their ability to request data from private entities, and the sharing of data with other governmental entities can pose significant risks to children's rights. As previously mentioned, it is also crucial to note the increasingly intertwined relationships between public and private entities, particularly facilitated by digital technology. This convergence not only blurs traditional boundaries but also enhances the level of integration, consequently intensifying associated risks (Livingstone; Stoilova; Nandagiri, 2018, p. 14).

249. Finally, commercial privacy pertains to the processing of children's data by commercial entities. As the private sector is currently gathering more data than governments ever did (Nyst; Gorostiaga; Geary, 2018), there is a preoccupation with how they process children's data and the tactics they use to access larger amounts of them. Despite this area's importance, the authors

identified a gap in the available empirical evidence related to children's awareness of commercial data gathering and its consequences. Although existing research shows the existence of certain commercial privacy concerns, children typically exhibit a degree of confusion regarding the concept of personal data and generally struggle to grasp why their data could hold value for others (Livingstone; Stoilova; Nandagiri, 2018, p. 14–15).

250. Within these three contexts, children experience privacy risks that, apart from being a problem in itself, can affect other dimensions, as presented in Figure 1. Hence privacy being considered a cross-cutting risk. The list is extensive and encompasses online marketing and other problematic commercial activities, reputational damage, blackmailing, stalking, identity theft, unwanted contact with strangers, location tracking, manipulation, discrimination and biased decisions, and the potential limitation of future opportunities (Livingstone; Stoilova; Nandagiri, 2018, p. 28–30).

251. Within the school environment, edtech poses significant risks to children's privacy and data protection, as they often process a large amount of data, especially for AI-powered edtech. These data can be aggregated to create detailed profiles of students that can be used for purposes not necessarily aligned with their best interests. Education data can inform decisions across a wide range of areas and serve as input for commercial and governmental strategies. The lack of proper data protection measures can thus directly impact several fundamental rights, such as the right to education, freedom to choose an occupation and non-discrimination more broadly. The specific challenges edtech brings to children's privacy and data protection will be discussed in Part III.

4.3 The importance of privacy and data protection for children's development and learning

252. A critical dimension to consider when evaluating the impacts of edtech on children is its influence on their opportunities to trust and to be trusted. As previously noted, the ubiquity of digital ICTs, coupled with a prevalent business model that encourages the commodification of data and its massive collection, plunges us into a constant state of surveillance. Therefore, the following discussion directly pertains to technologies specifically designed for monitoring children in educational settings, such as behavior tracking or e-proctoring systems. However, it also extends to seemingly innocuous or low-risk technologies that form part of a broader network of stakeholders and data sharing practices, potentially compromising children's rights in a similar fashion.

253. The use of surveillance technologies to monitor and control children can promote an approach to childhood that aims to leave little to chance and achieve a risk-free environment. This approach ignores the importance of balancing trust and risk and the opportunities for children to negotiate terms of freedom and develop skills and competencies (Rooney, 2010).

254. By creating unease and fear, surveillance technologies have the potential to change a child's experience of trust and even replace trust-based relationships. Children perceive surveillance as a means of control that restricts their options and hampers their capacity to act independently. Getting information through surveillance assumes that children cannot be trusted. It can influence their behavior by using punishment and reward as motivating factors instead of moral principles. This type of guidance deprives children of the chance to try out critical and ethical decision-making, ultimately leading to reduced self-regulation and autonomy (Nolan; Raynes-Goldie; McBride, 2011).

255. When children are monitored without their knowledge, it can be even more harmful to their trust in the adult. The deception involved in secret monitoring can damage the very foundation of trust. Therefore, using surveillance technologies can actually increase suspicion instead of fostering a sense of security (Rooney, 2010).

> Children, generally speaking, have less choice when it comes to the need to trust others, and are at a key stage in developing an understanding of others and society more broadly in a way that sets the foundation for their own sense of self. […] [T]he lack of opportunity for trust-based activity has the potential to undermine a child's developing sense of self-confidence and may even fail to provide the conditions for this development to occur in the first place. A child's capacity to become competent and responsible is therefore threatened if the role of trust in a child's emerging agency is overlooked rather than nourished" (Rooney, 2010, p. 353).

256. Children need to develop their own knowledge and skills to judge about potentially harmful information or people online. Trusting a child can help them develop skills and competencies for dealing with difficult situations, whereas the opposite may lead to more secretive and risky behavior. This is not to say that balancing trust and risk is not a complex issue for all actors involved in a child's development, who must consider whether they are protected from harm and whether certain technologies can help achieve this. However, avoiding risks altogether is unrealistic and when selecting the technologies children will interact with (if they are to be used at all), other factors should also be factored in (Rooney, 2010).

257. Surveillance technologies also affect the development of autonomous children and the way they understand privacy. The development of individual autonomy is crucial for both social and socio-emotional development during early childhood. By exploring autonomous actions, children learn to understand their role in society within a specific socio-cultural context, which

helps them become capable adults (Nolan; Raynes-Goldie; McBride, 2011, p. 25). Developing autonomy is also tied to fostering various aspects of their growth, including identity formation, independence, responsibility, individuation, resilience, and self-expression. Additionally, it is crucial for properly developing prosocial behavior, forming strong and trusting relationships, and enhancing critical thinking skills (Nolan; Raynes-Goldie; McBride, 2011, p. 25–26).

258. In contrast, heteronomous children tend to view choices in terms of rewards or punishments rather than critically evaluating them. For instance, heteronomous children typically believe that lying is wrong only if they get caught and punished, but it is acceptable if they do not. Heteronomy can be present in various aspects of a child's life, not only in relation to their parents but also through education, religion, and other institutional structures that reinforce reward and punishment (Nolan; Raynes-Goldie; McBride, 2011, p. 26), such as in the use of surveillance technologies in education.

259. In the context of healthy socio-emotional development, privacy and autonomy are intertwined and dependent on each other (Nolan; Raynes-Goldie; McBride, 2011, p. 27). Autonomy is essential for individuals to exercise their privacy and data protection rights, allowing them to make decisions free from external influence. Conversely, privacy and data protection are also crucial for children, as they need their own space to reflect on their values, beliefs, and preferences without manipulation or other external interference. This is especially important during the development of these values, as surveillance technologies may interfere and impact a child's perception of them.

260. If children cannot experience privacy in their daily lives, they may not develop the ability to establish and advocate for their own boundaries and privacy, or even recognize the boundaries of others. This heteronomous conditioning may be a contributing factor to the prevailing perception of today's youth as being inappropriate "over-sharers" who do not appreciate or value privacy (Nolan; Raynes-Goldie; McBride, 2011, p. 27).

261. In early childhood, children exhibit a desire for privacy and autonomy by engaging in acts of independence and resistance to authority, such as making a mess or noise or running away when called. However, this raises the question of whether it is possible to cultivate genuine autonomy in spaces where children are under constant surveillance and their only means of resisting heteronomy is through secrecy or subversion (Nolan; Raynes-Goldie; McBride, 2011, p. 27).

262. This also hampers creativity and experimentation, preventing individuals from expressing themselves freely due to the fear of consequences. Ultimately, it can stagnate society since these experimentations cannot slowly become commonplace, moral, and/or legal. “All social progress—from ending slavery to fighting for women’s rights—began as ideas that were, quite literally, dangerous to assert” (Schneier, 2018).

263. This directly affects the possibility of implementing a quality education that focuses on the holistic development of human beings. If children cannot trust the space and the adults who take care of them while being educated, this causes them to reduce their participation due to fear of making mistakes and being reprimanded. Considering that making mistakes is inherent and essential to get things right within the school environment, we might witness a generation struggling not only with learning but also with becoming critical and creative citizens who can navigate the world’s problems.

Interim conclusion

264. In this chapter, the aim was to present the reasons why children need special protection in relation to the rights to privacy and to the protection of personal data. I first described the theory of layers of vulnerability as developed by Luna (2009) and why being a child is an extra layer that entails special attention. This was complemented by the fact that children were born in a world where the analogue and the digital are in tandem like never before, meaning that their digital footprint is proportionally larger than previous generations’.

265. I also discussed why privacy and data protection are a cross-cutting dimension of risks to children’s online presence, which will be complemented in Part III by the specific risks brought about by edtech. Finally, I have presented why privacy and data protection are important for the development of children as a whole, especially for their autonomy, which is extremely important for education.

266. The multifaceted nature of children’s presence in the digital environment demands a comprehensive and nuanced approach that acknowledges their unique characteristics and developmental needs. Edtech has the potential to offer unprecedented opportunities for learning, accessing information, and developing physical, social, and digital skills. As presented in the introduction to this thesis, these benefits should be acknowledged as an important opportunity to take education to the next level, promoting more access and equity for all children. Recognizing that opportunities are often associated with risks, however, the former

should be balanced with the need to cater to other rights, striving for a delicate balance between protecting children and allowing them to develop autonomously as human beings.

Chapter 5. The CRC in the digital environment

267. The CRC was unanimously adopted on November 20, 1989 by the UN's General Assembly. It is so far the most ratified human rights treaty in history, with currently 196 parties (Nations Unies, 2023). Especially during a time of changing world order, the CRC brought about a significant paradigm shift. Children should not be viewed as mere possessions of their parents or miniature adults. Instead, children began to be internationally recognized as rights holders (UNICEF, [*s. d.*]).

268. The CRC fully applies to the digital environment, as the latter has become an integral part of children's lives, both positively and negatively impacting several of the rights enshrined therein. These rights are affected even when the child does not have access to the internet or other technologies themselves (Committee on the Rights of the Child, 2021). More evidently, the lack of access to digital ICTs itself compromises rights such as education, information, and social interaction. However, more indirectly, children are also affected by the spread of misinformation; by decisions made about them based on their data, even without their participation; and by the regulation (or lack thereof) of the digital environment.

269. To implement the rights-based approach described in the introduction to Part II, the following subsections will describe how some provisions outlined in the CRC are interconnected with the use of data-driven edtech, and, more specifically, affect children's right to privacy and to the protection of personal data.

270. Considering that the CRC is a comprehensive framework, I will focus on the provisions that are considered cross-cutting standards (being used to guide the interpretation or implementation of other rights) or that directly links to the scope of the thesis. As defined by Hanson and Lundy (2017), the concept of cross-cutting standards largely overlaps with the idea of general principles, as described by the Committee on the Rights of the Child. It is then important to briefly explain the idea of the CRC's general principles, how they came to be, as well as why this thesis does not fully adopt this concept.

271. Originally, the CRC did not make any hierarchical distinction in relation to its provisions nor mention the idea that some of them should be used to interpret and implement the rest of the Convention. The term "general principles" was introduced by the Committee on the Rights of the Child in its general guidelines on periodic reporting in 1996 (Doek, 2007). The Committee identified these principles as arts. 2, 3, 6 and 12 of the CRC, i.e., the right to

non-discrimination; the right to have the child's best interests taken as a primary consideration; the right to life and development; and the right to have their views given due weight in accordance with their age and maturity.

272. The idea of the general principles is largely adopted by scholars and have been widely used by many stakeholders. However, it was not included within the CRC itself and its meaning was not thoroughly developed by the Committee (Hanson; Lundy, 2017). It remains unclear, for example, why these specific provisions were selected as general principles and not others (Lundy; Byrne, 2017). Indeed, some provisions have an intersecting role in relation to all articles of the Convention, as evident from their wording and practical interpretation, such as arts. 2, 3, and 12, as will be detailed below. However, art. 6 on the right to live, survival and development "sits uncomfortably as a provision with a cross-cutting role" (Hanson; Lundy, 2017, p. 301).

273. It is evident that the right to life is a child's most fundamental human right since its fulfilment is a precondition for the realization of all other fundamental rights. In the same way, realizing all other rights enshrined in the CRC contributes to the child's survival or development. Nevertheless, it is not easy to grasp the added value of this right for the interpretation or implementation of other articles in the CRC (Doek, 2007, p. 37).

274. Having this in mind, Hanson and Lundy (2017) propose an alternative conceptualization. They argue that it is possible to identify in the CRC some "overall implementation obligations" related to implementing legislation, setting up of national bodies, development of policies, etc., such as arts 4, 41, 42, and 44 parag. 6, CRC. They also identify some substantive cross-cutting standards[13] that, as mentioned above, will be important to interpret and implement the CRC as a whole. The authors propose replacing art. 6 by art. 5 on the child's evolving capacities as it has been recognized not only by different child rights actors but also by the Committee (see *infra* Section 5.3) as having a cross-cutting role. The subsections below will then adopt this alternative conceptualization and also discuss the rights to privacy,

[13] The authors "choose the word 'cross-cutting' rather than 'general', or 'overall' because it directly expresses what these provisions do: they cross-cut or intersect with and apply to all other articles. We propose the word 'standard' since the common usage of this term expresses, in a general descriptive manner, a substantial norm and also refers to a required level of quality that can be measured. The term 'standard' hence expresses the two main functions of the four provisions (non-discrimination, best interests of the child, respect for the evolving capacities and respect for the views of the child) which are to provide a framework to interpret the CRC as well as to assess progress made with the implementation of the Convention as a whole" (Hanson; Lundy, 2017, p. 302).

education, and protection against economic exploitation as enshrined in the CRC, since they are directly related to the core focus of the thesis.

5.1 The right to non-discrimination

275. Neither art. 2, CRC, nor the Committee on the Rights of the Child define the concept of "discrimination". However, the latter has already invoked some elements of the right to non-discrimination that can help understand it. This right can be defined as "the prohibition of treating similar situations differently without an objective justification" (Besson; Kleber, 2019).

276. Besson and Kleber (2019, p. 60–64) identify and analyze three elements from this definition. First, discrimination implies an unfavorable treatment of any kind, be it a different treatment in similar situations or similar treatment in different situations. There is no need to show intent to discriminate, which means that it encompasses both direct and indirect discrimination.

277. The second element is the necessity of this discrimination to be based on a prohibited ground. Art. 2(1), CRC, provides a list of discriminatory grounds, but this list is purely indicative and can be extended to other similar grounds. It is also important to mention that art 2(2), CRC, extends this protection to discrimination or punishment based on the child's parents, legal guardians, or family members' characteristics. Linked to the discussion on the existence of layers of vulnerability is the emphasis by the Committee that discrimination can be based on multiple grounds (multiple discrimination). In a concrete case, it may be challenging to separate these grounds, but they are "useful to highlight the especially vulnerable position of children in society, and the Convention's lack of explicit protection against discrimination based on age together with other grounds" (Besson; Kleber, 2019, p. 63).

278. Finally, a third element is the absence of justification. The Committee on the Rights of the Child (2016, parag. 21) is of the opinion that "not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose that is legitimate under the Convention". Ultimately, the mere existence of the CRC and of a framework that specifically recognizes children's rights already target a justifiable differentiation between children and adults. Here, the principle of the best interests of the child can be understood as a tool to help justify differential treatments, either between children and adults or between children themselves (Besson; Kleber, 2019, p. 64).

279. In the digital environment, discrimination manifests in multiple ways, such as in unequal access to technology or hate speech. More important for this thesis, though, is the potential for discrimination stemming from biased algorithms. As exemplified before, this can happen "when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child" (Committee on the Rights of the Child, 2021, parag. 10). This also occurs when children in different regions of the world have varying levels of protection concerning their personal data, not necessarily due to the absence of minimal legal protection regarding the technologies that affect them, but rather due to the lack of enforcement and the presence of economic incentives conflicting with their fundamental rights.

5.2 The right to have the child's best interests taken as a primary consideration

280. Art. 3, 1, CRC, provides children with the right to have their best interests taken as a primary consideration in all actions that concern them. This is not a new concept and was first introduced in the 1959 Declaration on the Rights of the Child. Here, it is important to understand the meaning of best interests and what is the role of this right in the CRC.

281. The best interests of the child is purposefully an indeterminate concept, and it will vary according to different societies and historical periods. An interesting definition is given by John Eekellar, who understands it as "[b]asic interests, for example to physical, emotional and intellectual care; developmental interests, to enter adulthood as far as possible without disadvantage; autonomy interests, especially the freedom to choose a lifestyle of their own" (Eekellar, 1992, 230-231, as cited in Freeman, 2007, p. 27).

282. Determining what is in the best interest of a child or group of children must necessarily be done through a rights-based approach, considering all the rights enshrined in the CRC. Ultimately, this is an open and dynamic concept and will largely depend on the assessment of the specific context where it is applied (Committee on the Rights of the Child, 2013a).

283. In its General Comment on the matter, the Committee on the Rights of the Child does not attempt to prescribe what is in the best interests of a child in any given situation but provides a framework for identifying it. It recognizes three primary roles of this right. First, it is a substantive right, which means that children need to have their best interests taken as a primary consideration (the child's interests have high priority and should not be seen as just one of several considerations) when different interests are being considered and whenever a decision

concerning the child is taken. Second, when it is possible to interpret a legal provision in multiple ways, the interpretation that best serves the child's best interests should be selected, having as a basis the rights recognized by the CRC (best interests understood as a fundamental, interpretative legal principle). Finally, it is also a rule of procedure, and an evaluation of the positive or negative impacts of a decision on the child or group of children should be included in every decision-making process that could affect them (Committee on the Rights of the Child, 2013a, parag. 6).

284. It is important to mention that this applies not only to decisions made within the scope of the state, but also to the ones made by the private sector, "including those providing services, or any other private entity or institution making decisions that concern or impact on a child" (Committee on the Rights of the Child, 2013a, p. para 14, (c))

285. In a concrete case, in order to define what the best interests actually are, the Committee provides the following parameters:

> a) The universal, indivisible, interdependent and interrelated nature of children's rights;
> b) Recognition of children as right holders;
> c) The global nature and reach of the Convention;
> d) The obligation of States parties to respect, protect and fulfill all the rights in the Convention;
> e) Short-, medium- and long-term effects of actions related to the development of the child over time (Committee on the Rights of the Child, 2013a, parag. 16).

286. For this thesis, the last criterion is especially important. In the decision-making process, decision-makers will mainly focus on the current interests of the child, which are often formulated in relation to experiential considerations (Freeman, 2007, p. 3). Nevertheless, future interests that are frequently more focused on developmental considerations (Freeman, 2007, p. 3) should also be taken into account. The right to have the child's best interest into consideration should also be seen as a *precautionary principle*, which "requires assessing the possibility of future risk and harm and other consequences of the decision for the child's safety" (Committee on the Rights of the Child, 2013a, p. 74). The understanding obliges us to act cautiously even when the potential danger of a certain technology is not fully established, but there are indications that not acting upon them could inflict harm. This is especially true for the decisions related to the use of technologies, the benefits of which are not confirmed by scientific evidence (Lievens, 2021). We can thus say that the precautionary principle flips the coin and adds extra importance to proving that technology does good rather than proving that it actually causes or will at some point in the future cause harm.

287. Here, the link with the evolving capacities of the child should also be made. The maturity of the child should not only be considered when assessing their best interests but also be used as a criterion for reassessing the decision over time. The scenarios of the child's development should be taken into account, and "decisions should assess continuity and stability of the child's present and future situation" (Committee on the Rights of the Child, 2013a, parag. 84).

288. As a General Measure of Implementation for the CRC, the best way to identify and balance all the interests involved in a decision that affects children is to perform a Child-rights Impact Assessment (CRIA) (Committee on the Rights of the Child, 2003). Every policy, whether intended or not, has a positive or negative impact on the lives of children (Payne, 2019) and understanding the role of art. 3, 1, as a rule of procedure demands states to explain, in every decision, what has been considered in the child's best interest, which criteria have been used, and how different interests have been weighed (Committee on the Rights of the Child, 2013a, parag. 6).

289. Although initially targeting state's initiatives, this tool was later also extended to businesses (Mukherjee; Pothong; Livingstone, 2021), especially under the UN Guiding Principles on Business and Human Rights (United Nations Human Rights. Office of the High Commissioner, 2011).

> Child-rights impact assessments can be used to consider the impact on all children affected by the activities of a particular business or sector but can also include assessment of the differential impact of measures on certain categories of children. The assessment of the impact itself may be based upon input from children, civil society and experts, as well as from relevant government departments, academic research and experiences documented in the country or elsewhere. The analysis should result in recommendations for amendments, alternatives and improvements and be publicly available (Committee on the Rights of the Child, 2013b, parag. 80).

290. The Committee's understanding has been reinforced in its General Comment 25, which focuses on the impact of the digital environment on children's rights. CRIAs should be carried out by businesses "with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children" (Committee on the Rights of the Child, 2021, parag. 38).

> States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child.

> They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service (Committee on the Rights of the Child, 2021, parag. 39).

291. Given its rapid pace of change and complex nature, especially in relation to its long-term consequences, the digital landscape particularly requires the use of such tools. Many stakeholders agree that "if CRIA were used effectively, and its results evaluated transparently, it will make a real difference to realizing children's rights in a digital world" (Mukherjee; Pothong; Livingstone, 2021, p. 26).

5.3 The right to be given appropriate direction and guidance in a manner consistent with the evolving capacities of the child

292. The reference to "evolving capacities" happens twice in the CRC in art. 5 and art. 14(2). Both are related to parental direction and guidance and do not create by itself a right of the child to exercise the rights enshrined in the convention based on their evolving capacities. They actually recognize the right of children to receive parents' and guardians' due guidance and to secure the realization of these rights according to their evolving capacities (Tobin & Varadan, 2019, as cited in Varadan, 2019, p. 308). More broadly, it can be understood as a principle that addresses the processes of children's maturation, as well as their acquisition of competencies, understanding, and agency to assume more responsibility and exercise their rights. This should directly impact their parents' guidance towards an exchange on an equal footing (Committee on the Right of the Child, 2016, parag. 18; Committee on the Rights of the Child, 2009, parag. 84).

293. However this concept has taken a broader role over time. Having analyzed all the comments and jurisprudence from the Committee on the Rights of the Child that mention the notion of evolving capacities, Varadan (2019) concludes that the Committee has indeed recognized it as a principle that should be used while interpreting and implementing the CRC, confirming the need to include it as a cross-cutting standard, as defended by Hanson and Lundy (2017). The Committee's understanding can be categorized into three distinct groups:

> 1) "evolving capacities" as an enabling principle, in which the term is used to empower children in the exercise of their rights under the UNCRC; (2) "evolving capacities" as an interpretative principle, in which the term is used to interpret specific provisions of the Convention in a manner that recognizes children's capacities in the exercise of their rights; (3) "evolving capacities" as a policy principle, in which the term is used to guide states in policy-making and programming on children's rights (Varadan, 2019, p. 316).

294. Understanding the evolving capacities of the child as a principle has profound implications for children's human rights. Is crucial for striking a balance between "recognising [them] as active agents in their own lives, entitled to be listened to, respected and granted increasing autonomy in the exercise of rights [… and] being entitled to protection in accordance with their relative immaturity and youth" (Lansdown, 2005, p. 3).

295. These three categories can be directly applied when children navigate the digital environment and specifically when they are supposed to use edtech. When it comes to empowering children by recognizing children's evolving capacities, data protection frameworks can include means for them to actively and autonomously participate in decisions regarding their personal data. Examples would include enabling children to consent to the processing of their personal data or exercise certain data subject rights depending on their complexity. The Committee emphasizes that the right to exercise increasing levels of responsibility does not mean that other protective measures should not apply (Committee on the Right of the Child, 2016, parag. 19).

296. Viewing the evolving capacities as an interpretative principle implies that data protection laws should be interpreted and applied in a way sensitive to children's developmental stages and respect their evolving understanding of privacy and data protection. Finally, as a policy principle, it could translate into discussions of age appropriateness, which refers to "a developmental concept whereby certain activities may be deemed appropriate or inappropriate to a child's 'stage' or level of development" (Cassidy, 2013, p. 83). This is because the risks and opportunities faced by the child in this realm will vary according to their age and stage of development (Committee on the Rights of the Child, 2021, parag. 19). Many DPAs in Europe, in this sense, have already issued specific guidelines interpreting the data protection laws according to children's specificities, helping controllers to act in accordance to children's evolving capacities and assisting technologists in designing with this principle in mind.

5.4 The right to have their views given due weight in accordance with their age and maturity

297. Art. 12, CRC, guarantees the right for children to express their views freely and be given due weight in all matters that affect them, according to their age and maturity. It is closely linked to the concept of participation, which are ongoing processes that "include information-sharing and dialogue between children and adults based on mutual respect, and in which children can learn how their views and those of adults are taken into account and shape the

outcome of such processes" (Committee on the Rights of the Child, 2009, parag. 3). The idea of participation also emphasizes that this should be not only a momentary act, but the foundation for an ongoing dialogue between children and adults in the development of policies, programs, and measures across all areas of children's lives (Committee on the Rights of the Child, 2009, parag. 13).

298. In order to better understand the scope of this right, it is important to unpack some of its foundational aspects. First, children should have the ability to freely express their views. The term "freely" implies that no pressure should be exerted upon the child, allowing them to decide whether or not to exercise this right. Additionally, it entails that children should not be manipulated or subjected to undue influence or pressure and that they should be able to express their own perspectives rather than adopting the opinions of others (Committee on the Rights of the Child, 2009, parag. 22).

299. Children also need to have their rights to freedom of expression (art. 13, CRC) and access to information (art. 17, CRC) fulfilled. The latter is indeed a prerequisite to the right to be heard, as children need information to take well-informed stances and make decisions. This includes "matters, options and possible decisions to be taken and their consequences [… as well as information] about the conditions under which she or he will be asked to express her or his views" (Committee on the Rights of the Child, 2009, parag. 25). The Committee also emphasizes that children should receive all the information and advice to make a decision in favor of their best interests (Committee on the Rights of the Child, 2009, parag. 16). The quality of the information received by the child should be child-friendly, comprehensible according to their age and maturity, and accessible.

300. Simply hearing the child is not sufficient. Their views should be seriously considered in accordance with their age and maturity. Considering that children's level of understanding are not homogeneously linked to biological age, the Committee included the criterion of maturity, which refers to "the ability to understand and assess the implications of a particular matter" (Committee on the Rights of the Child, 2009, parag. 30).

301. In its General Comment on the matter, the Committee also explicitly provides guidance on hearing children's views in the school environment, as it is fundamental to the realization of the right to education and to address issues such as bullying and discrimination. It emphasizes the importance of encouraging children's active engagement within a participatory learning

setting, particularly when it comes to designing curricula and school programs (Committee on the Rights of the Child, 2009, parag. 107). States parties should also

> consult children at the local and national levels on all aspects of education policy, including, inter alia, the strengthening of the child-friendly character of the educational system, informal and non-formal facilities of learning, which give children a "second chance", school curricula, teaching methods, school structures, standards, budgeting and child-protection systems (Committee on the Rights of the Child, 2009, parag. 111).

302. In the digital realm, the right to be heard could be promoted through consultative online processes, for example. States parties should also involve all children in the development of legislation, policies, programs, services and training on children's rights targeting this environment. It is also their role to ensure that "digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services" (Committee on the Rights of the Child, 2021, parag. 17–18). Realizing this right in the context of datafication is especially important when the dominant discourse is that data can speak for themselves.

303. The right to be heard and, consequently, the right to participate hold particular significance in selecting and implementing technologies within schools. Involving children in decision-making processes regarding the edtech used in their educational environments empowers them to shape their learning experiences, including how their rights to privacy and data protection are considered; ensures that edtech meets the diverse needs and preferences of the student body; and fosters a sense of ownership and accountability, ultimately leading to more effective and inclusive educational practices.

5.5 The right to privacy

304. Art. 16, CRC, basically mirrors art. 12 of the Universal Declaration of Human Rights (UDHR) and art. 17 of the International Covenant on Civil and Political Rights. However, this provision should be interpreted through a child-centric approach, given the different ways that children experience privacy in comparison to adults (Schmahl, 2021). It aims to protect six different but related interests against arbitrary or unlawful interference: privacy, family, home, correspondence, honor, and reputation. The literature often includes all these interests within the concept of privacy, which is justified by a broad understanding of it (Tobin; Field, 2019).

305. Although the concept of privacy is widely used, it has never been properly defined, neither by the Committee on the Rights of the Child, nor by the Human Rights Committee.

However, having analyzed the jurisprudence of international human rights bodies, Tobin and Field (2019) identified the development of at least five dimensions of this right: physical and psychological integrity; decisional autonomy; personal identity; informational privacy; and physical/spatial privacy. For the purposes of this thesis, I will focus on the second, third and fourth dimensions.

306. The decisional autonomy dimension is related to "the capacity to make decisions regarding how an individual leads his or her private life" (Tobin; Field, 2019, p. 565). This idea poses a challenge for children due to child's maturity and a potential conflict between a child and their parents. Both issues can be solved by a contextual analysis of the child's best interests and evolving capacities. This is also a relational concept and includes the autonomy of a child to enter into relationships with others.

307. Privacy is also related to the ability to freely express one's identity. The concept of a child's identity would include, for instance, "the rights to a name, a nationality, to be registered immediately after birth, as well as elements of a child's religious and cultural identity" (Tobin; Field, 2019, p. 568). This right to identity is key to accessing other rights, as it is related to the very recognition of children as rightsholders.

308. Finally, the informational privacy dimension is closely linked to the control of personal information and, therefore, to the right to the protection of personal data. The analyzed jurisprudence reinforces that it applies the access to data created by a person for personal use (such as in personal diaries or text messages) as well as, more broadly, information about a child that either public or private actors can hold.

309. The protection of personal data is an essential safeguard since many children's activities now take place in the digital environment. Practices such as "automated data processing, profiling, behavioral targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine [… and] may lead to arbitrary or unlawful interference with children's right to privacy" (Committee on the Rights of the Child, 2021, parag. 68).

310. In its General Comment n. 25, the Committee on the Rights of the Child states that surveillance and automated processing of data should not only respect children's rights to privacy but also not be

> conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; *nor should it take place without the right to object to such surveillance*, in commercial settings *and educational and care settings*, and consideration should always be given to the least

> privacy-intrusive means available to fulfil the desired purpose (Committee on the Rights of the Child, 2021, p. 75, emphasis added)
>
> […] By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child (Committee on the Rights of the Child, 2021, parag. 110).

311. This is especially important when considering the use of technology in education, as it highlights the inherent power imbalances among educational institutions, technology providers, and students/their parents. Unfortunately, in many instances, individuals are left with no viable option to opt out of pervasive surveillance and select a less intrusive technological solution.

312. More specifically, the Committee emphasizes that processing children's data may lead to the violation of their rights, such as "through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content" (Committee on the Rights of the Child, 2021, parag. 40). It also explicitly states that

> States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children (Committee on the Rights of the Child, 2021, parag. 42).

313. Considering all these dimensions of the right to privacy, according to international human rights bodies' jurisprudence, it is important, however, to avoid a purely protectionist approach. While shielding children from potential risks that may be encountered in the digital environment is a legitimate aim, this should be balanced against the realization of other rights, such as freedom of expression, freedom of association and even education (Lievens *et al.*, 2019). The right to privacy, understood broadly, is essential but is just one of the human rights of children that should be considered in decision-making processes in any given case.

5.6 The right to education

314. The right to education is widely accepted and recognized and, in its enabling role, is essential for enjoying many other human rights. It is a prerequisite for engaging in political activities and ensuring the proper operation of democratic systems; a requirement for many

employment opportunities; a valuable resource to deal with poverty; and a factor that deeply influences individuals' well-being and environmental health (Courtis; Tobin, 2019, p. 1058).

315. The right to education is thus vital to empower children, "providing them with the skills necessary to be on guard against exploitation in all its forms, understand democracy and human rights" (Courtis; Tobin, 2019, p. 1060), as well as enjoy a "well-educated, enlightened and active mind, able to wander freely and widely" (Committee on Economic Social and Cultural Rights, 1999a, parag. 1).

316. Although generally classified as an economic, social and cultural right, its centrality for the enjoyment of civil and political rights defies human rights classifications and "epitomizes the indivisibility and interdependence of all human rights" (Committee on Economic Social and Cultural Rights, 1999b, parag. 2). It should be then recognized both as a right with an intrinsic value and as a multiplier right (Tomaševski, 2001, p. 10), "whose aims promote, support and protect the core value of the Convention: the human dignity innate in every child and his or her equal and inalienable rights" (Committee on the Rights of the Child, 2001, parag. 1).

317. The CRC addresses the right to education in two provisions. Art. 28 recognizes the existence of a right to education in and of itself and mainly focuses on the issues of access to education. Art. 29 addresses the aims of education, directing the actions of State parties in relation to the quality of the education that should be provided. The CRC adopts a holistic notion of education that includes not only the acquisition of knowledge, but also "the development of life skills necessary to realize a child's full potential within the broader context of the community and environment in which the child lives" (Courtis; Tobin, 2019, p. 1063).

318. This holistic understanding of the role of education in individuals and society is fully aligned with the educational concept adopted in this thesis, based on Freire, as discussed in Chapter 1. By viewing history as a possibility, children as individuals whose agency should be fostered, and education as the engine of change towards a more egalitarian world, we realize how reductionist it is to treat education merely as synonymous with "learning". Considering the current landscape of available edtech, this broad view of education has yet to be solidified and embedded in technologies.

319. Katarina Tomaševski, the first UN Special Rapporteur on the Right to Education, suggests the "4As" conceptual framework to identify qualitative dimensions of education that should be implemented in order to fully realize the right enshrined in art. 28, CRC. According

to this framework, states have the obligation to make education available, accessible, acceptable and adaptable (Tomaševski, 2001).

320. The dimension of availability is related to states' obligation to make enough resources available to fulfil children's educational rights, as well as to allow the establishment of educational institutions by non-state actors (Tomaševski, 2001). Accessibility refers to the need for education to be open to all. This implies non-discrimination, physical accessibility, and economic accessibility. Acceptability means that

> the content of education and teaching methods is relevant, culturally appropriate, and of good quality. [… T]he meaning of quality is to be determined by reference to the extent to which a state is able to provide an educational setting which is consistent with the broad and general aims of education outlined in article 29 of the Convention (Courtis; Tobin, 2019, p. 1069).

321. Finally, adaptability relates to the need for education to be flexible to the student's needs and contexts (e.g. students with disabilities, working children, children in situations of humanitarian crises etc.) (Tomaševski, 2001), as well as to the challenges that an evolving society poses (Courtis; Tobin, 2019).

322. These dimensions that should inform the realization of the right to education, as stated in art. 28, CRC, are closely related and establish the link to art. 29, CRC, which describes the aims of education. The very first General Comment issued by the Committee on the Rights of the Child was focused on art. 29, CRC, and it understands that education should provide children with life skills. This includes not only literacy and numeracy but also the capacity "to make well-balanced decisions; to resolve conflicts in a non-violent manner; and to develop a healthy lifestyle, good relationships and responsibility, critical thinking, creative talents, and other abilities which give children the tools needed to pursue their options in life" (Committee on the Rights of the Child, 2001, parag. 9). Education should then "embrace the broad range of life experiences and learning processes which enable children, individually and collectively, to develop their personalities, talents and abilities and to live a full and satisfying life within society" (Committee on the Rights of the Child, 2001, parag. 2).

323. The Committee also emphasizes that education should be child-friendly and developed in an environment that allows children to grow based on their evolving capacities. This means that the kind of teaching, as well as methods and technologies used within education, that focus "primarily on accumulation of knowledge, prompting competition and leading to an excessive burden of work on children, may seriously hamper the harmonious development of the child to

the fullest potential of his or her abilities and talents" (Committee on the Rights of the Child, 2001, parag. 12).

324. Art. 29 challenges an instrumentalist view of education, which considers education a tool for children to ensure economic prosperity and social cohesion (Lundy; Tobin, 2019, p. 1117). Although these are valid and welcomed objectives, the key goal of education should be the "[…] development of the individual child's personality, talents and abilities, in recognition of the fact that every child has unique characteristics, interests, abilities, and learning needs" (Committee on the Rights of the Child, 2001, parag. 9). More broadly, "the enjoyment of the right to education is not conditioned upon, or subordinated to, the achievement of instrumental societal goals" (Courtis; Tobin, 2019, p. 1062–1063). The list included in art. 29 also rejects "strict individualism in favor of a relational conception of rights in which children are aware of the rights and interests of others and their moral obligation to assume a constructive role in their society" (Lundy; Tobin, 2019, p. 1122).

325. The digital environment has the potential to enhance the right to education and its aims recognized in art. 28 and 29, CRC. It can increase access to education and support learning opportunities in extracurricular activities. It can also qualitatively improve education, as children can access more information and educational resources and exchange their views with more people. However, as described above, providing education through digital technologies poses many challenges. Among the specific recommendations specified by the Committee on the Rights of the Child for fulfilling the right to education in the digital environment, two should be highlighted.

326. First, procurement and use of educational technologies by state parties should adhere to evidence-based policies, standards, and guidelines. These technologies must be ethically sound, suitable for educational purposes, and ensure the protection of children from violence, discrimination, data protection violations, and commercial exploitation, among other potential risks (Committee on the Rights of the Child, 2021, parag. 103).

327. Second, digital literacy is of vital import so children gain an understanding of the digital environment's "infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies" (Committee on the Rights of the Child, 2021, parag. 105). Media literacy should serve a dual purpose for children and young individuals, encompassing both a protective and a participatory aspect. It equips them with the necessary skills and competencies

to navigate and control their online presence. Policies and initiatives concerning media literacy should thus be developed in alignment with all children's human rights (Lievens *et al.*, 2019, p. 500) and the school curriculum appears to be the best place to discuss and implement these initiatives with children and educators.

5.7 The right to protection against economic exploitation

328. Art. 32, 1, CRC, recognizes the child's right to be protected from economic exploitation. Although the interpretation of this provision is generally focused on the protection against child labor, it is possible to understand this right in a much broader sense. Verdoodt (2020) proposes to separate this right in two to argue for the expansion of its interpretation. First, "economic" indicates a material interest, namely, the pursuit of gain or profit through the production, distribution, or consumption of goods and services. This material interest can influence the economy at various levels, such as the state, the community, or the family. Second, "exploitation" refers to unfairly taking advantage of others for one's own advantage or benefit. Specifically, this encompasses actions like manipulation, misuse, abuse, victimization, oppression, or ill-treatment (Verdoodt, 2020, p. 98).

329. The broader understanding of these elements allows us to recognize them in the digital environment, as already described above. The need to prioritize children's best interests over commercial interests in the digital environment has also been recently emphasized by the Committee on the Rights of the Child. In its General Comment 25 (2021), the Committee highlighted how commercial interests can negatively impact children's rights to independent information (parag. 53), children's freedom of expression (parag. 61), and children's right to play (parag. 110).

330. More specifically on the negative impacts on children's data protection, the Committee is of the opinion that a) profiling and targeting must not occur for commercial purposes[14]; b) surveillance should not be part of a child's routine and they have the right to object to it in

[14] "States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children." (Committee on the Rights of the Child, 2021, parag. 42).

commercial, educational and care settings[15]; and c) privacy- and safety-by-design approaches should be implemented to prioritize children's rights over commercial interests[16].

331. We should note that although the CRC is not legally binding to the private sector, based on the UN Guiding Principles on Business and Human Rights,

> the Committee recognizes that duties and responsibilities to respect the rights of children extend in practice beyond the State and State-controlled services and institutions and apply to private actors and business enterprises. Therefore, all businesses must meet their responsibilities regarding children's rights and States must ensure they do so […] (Committee on the Rights of the Child, 2013b, parag. 8).

332. It would be fair to argue that students and their parents would not expect that their data be used for purposes unrelated to their education (Chakroun *et al.*, 2022). The Consultative Committee of Convention 108, for instance, stated that "educational institutions need strong legislative frameworks and codes of practice to empower staff, and to give clarity to companies to know what is permitted and what is not when processing children's data in the context of educational activities, creating a fair environment for everyone" (CoE, 2021, p. 7). The Global Privacy Assembly is also of the opinion that "States should consider promoting regulations prohibiting the use or transmission to third parties of children's data for commercial or advertising purposes and the practice of marketing techniques that may encourage children to provide personal data" (Global Privacy Assembly (GPA), 2021, p. 6).

333. The discussion on the legitimacy of a for-profit approach to student's data and its impact on children's rights is intrinsically related to the business models of edtech solutions as discussed in Chapter 3. It prompts us to consider how the commodification of data may provide the incentive to collect and process increasingly larger amounts of children's data in ways that prioritize profit over their well-being and rights. Therefore, discussing the effectiveness of the current data protection gal framework becomes necessary, considering that they still do not focus on the root of many of these problems.

---

[15] "Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose" (Committee on the Rights of the Child, 2021, parag. 75).

[16] "Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child"(Committee on the Rights of the Child, 2021, parag. 110).

Interim conclusion

334. The CRC is a pivotal milestone in the history of children's rights, representing a paradigm shift in societal perceptions and treatment of children. Their unique needs stemming from their evolving capacities and inexperience give rise not only to protective rights but also to provision and participation rights, fostering their holistic development.

335. This chapter aimed to highlight CRC provisions most pertinent to the scope of this thesis. I presented a reconceptualization of the CRC's core principles developed by Hanson and Lundy (2017), outlining four provisions crucial for implementing and interpreting all other rights in the Convention. These include the rights to non-discrimination, to have their best interests taken as a primary consideration, to be given appropriate guidance aligned with their evolving capacities, and to have their views given due weight according to their age and maturity. I elaborated on how these cross-cutting standards influence the interpretation of children's data protection, offering some examples of their application in edtech.

336. Additionally, I discussed other significant provisions, notably the right to privacy (broadly interpreted), the right to education, and the right to protection against economic exploitation. In the realm of education, technologies should are part of a comprehensive strategy aligned with the educational objectives mandated by art. 29, CRC, rather than being adopted solely for convenience or because they are freely available. Such technologies must also harmonize with children's rights to privacy and protection against economic exploitation. This entails that if other interests, such as commercial ones, clash with the right to privacy, or if there is a foreseeable risk of harm from the technology in the future, the child's best interests should serve as both an interpretative guide and a precautionary measure.

Chapter 6. EU's relevant legal and policy frameworks

337. The right to privacy as a human right was recognized in art. 8 of the European Convention on Human Rights (ECHR) in 1950 and has been broadly interpreted to encompass the protection of personal data (European Court of Human Rights, 2022). This is crucial for interpreting the rights enshrined in the Charter of Fundamental Rights of the European Union (CFR), as the interpretation of the latter must be informed by the interpretation of the ECHR by the European Court of Human Rights (ECtHR). Moreover, when applying the CFR, it is essential to ensure that the level of protection provided is, at a minimum, equivalent to that offered by the ECHR, according to art. 52(3), CFR.

338. In the 1960s, many European countries started to realize the potential risks to privacy and human autonomy that arose with technological developments. This has led to various waves of laws that intended to regulate the processing of personal data, as well as to the recognition of data protection as a fundamental right in national constitutions. The German federal State of Hesse was the first to adopt a legal act on governmental records in 1971, and Sweden was the first European country to introduce a national-wide regulation in 1973 (Vogiatzoglou; Valcke, 2022, p. 13).

339. In 1980, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted by the OECD, representing the world's first international statement of principles governing data processing. The principles focused on the protection of privacy and individual liberties and the guidelines were intended to balance it with the free flow of information (González Fuster, 2014).

340. The Council of Europe (CoE)'s Convention 108 was also adopted in 1980 and opened for signature in January 1981. It was mainly driven by an understanding that although the national data protection regimes shared fundamental principles, there were significant disparities that justified further action (González Fuster, 2014, p. 86). Unlike the OECD Guidelines, it formally aimed to ensure data protection. However, it was also directly concerned with securing the free flow of data, and its preamble links it to the freedom of information across frontiers. This was mainly influenced by the exchange that occurred between the Committee of Experts on Data Protection and the OECD since the first meeting to discuss the Convention. They had a common view that the Convention should "respect the principle of free international flow of information as supported by the OECD, and to refrain from laying

obstacles in the way of international trade and commerce" (Hondius, 1978, p. 8, as cited in González Fuster, 2014, p. 87).

341. On the EU level, the first legislation on the topic was the Data Protection Directive (DPD (European Union, 1995)), which was adopted in 1995 and remained in force until the GDPR application in 2018. Heavily influenced by the DPD and the increasing use of personal data to fuel new technologies, the CFR, adopted in 2000 (but becoming binding only in 2009) recognized not only the right to respect for privacy and family life, in its art. 7, but also the protection of personal data in its art. 8 as a separate right (Fabbrini, 2015). The entry into force of the Lisbon Treaty in 2009 also led to important developments for the data protection right in the EU (Kranenborg, 2021). It was explicitly recognized both in art. 16 of the Treaty on the Functioning of the European Union (TFEU), and art. 39 of the Treaty on the European Union (TEU). Furthermore, the CFR was granted legal binding force.

342. The separation of the two rights in the CFR was, however, not obvious, and there is still intense scholarly discussion concerning their relationship, particularly the nature and role of the right to data protection (Vogiatzoglou; Valcke, 2022). The case law of the Court of Justice of the European Union (CJEU) often presents these two rights in an interwoven manner (González Fuster; Hijmans, 2019, p. 4) and, when discussing art. 8, "generally uses a secondary law parlance" (Vogiatzoglou; Valcke, 2022, p. 22). Therefore, the risk of downgrading the fundamental right to data protection to the level of secondary law should be considered. This could potentially limit its content and protective value, opposing the prevalence of EU primary law over EU secondary law (Vogiatzoglou; Valcke, 2022, p. 22).

343. Although the discussion about the adequacy and differentiation of these two rights is not the focus of this thesis, it is essential to highlight their relevance to the conceptualization of data protection in Europe. Ultimately, the separate consideration of personal data protection from privacy, aiming to promote the free flow of information, may serve as the foundation for the current regulation of data as itself a subject of law. Therefore, it is crucial to understand the challenges and potentials of art. 8 as a standalone right (Vogiatzoglou; Valcke, 2022), especially when this interpretation could provide a higher level of protection for citizens' fundamental rights.

344. Apart from arts. 7 and 8, CRF, it is also important to briefly highlight the importance of art. 24, CRF, on the rights of the child, as it could also influence the way we interpret children's rights to privacy and to the protection of personal data. According to its explanation note, art.

24 is “based on the New York Convention on the Rights of the Child signed on 20 November 1989 and ratified by all the Member States, particularly Articles 3, 9, 12 and 13 thereof” (European Union, 2007b). The provision does not adopt the exact wording of the CRC provisions but rather reformulates them in a less detailed way (Lamont, 2021, parag. 24.45). Contrary to what one might expect, the provisions it is based on are not exactly the CRC so-called general principles or overarching standards, but an interesting mix of the right of the child to have their best interests considered as a primary consideration; the right of the child not to be separated from their parents against their will; the right to be heard; and the right to freedom of expression.

345. The TFEU defines no direct competence over the general promotion of children’s rights. However, different aspects of EU Law directly impact children, which means that art. 24 has the potential to shape the development and interpretation of EU measures concerning children (Lamont, 2021, parag. 24.03). The inclusion of this right in the Charter was also seen as a symbolic shift towards recognizing children as rights holders (Lamont, 2021, parag. 24.48).

6.1 The General Data Protection Regulation (GDPR)

346. This section will serve the purpose of a functional analysis of the GDPR, aiming to map key provisions related to the challenges identified in Part III of this thesis. I will specifically focus on provisions targeted at the specificities of children, as well as the ones regarding principles, transparency obligations, roles and responsibilities, legal bases, data subject rights, and the necessity of performing risk/data protection impact assessments.

6.1.1 General Principles

347. Art. 5, GDPR, outlines general principles to be followed when processing personal data. Throughout the various generations of data protection laws in Europe, these principles have undergone few modifications (Terwangne, 2020a), demonstrating the growing importance and stability of data protection fundamentals. They serve not only as the starting point for more detailed provisions throughout the regulation (European Union Agency for Fundamental Rights (FRA), 2018), but also as a means to interpret it. The principles are lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

348. The GDPR highlights the specificities of the processing of children's data in the principle of lawfulness (art. 6(1)(f) and art. 8, GDPR), and transparency (art. 12(1), GDPR). Although considered a cornerstone of data processing, the principle of fairness is not further elaborated in the GDPR. Fair processing of personal data is closely related to the analysis of the reasonable expectations of the data subject, but what it means exactly, especially in the case of children, is still unclear (Milkaite, 2021, p. 206). The rights enshrined in the CRC, especially the principles of the best interest of the child, evolving capacities, the right to be heard and the right to non-discrimination, should be used as a means of defining what are children's reasonable expectations and how they can be incorporated into the processing of their personal data.

349. It is also important to highlight the principles of purpose limitation and data minimization, as they should be more strictly interpreted when it comes to processing children's data (Article 29 Data Protection Working Party (WP29), 2013a, p. 26). The principle of purpose limitation encompasses two sub-principles: purpose specification and compatible use. This means that, first, the purpose of the data processing must be specified prior to the data collection and they should be legitimate, explicit and unambiguous understood by all parties. Second, data cannot be further processed for purposes not aligned with the original one (Drechsler; Vogiatzoglou, 2023). Aligned with this principle is data minimization, which mandates that only data necessary to fulfil a certain purpose be processed.

350. In the era of big data and complex AI systems, however, when the mindset of understanding data as an economic good prevails, these two principles face significant challenges in their application. As we will further discuss in Part III, advanced AI systems, especially ML ones, depend on large amounts of data to be trained and to perform their activities. The way they function also makes it difficult to determine which exact piece of data influenced the inferences or decisions, complicating even further the assessment of data minimization. Especially regarding general-purpose AI, developers may not always foresee all their potential applications, leading to possible changes in the purposes for which data will be processed along the way.

351. Given the challenges already posed by applying these principles to data processing by ML algorithms, we should understand how they can be interpreted even more strictly for processing children's data. In this regard, comprehending the rationale behind these principles in the GDPR can help guide the interpretive approach.

352. The principle of purpose limitation in the GDPR exists for various reasons, such as narrowing down the scope of the processing operation, serving as a factor of foreseeability of data processing activities, and as a barrier to concentration of informational powers. It also enhances legal certainty, transparency, accountability, and individual's trust. At the same time, the possibilities for further use offer a balanced approach between individuals' interests and the pragmatic needs from other public or private actors (Drechsler; Vogiatzoglou, 2023; Ducuing; Schroers, 2020).

353. In order to interpret the purpose limitation and data minimization more strictly, we should shift the focus to the interests of other involved parties beyond the data subject, particularly regarding further use of data. Given that the best interests of children should *primarily* be taken into consideration, other interests should only prevail when they overwhelmingly outweigh children's rights.

354. When conducting the compatibility test outlined in art. 6(4), GDPR, one must assess how the fact that the data are from children influence the assessment. Examples include considering the nature of the data; strengthening the link between the purposes for which data have been collected and the purposes for which they are going to be further processed; the potentially heightened consequences for child data subjects; and the expectations of children as data subjects, which, as mentioned above, can be particularly challenging to grasp as they are still developing their discernment and should be interpreted according to the realization of their rights within the CRC.

355. These general principles can be better implemented through the principle of data protection by design and by default using appropriate technical and organizational measures (art. 25, GDPR) to put in practice a comprehensive and holistic approach to children's rights (Hof; Lievens, 2018, p. 2). According to recital 78, GDPR, these measures include

> minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

356. The list above is non-exhaustive and controllers must be creative while implementing other measures and safeguards that are appropriate to the nature, scope, context and purposes of the data processing. Based on the accountability principle, "[a]n organization should be able to show how the best interests principle has driven the design, development, implementation and/ or operation of any service which is directed at/ intended for, or is likely to be accessed

by, children and how measures implemented are effective in achieving this" (Data protection Commission (DPC), 2021, p. 63).

6.1.2 Roles and responsibilities

357. The roles and responsibilities described in the GDPR do not change when children's data are processed. Nonetheless, interpreting the requirements of the GDPR appropriately, as well as understanding the challenges posed by complex AI supply chains and by certain specific situations within edtech, will be crucial for the analysis conducted in Part III.

358. The concepts of controller and processor as described in the GDPR are functional concepts, which means that roles should be identified solely based on an assessment of the factual elements or circumstances of the case (European Data Protection Board (EDPB), 2021, parag. 12). According to art. 4(7), GDPR, the data controller is

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (emphasis added).

359. To be able to determine the purposes and means of the data processing (the "why" and "how", the actor should be able to truly exercise the decision-making power, which could stem from legal provisions or the factual influence (EDPB, 2021, parag. 21). The level of influence of each actor will certainly vary depending on the situation, which requires that clear criteria be defined in order to draw the line, especially when processors are involved.

360. The EDPB is of the opinion that decisions on the purpose of the processing are always for the controller to make, while decisions in relation to the means can be done by both controllers and processors. What needs to be considered in relation to the latter is if the means are essential or not:

> "Essential means" are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?"). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on (EDPB, 2021, parag. 40).

361. When the public school is providing the edtech to children, the school will likely be the controller for the majority of the processing activities, meaning that most of the compliance

obligations will fall on them. The edtech provider, as a processor, will be basically the “digital extension of the school’s offline activities and the school exercises the decisive influence over the processing. [The] edtech product or service is not merely helpful for the school, but forms an integral part of the school’s functions” (Information Commissioner's Office (ICO), 2023a, n.p.).

362. From the case law of the CJEU, we can ascertain that the concept of controller should be understood broadly, in order to protect data subjects and encompass those who exert influence over the processing of personal data for their own purposes, participating, as a result, in the determination of the purposes and means of that processing (European Union, 2018a). To exert influence includes, for instance, defining parameters, contributing to determining the purposes of another controller’s processing, and making processing by other controllers possible (European Union, 2018b, 2019).

363. An example can elucidate how this functions in practice. When schools procure a LMS to provide a digital platform for teachers to upload assignments, they enable the processing of students’ and staff members’ data by the LMS provider. The schools also establish the purpose of the processing, which in this case is to realize the functionality provided by the LMS provider.

364. This remains the case even when the school does not have access to the data directly (EDPB, 2021). For instance, if the platform employs algorithms for personalized learning, the means of the processing (algorithmic analysis) and the purposes (enhancing individualized learning experiences) are determined by the school which procured the service for this specific finality.

365. Defining the roles, however, is not always so straightforward. First, because the platform can participate in defining the essential means of the processing activities such as which data is processed; for how long they are processed; if decisions are automated etc. Second, platforms may exert influence or engage in processing for their own purposes that are not directly related to providing the contracted service. If the platform process personal data for their own purposes beyond what is necessary to deliver the requested service to the customer or influence the purposes of processing operations for their own commercial gain (so more or different types of data are collected in the first place, for instance), they cannot be considered a processor anymore (Cobbe; Singh, 2021).

366. When the edtech provider wants to be a controller for its own purposes, another relationship with the data subject will need to be established, such as through a separate contract. On the other hand, according to the EDPB guidelines on the matter, joint controllership may be identified when decisions about the data processing are inextricably linked (EDPB, 2021)**.** Therefore, if the edtech provider intends to process data for its own purposes that it accessed solely due to the contract with the school, then the school will necessarily be considered a joint controller. In this case, the school could only participate in such a joint controllership if the data processing activity is part of its mandate.

6.1.3 Article 8, GDPR

367. Unlike the DPD, the GDPR (European Union, 2016) contains specific provisions focusing on protecting children's data. Recital 38, GDPR, sets the tone of this special protection, stating that

> [c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

368. Based on the need for a special protection, art. 8 outlines the specific conditions under which consent can be used as a lawful basis for processing children's data by Information Society Services (ISS). As a general rule, consent should be given or authorized by the holder of parental responsibility until the child reaches 16 years of age. However, MS could lower it until 13 years. This section will aim to explain the specificities of this provision.

6.1.3.1 ISS

369. The rule contained in art. 8 solely applies to ISS. These services are defined in art. 4(25), GDPR, through a cross-reference to the art. 1(1)(b) of the Single Market Transparency Directive. They should be understood as

> any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

370. This is a comprehensive definition and will encompass almost any online service. For the purposes of this thesis and for the applicability of art. 8 to the use of edtech within the school environment, it is important to clarify two aspects.

371. First, regarding the necessity for remuneration, it should be understood broadly (Kosta, 2020). According to the CJEU caselaw, remuneration does not need to come directly from the user through a monetary transaction in so far as the service represents an economic activity (European Union, 2014, parag. 28–29). There is also no need for the provider of the service to be seeking to make a profit, which would encompass the provision of the service for educational, charitable or recreational purposes as well (European Union, 2007a, parag. 34; Tosoni, 2020, p. 297). Additionally, it is possible to argue that in the cases where the service is provided on a non-profit basis, but it is still commonly provided on a for-profit basis, then it will be considered to be "normally provided for remuneration" (ICO, 2023b).

372. Second, it is important to clarify what an individual request is. As mentioned above, under the Single Market Transparency Directive, this means that the service is provided through the transmission of data upon individual request. This would not include, for example, television and radio broadcasting services as clarified by Annex I of the Directive. Within the CJEU caselaw, the Mediakabel case is an interesting example of how this requirement is interpreted. Mediakabel was a pay-per-view service where users would order a film from their catalogue using their personal identification. The CJEU did not consider it to be a service at the individual request since the list of films available for watching is solely determined by the service provider (European Union, 2005, parag. 38–39; Tosoni, 2020).

373. This raises the question of whether edtech services provided for or procured by schools would fall under this definition. One could argue that even if the school is an intermediary in relation to the provision of the service, if the student or their parents need to create an account or log in to use the service, or even interact individually with a service using a school device, this could already be considered as an individual request for data to be transmitted (Hooper; Livingstone; Pothong, 2022, p. 12).

374. However, in cases where the school assumes the role of controller in processing activities, it seems evident that they do not fall within the scope of art. 8, as they would not be considered ISSs. As we will delve into further below, using consent as a legal basis within the school environment will often prove unsuitable due to the inherent power imbalance between them and the data subjects. Nonetheless, in situations where consent is deemed appropriate and

art. 8 does not apply, the question arises regarding the possibility of using this legal basis at all, as well as the appropriate age for providing consent and who should provide it if not the child. If we consider that consent is still a possible legal basis, it appears that the age of majority rules governing civil acts in each country will need to be applied instead of art. 8, GDPR.

6.1.3.2 Offering directly to a child

375. The application of art. 8, GDPR, also depends on the service being provided directly to a child. In order to better protect children's best interests, we should interpret this provision broadly. The provision should not be understood to cover only services exclusively built for children (such as YouTube Kids, Messager Kids, or other services solely focused on children). If children are also a target audience for the service, along with adults, parental consent should also be obtained depending on the child's age (Kosta, 2020). If a service intends to exclude children from its usage, it is crucial to clarify that they only offer their services to adults (EDPB, 2020, parag. 130).

376. Based on the fairness, accountability and data protection by design principles, it is possible to argue that all necessary measures should be taken to effectively prevent children from using it and merely stating this in their ToS would not be enough. This is also supported by the EDPB when it argues that more important than what is stated by the service is the evidence related to the actual offering of the service to children (EDPB, 2020, parag. 130).

377. If the service is not directed to a child and still needs to process children data for any reason, art. 8 would not apply, and national laws on age majority will need to be complied with. Still, data should be processed in children's best interest, and all principles of the GDPR should be interpreted based on that.

6.1.3.3 Age for consent

378. Art. 8 is a clear attempt to balance the fact that children are rights holders with evolving capacities and their need for special protection. Determining an age at which certain rights should be acquired or certain protections should be lost is a complex issue (UNICEF, 2007, p. 1). As the UN Special Rapporteur on the right to privacy puts it,

> [c]hildren's readiness for decision-making and self-responsibility is best determined not by chronological age alone but by context, including the risks and support available, individual experience, the rights affected and capacity for understanding the implications of their actions (or non-actions). Determinations on when children are capable, for example, of consenting to the processing of their personal data, must take into consideration their actual understanding of the data processing, their best interests, rights and views (Cannataci, 2021, parag. 114).

379. As previously discussed, this should ideally be done on a case-by-case basis as each child grows and develops their capacities at varying ages. However, especially while formulating policy and legislation, these decisions should consider children as a group.

380. When this is the case, recognizing the best interests of the child as a rule of procedure will necessarily require an evaluation of the decision's impacts on the specific group of children being targeted. Children should be involved in the process to ensure their right to be heard is fulfilled. However, it appears that this was not the case when determining the age range for consent to be included in the GDPR (Carr, 2016; Lievens, 2016).

381. The impact assessment that accompanied the GDPR states that the rules for consent that require parental authorization took direct inspiration from the USA's Children's Online Privacy Protection Rule (COPPA) of 1998. According to the document, this would benefit online businesses since they would not "impose undue and unrealistic burden upon providers of online services and other controllers" (European Commission, 2012, p. 68).

382. Instead of assessing the provision's impact on children's rights, as mandated by the CRC, the Commission relied on a foreign rule implemented to benefit businesses. The threshold for consent in COPPA itself was also not based on empirical evidence but was the product of political compromise (Macenaite; Kosta, 2017, p. 183). The rule that emerged for online marketing in the 1990s can also poorly reflect the need for greater protection in today's digital environment, where children's data are processed in an unprecedented volume.

383. Research carried out by Livingstone and Ólafsson (2017), based on data from UK, indicates that children's commercial literacy tends to increase consistently from the age of 8 to young adulthood. Additionally, there would be a noticeable enhancement in commercial literacy between the ages of 13 and 16. It is uncertain whether these outcomes apply to the entirety of Europe. As previously mentioned, various factors in children's development influence their vulnerability and the acquisition of specific skills at different times and in different ways. Nonetheless, these findings highlight how such evidence can be readily collected to inform policymaking and enhance the protection of children's fundamental rights.

384. Within the EU, MS have selected all possible ages to establish the consent threshold, which would hinder the goal of achieving consistency under the GDPR. The implementation of art. 8 has resulted in a fragmented scenario, making it challenging for data controllers to conduct their operations within the EU (Milkaite, 2021, p. 168–169). This is also problematic because

it creates a form of discrimination among children from different countries without clear justifications (Milkaite, 2021, p. 170).

6.1.3.4 Consent as an appropriate legal basis for processing children's data

385. In societies that foster individual freedom, consent plays an important role as a legal and ethical tool for status change. Consent legitimizes an act that would otherwise be initially illegal or immoral (Kim, 2019). However, to have this transformative role, consent needs to be valid.

386. For decades, a vast literature has highlighted the problems related to consent in the most different areas and, more specifically, as a legitimizing tool for the processing of personal data. In a recent analysis, Solove (2023) maps six main issues, which will be briefly rearranged and summarized below. I will afterwards discuss the specificities of children's consent.

387. The first problem of consenting is related to its formal requirements, its ambiguity and the difficulty of providing evidence that a person *de facto* consented. An invalid consent is an oxymoron, but discussing its validity is an important way to determine the conditions that warrant its transformative role (Kim, 2019-, p. 7). In the case of the GDPR, art. 4 (11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The formal requirements include that it should be freely given, specific, informed, and unambiguous. Even with the requirements that consent should be specific and unambiguous, it is not easy to prove that it was indeed freely given or informed, as will be discussed below.

388. The second issue is related to the substance of one of these requirements: the necessity of consent to be freely given. The information provided to individuals so they can consent is included in privacy policies, in its majority standardized texts with boilerplate language that cannot be negotiated. EDPB Guidance on the issue states that consent is invalid when a data subject "has no real choice, feels compelled to consent or will endure negative consequences if they do not consent […]" (EDPB, 2020, parag. 13). However, in most of the cases, there is no adequate alternative and not consenting to these unilaterally imposed clauses means to give up of many of the essential services in today's society.

389. Recital 43, GDPR, also takes into account power imbalances and indicates that consent will not be valid in these cases, especially when the controller is a public authority. This is

especially important in the case of more vulnerable data subjects as children, who will likely be in a situation of power imbalance. The educational context is an important example in this regard. The CoE highlights that "children in an educational setting constitute a typical example of a situation where there is an imbalance between the data subject and the controller and where another legal basis should rather be applied" (CoE, 2021, p. 8, footnote 7).

390. Although the GDPR tries to avoid situations of coercion, manipulation is much more difficult to deal with and much less restricted in privacy laws (Solove, 2023). Humans' rationality is bounded due to their cognitive capacity, time, and access to information. This makes people sometimes to act "irrationally and in ways contrary to their beliefs, desires and self-interest for a variety of reasons" (Kim, 2019-, p. 11). Manipulation techniques are used then to explore these intrinsic human vulnerabilities and, in digital technologies, they are often embedded in their design (e.g. dark patterns) (Hartzog, 2018-). Considering that children are still developing their critical sense and discernment, they are even more easily manipulated, making it crucial to protect their data by design.

391. A third issue concerning using consent as a lawful basis for data processing is the challenge of effectively informing individuals about their choices and the potential impacts. This issue arises for four primary reasons (Solove, 2023). First, making the information available does not mean that people will see it or read it. Second, privacy notices are often excessively lengthy and intricate, filled with legal jargon, which leads to people disregarding them even when they are aware of their existence.

392. Art. 12, GDPR, explicitly states that information must be communicated "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child". However, more straightforward notices can end up being vague and not containing important information that could potentially lead to a better understanding of the data processing. Third, being exposed to the information does not mean that people really understand what it means and the risks they are assuming. Finally, incorrect or pre-existing notions that each individual carries will affect how they interpret the terms, and they can end up acting upon false beliefs or inferences about how their data are being processed (Solove, 2023).

393. A fourth problem is the individual's inability to make decisions (Solove, 2023). When people are in a situation where they need to rapidly decide in order to access something they desire, the cost-benefit analysis can be hampered. While the benefits are often immediate and

concrete (such as accessing a service, a discount, a game, etc.), the risks are difficult to determine. Due to the bias of imaginability, evaluating the predictability of future events is "especially problematic where the future event is novel, unfamiliar or unprecedented. In these situations, the consenting party lacks the experience to make accurate predictions, including the ability to predict his own reactions to the anticipated outcome" (Kim, 2019-, p. 12).

394. To really calculate the costs and benefits, reading and understanding a very lengthy privacy notice would not be enough. One would ideally

> know a lot more about the security program that the organization has in place. Does the organization use good encryption? Does it have all the appropriate policies and procedures? Does it train its workforce? Does it adequately vet any vendor that handles personal data or has access to it? To assess confidentiality, the person needs to know about the privacy program. How well-resourced is it? What are the rules for when various types of parties can subpoena the data? How readily and likely will the government access the data? Is the workforce trained about privacy? How are access controls managed? The list can go on and on. Most people end up consenting based on bald statements that data is being protected, but these statements are often boilerplate written by lawyers to sound reassuring without promising very much. People simply do not know enough to meaningfully consent. In most cases, consent means taking a leap of faith in dark (Solove, 2023, p. 31).

395. If it is not possible to understand the full picture and calculate the risks of letting their personal data be processed, then consent cannot be deemed to be informed. Therefore, using consent as a means to exercise individual autonomy and data control in a complex digital environment is often an illusion.

396. The fifth problem revolves around structural limitations related to how consent choices are framed (Solove, 2023, p. 32 et seq.). Some situations involve inadequate, binary choices, where people are can either opt in or not. Other situations will involve too many choices, and an approach that is too granular can also be overwhelming. As Kim (2019-, p. 13) argues, more information is not always better, and can "even impair decision-making ability. Psychological studies show that for humans, attention is a scarce resource, and complex information may escape a decision-maker's notice". Lastly, and as a consequence of the above, the sixth issue is consent fatigue. When one asks for consent too many times, the actual warning effect of consent mechanism is diminished (EDPB, 2020, parag. 87–88). Even if consent could be informed and freely given, it is difficult to scale.

397. These six issues of consent as a mechanism of individual autonomy and control over one's personal data are applicable to all data subjects. Nevertheless, children can face even direr challenges. Van der Hof (2017, p. 124–133) uses three lenses based on a rights-based approach to analyze their specificities. First, under a protection lens, although specific rules for children's

consent are legitimate and even imperative, parents are not necessarily more capable of making these decisions on their behalf. This is mainly because of the facts already enumerated above. From an emancipation and participation perspective, parental consent can also be problematic as it raises tensions between parents and children and can encourage parental surveillance. Especially when it comes to teens, a private space between them and their parents is also essential for their development. In this regard, the GDPR only focuses on one exception in its Recital 38, stating that parental consent "should not be necessary in the context of preventive or counselling services offered directly to a child".

398. Finally, when viewed through a developmental lens, obtaining consent from children presents significant challenges owing to their varying stages of cognitive and emotional development, coupled with an added layer of vulnerability. Therefore, safeguarding children's data demands a broader approach beyond merely seeking consent, as it can be seen as a way to free states, private actors and society in general from their responsibility for possible violations (Barret *et al.*, 2021).

399. All the challenges explained above only highlight that the burden of protecting personal data cannot be on children or their parents, and there is a strong need to shift the main responsibility to controllers (Macenaite; Kosta, 2017). In this sense, protecting children's data will necessarily involve the implementation of high standards of privacy by design (Hof; Lievens, 2018), the establishment of prohibitions on processing certain types of personal data or for certain purposes (e.g. art. 28(2) of the Digital Services Act (DSA), which prohibits processing children's data for advertisements based on profiling), reframing the role of children's and parental consent (Solove, 2023), as well as conducting CRIAs alongside Data Protection Impact Assessments (DPIAs).

6.1.4 Other legal bases for processing children's data

400. Art. 6, GDPR, provides an exhaustive list of legal bases for personal data to be lawfully processed. In order to decide which one is the most appropriate, controllers should consider the impact of the processing on data subjects' rights, as well as the fairness principle (EDPB, 2019, parag. 1). This includes assessing "the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller" (EDPB, 2019, parag. 12). As consent has been discussed in the previous subsections, I will here focus on the other five legal bases and how they could be applied within the school environment.

6.1.4.1 Contractual necessity

401. Art. 6(1)(b), GDPR, allows the processing of personal data when it "is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". In order to use this legal basis, a contract exists must first exist and be valid under the relevant contract law. In the case of children, for example, it is necessary to comply with the age of contractual capacity set by each MS, as well as check the child's competence to understand what they are agreeing to (DPC, 2021). This age may differ from the legal age of majority, which is currently set at 18 years old in all EU MS. Consequently, unlike consent, the contractual partner does not have the option to revoke their agreement to cease data processing. Instead, the contract would have to be deemed void or terminated in accordance with national contract law (Milkaite, 2021, p. 189).

402. Second, the processing must be necessary for the performance of the contract. This evaluation need to combine a fact-based assessment of the processing for a specific purpose and whether it is less intrusive than other options. If the processing is just beneficial for the controller or included unilaterally in the contract but not objectively indispensable for providing the contractual service, then it is not necessary for the performance of the contract (EDPB, 2019, parag. 25). The principles of purpose limitation and data minimization are particularly important for contracts as they are generally not negotiated on an individual basis within the digital environment (EDPB, 2019, parag. 16).

403. In this context, it is crucial to examine not only the viewpoint of the controller but also that of an average data subject to ensure a genuine mutual understanding of the contractual purpose (EDPB, 2019, p. 32). This becomes particularly pertinent when dealing with children. Even with parental assistance in contracting activities, the child retains their status as the data subject, emphasizing the importance of considering children's expectations.

404. The necessity criterion requires a strict interpretation, and, based on the accountability principle, the controller must be able to "demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur" (EDPB, 2019, parag. 30).

405. In the case of edtech for teaching and learning, the use of this specific legal basis will depend on whether the service is directly provided to children or their parents by the private entity, or if the service is provided by the school. If the relationship is between the private actor and the child or their parents, then some processing activities will probably be necessary for the

performance of this contract. The same applies to the situation where a private school provides the service to a child or their parents based on a contract.

406. Specifically for the purpose of content personalization, as it might be the case for personalized learning, the EDPB is of the opinion that it "may (but not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract" (EDPB, 2019, parag. 57, emphasis in the original).

407. However, the scenario shifts when a public school delivers a public service, a situation not governed by a private contract. In cases where schools act as the controller or joint controller, they will likely need to seek an alternative legal basis as the only contract that may exist is the one between them and the edtech company, to which the child or their parents are not direct parties.

6.1.4.2 Compliance with a legal obligation

408. Art. 6(1)(c) could be invoked by schools or edtech companies when they must process personal data to fulfil requirements mandated by EU or national laws. It also encompasses situations where the obligation is not defined within a law but rather arise from an additional legal act such as a delegated legislation or binding decision of a public authority. However, it clearly does not cover legal provisions that merely authorize or license something (Kotschy, 2020). To rely on this basis, an organization must be able to pinpoint the precise legal obligation and demonstrate how processing the data is essential for fulfilling it.

409. This is a legal basis which is mostly used by private actors within the educational realm since the public sector will be able to rely on the performance of an official or public task (art. 6(1)(e)). If a public authority is legally obliged to provide education, but the specific means are not defined (such as using digital technologies), the law may not serve as a valid legal basis. In such instances, the authority has ample discretion to determine the manner in which this obligation is met. This lack of specificity would fail to satisfy the binding element for a law to be employed as a legal basis for processing personal data.

410. It is important to mention that the applicability of this legal basis by the public sector had not been entirely ruled out by WP29 in its interpretation of art. 7(c), DPD. However, this provision could only be relied upon when the obligation comes directly from a legislative provision (Kotschy, 2020).

6.1.4.3 Vital interest

411. Using art. 6(1)(d) as a legal basis is less common, as it usually applies to atypical circumstances. Examples would be situations such as "monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters" (Recital 46, GDPR) and other life threats such as when a child is missing or severely ill. Certainly, these situations can be experienced in a school environment. However, in scenarios where elements of urgency and risk or concrete/imminent danger to the data subject's life are not present, this legal basis is less likely to apply. It could be used in cases of child protection and child welfare measures, for instance.

412. The threshold for fulfilling the necessity element of this legal basis will most probably be lower than when adults' data are processed, as children are considered to be more vulnerable (DPC, 2021, p. 24). The principle of fair processing may be used as a basis to require that the data subject is consulted when possible (Kotschy, 2020). In the case of children, their right to be heard should be respected as well as their will considering their evolving capacities. It is also important to consider that processing parents' data may also be necessary to protect the child's vital interests.

6.1.4.4 Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

413. Art. 6(1)(e) is a general legal basis for the public sector to process personal data. It can be used when data processing is necessary for a task entrusted to the controller[17] to be carried out in the public interest or in exercising official authority. Recital 41, GDPR, clarifies that the EU or national law determining the purpose of processing "should be clear and precise and its application should be foreseeable to persons subject to it".

414. In contrast to art. 6(1)(c), this provision does not establish specific obligations for the controller. Instead, it grants a broader authorization to take necessary actions to fulfil the assigned task. Based on that, Kotschy (2020, p. 335) argues that art. 6(1)(e) is quite similar to

[17] Kotschy (2020, p. 335) highlights that "[i]n the English version of Article 6(1)(e) it is ambiguous whether the words 'vested in the controller' relate to 'exercise of official authority' or to 'a task'. The meaning of Article 6(1)(e) is clearer in the German version where commas are set in order to structure the sentence. Transferring this structure into the English version, it would read as follows: 'Processing is necessary for the performance of a task, carried out in the public interest or in the exercise of official authority, vested in the controller'. […] Vesting such a task in a controller requires a legal provision to this effect. Such understanding excludes cases of assignment of 'tasks' by contract, even if they were 'in the public interest', which will be particularly significant where private entities shall be 'vested with a task' in the sense of Article 6(1)(e)."

art. 6(1)(f), as it also demands interpreting and balancing interests. This similarity would probably be the reason why only these two legal bases are subject to the data subject's right to object (art. 21, GDPR).

415. In the case of schools, any activities considered necessary to provide education or to fulfil other obligations related to providing education will likely meet the requirements for using this legal basis as long as they are based on EU or MS legislation. The challenge associated with this legal basis is that the corresponding legal obligations often lack specificity regarding the processing operations they can encompass and the types of data that can be processed for the intended purpose. Consequently, the principle of data minimization serves as a crucial guideline for determining what data are necessary in order to fulfill a specific regulatory requirement.

416. When it comes to the necessity of using edtech, their indispensable utilization was perhaps more evident during the COVID-19 pandemic, when students were learning from home and had to receive education remotely. However, this is less clear in hybrid learning environments.

6.1.4.5 Legitimate interests

417. Based on art. 6(1)(f), GDPR, another possible lawful basis for processing personal data is the legitimate interest of the controller or a third party. It can be used when these interests are not "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, *in particular where the data subject is a child"*.

418. The concept of legitimate interests is comprehensive and there is no exhaustive list of interests encompassed by it. The GDPR provides some examples in its recitals, such as preventing fraud and direct marketing (recital 47); the transmission of personal data within a group of undertakings for internal administrative purposes (recital 48); or network and information security (recital 49). More generally, *interests* can be defined as "the broader stake that a controller may have in the processing, or the benefit that the controller derives—or that society might derive—from the processing" (WP29, 2014, p. 24).

419. Art. 6(1)(f) calls for a balancing test to assess if the interests of the controller or a third party outweighs the interests or fundamental rights and freedoms of the data subject. Several methodologies have been developed by national DPAs over the years to help controllers carry out this assessment. WP29 provided a list of key steps that should be considered when applying

the balancing test, which includes assessing the particular interest of the controller (if it is a fundamental right, an interest of the wider community or other legitimate interests, as well as the legal and cultural/societal recognition of the legitimacy of the interests); the impact that the processing operation will have on data subjects' interests or fundamental rights (including a risk assessment, the nature of the data, the way data are being processed, the reasonable expectations of the data subject, and the status of the data controller and data subject); carrying out a provisional balance; and applying additional safeguards (such as opt-out mechanisms, immediate deletion of data after being used, anonymization, the use of privacy-enhancing technologies, etc.) (WP29, 2014, p. 33 et seq.).

420. When considering the legitimate interests legal basis, which in general would allow for a proportionate level of interference with data subjects' rights, it is important to adjust the balancing test to the specific situation of children as data subjects (DPC, 2021, p. 25). It cannot be asserted in the abstract that there are no situations where a child's interests cannot be overridden. However, the analysis of the best interests of the child, which include all their fundamental rights enshrined in the CRC, should be a primary consideration when taking a decision that affects them and not just one of the criteria to be weighted.

421. This can be observed when children's data are processed for commercial purposes, such as in profiling, which is suggested to be prohibited by the Committee on the Rights of the Child. Therefore, unless an organization can demonstrate, in accordance with the accountability principle, that profiling children is indispensable to achieve a goal consistent with their best interests, such processing should not proceed.

422. More specifically in relation to the use of the legitimate interests legal basis by schools or edtech, it is important to note that it shouldn't apply to cases in which public authorities perform their official tasks. When it is used by private entities—especially technology companies providing the service directly to a child or in the case of processing operations where they act as a sole controller—this legal basis could be used for example, when measures should be taken or safeguards employed to protect children's health or safety (e.g. processing children's data for the purpose of network safety) (Atabey, 2021).

6.1.5 Analysis of selected data subjects' rights

6.1.5.1 Transparency obligations and the right of access

423. The principle of transparency is further elaborated in arts. 12, 13, and 14 GDPR. According to recital 39, GDPR, natural persons should receive transparent information about the processing of their personal data. It also requires that "any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used".

424. Art. 12, GDPR, demands that information provided by the controller be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *in particular for any information addressed specifically to a child*" (emphasis added). This is reinforced by recital 58, which asserts that "any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand". This requirement is certainly linked to the right of the child to receive and impart information, enshrined in art. 13, CRC (Milkaite; Lievens, 2020, p. 9). Arts. 13 and 14, GDPR, further list the specific information that should be provided by controllers to data subjects.

425. In relation to children, the way information is provided is crucial for their understanding. Controllers should ensure that "the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognizes that the message/information is being directed at them" (WP29, 2018, parag. 14). Other means of conveying the information apart from text should also be used such as "diagrams, cartoons, graphics, video and audio content, […] gamified or interactive content […,] privacy dashboards, layered information, icons and symbols to aid children's understanding and to present the information in a child-friendly way" (ICO, 2020, p. 39).

426. It is essential to also consider the evolving capacities of the child, as the means to inform a younger child should be different from the ones used for teenagers. If many versions of the same information are available, controllers should make all of them "easily accessible and incorporate mechanisms to allow children or parents to choose which version they see, or to down-scale or up-scale the information depending on their individual level of understanding" (ICO, 2020, p. 40).

427. Lastly, it is important to highlight the limitations of providing information to data subjects, especially as a means to allow for more control, as previously discussed. If it is not fair to expect that data subjects understand such intricated processes involving their data, then

the primary burden for protecting personal data should not rest on their shoulders (Milkaite; Lievens, 2020, p. 18). In any scenario, maintaining transparency is of utmost importance, especially as a tool of fostering digital literacy for children.

6.1.5.2 Rectification and erasure

428. Art. 16 stipulates the right to rectification, including not only correction of inaccurate personal data, but also the right to have incomplete data completed. This reflects the principle of accuracy and grants data subjects with more control over the quality of their data (Terwangne, 2020b).

429. In its turn, art. 17 provides data subjects with the right to erasure ("right to be forgotten"), where specific grounds should be identified. Three of these grounds are related to the lack of basis for the processing (personal data are no longer necessary; consent had been withdrawn; personal data are unlawfully processed). The others demand erasure as a consequence of the right to object (art. 21), the compliance with a legal obligation, and the collection of data when the data subject was a child and consent has been given by the holder of parental responsibility (art. 8(1)).

430. Recital 65 emphasizes that the right to erasure is particularly important in cases where the data subject was a child when the consent had been given and was not fully aware of the risks associated with the processing. This right can be exercised even when the data subject reaches adulthood. Some scholars view the right to be forgotten as the most prominent empowering right in the GDPR (Macenaite, 2017), as it not only provides children with the right to remove information about them that could be damaging to their reputation but also information that is no longer relevant with the passage of time (Haley, 2020).

431. It must be recognized, however, that this right has several limitations. It only applies to the situations where consent was adopted as a legal basis—which is increasingly rarer— (unless other items in paragraph 1 apply), and the processing is not necessary for the purposes listed in paragraph 3. It remains a crucial right, though, particularly in cases where the child disagrees with the consent provided on their behalf and wishes to delete the data in the future, regardless of their reason. It is important to recall that while the holder of parental responsibility exercises this right on behalf of the child, the child remains the ultimate rights holder and should have the opportunity to reassess these decisions when they become capable of doing so.

432. Apart from art. 16 and 17, it is important to mention the more adjunct rights laid down in arts. 18 and 19. Art. 18 sets forth the right to the restriction of process, which permits the temporary limitation of processing until specific rights are granted, serving as a measure to hinder processing that would otherwise be deemed lawful (González Fuster, 2020). Art. 18 can then be used when the data subject claims that their data are not accurate, during the period in which the controller verifies the data; when the processing is unlawful, and instead of erasure, the data controller requests restriction; when the controller no longer needs the data for the intended purpose, but the data subject requests restriction in order to exercise or defend legal claims; and when the right to object has been exercised, during the period in which the analysis under art. 21(1) is conducted. Conversely, under art. 19, controllers need to notify data recipients with whom they have shared the data that a rectification, erasure or restriction of process has been carried out.

6.1.5.3 Right to data portability

433. Data portability is a very important right when it comes to changing schools. Laird and Quay-de la Valle (2019) note that student mobility is often associated with disengagement, increased dropout rates, and lower educational achievements. Challenges related to data portability could contribute to these issues. For instance, the absence or poor execution of data portability may lead to delayed student enrollment, incorrect class placement, discontinued special services (such as for students with disabilities) and lack of security (such as in cases of food allergies) (Laird; Quay-de la Vallee, 2019).

434. Although rooted in competition concerns, the right to data portability under the GDPR is also meant to empower data subjects. According to art. 20, individuals have the right to receive their personal data provided to the data controller (i.e., data knowingly and actively provided by the data subject or observed data) in a structured, commonly used, and machine-readable format.

435. The scope of this right is limited to data which are processed based on consent or contract, which, as previously observed, are used quite scarcely in the educational domain when it comes to public education. The situation differs in private schools, where a substantial portion of student data is processed based on the contract established between the two parties. Recital 68 and art. 20(3) emphasize that data portability will not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Nevertheless, WP29 guidelines on the matter

(endorsed in 2018 by the EDPB) suggests that it is a good practice. Data portability within the school environment is also very often regulated by specific laws in each EU MS.

436. Restricting data portability to data that are provided by the data subject can also be a challenge, especially when personalized learning activities are in place. The lack of context or insufficient data could hinder the right to education and lead to incorrect decisions. WP29 clarifies that data should be provided to the data subject along with relevant metadata at a suitable level of granularity to accurately describe the information's meaning and facilitate its function and reuse (WP29, 2017, p. 18). At the same time, oversharing information, especially without context, could enhance biased decision-making and create social stigma. For instance, a student with a history of disciplinary measures might face issues in the new school if the context that the issues were a result of persistent bullying is also not shared (Laird; Quay-de la Vallee, 2019, p. 8).

6.1.5.4 Right to object

437. Enshrined in art. 21, GDPR, the right to object refers to the data subject's ability to request that the processing activities stop according to his or her particular situation. Art. 21(1) lays down a more general right to object, which must be aligned with certain requirements, while art. 21(2) refers to an unconditional right to object when the data are processed for direct marketing.

438. The general right to object applies only when the data has been processed based on the necessity for a task in the public interest or in the exercise of official authority vested in the controller, or on the legitimate interests of the controller (art. 6(1)(e) and (f)). This is an particular right as it demands a balance test of its own (beyond the *ex-ante* balancing test performed when processing based on 6(1)(e), for example) and, therefore, is a manifestation of the fairness principle (Ausloos, 2017).

439. When data subjects object to the processing of data, they cannot be processed anymore, unless the controller has compelling legitimate grounds not to do so—i.e., grounds that overwhelmingly override the interests, rights, and freedoms of the data subject—or needs the data to exercise or defend legal claims. The burden of proof lies with the controller to assess the interests at stake and prove that their interest compellingly overrides the ones of the data subject.

440. Understanding what can be considered compelling legitimate grounds is crucial, since all processing based on art. 6(1)(f) already has to pass through a balancing test. If the legitimate interest merely overrides that of the data subject, there would not be a situation where the latter could object (Zanfir-Fortuna, 2020). When it comes to processing activities based on art. 6(1)(e), however, this stricter balancing exercise is not mandatory (although, of course, the principles of necessity and proportionality should always apply) and would need to be done if the data subject objects to the processing activity.

441. Regarding the burden of proof, it rests on both the controller and the data subject, albeit with the former bearing a more substantial responsibility. The accountability principle requires the controller to conduct a prior analysis of the appropriate legal basis before data processing begins. In the case of processing based on legitimate interests, a balancing exercise must be undertaken under the controller's burden of proof. However, if this analysis is challenged, the data subject is required to substantiate their claim (Ausloos, 2017).

442. Since these two legal bases are commonly used in educational settings for data processing related to teaching and learning, the right to object holds significant importance for children. Considering the unique circumstances of being a child in the digital environment, as elaborated in Chapter 4, it may already satisfy the condition of the data subject's "particular situation".

443. With regards to justifying the data processing based on legitimate interest, it can be argued that the principle of best interests would inherently elevate the standard in terms of the necessary balancing test, and the controller's interest would need to substantially outweigh the child's interest. However, this is not the case for art. 6(1)(e). Although the principle of the best interest should necessarily apply to all decisions concerning a child and, therefore, to the processing of their data, this specific right grants children a direct method to enforce it after the data processing has started.

444. Upon its application, it compels schools or other institutions that may process their data under art. 6(1)(e) to conduct a balancing test. This is endorsed by the Committee on the Rights of the Child (2021, parag. 72), which in its General Comment 25 states that children should be ensured the right to "object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing", especially when this could be seen as surveillance in the educational setting (parag. 75).

445. One example could involve the processing of personal data for the purpose of personalizing learning. Such processing could indeed be perceived as a way to uphold children's rights to education and lawful under the GDPR. Nevertheless, depending on the specific use case, if a child or their parents perceive that this process would encroach upon their right to privacy or non-discrimination, they could make use of the right to object to cease the processing. The school would, therefore, be required to conduct a balancing test and provide an alternative service if their legitimate grounds does not outweigh the rights of the child.

6.1.5.5 Automated individual decision-making

446. Art. 22, GDPR, gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similar significant effects on them. Unlike the DPD, this article includes not only profiling, but also other types of automated decisions. In practice, however, most types of automated decisions which fall under the scope of art. 22 will likely include profiling (Bygrave, 2020b). Although worded as a right, the WP29 was of the opinion that it establishes a general prohibition for decision-making based solely on automated processing in certain circumstances. This opinion was endorsed by the EDPB (EDPB, 2018) and very recently confirmed by the CJEU (European Union, 2023).

447. When it comes to profiling, art. 4(4), GDPR, defines it as encompassing two processes. First, it involves inferring the characteristics of an individual or group (creating a profile). Second, it involves interacting with that individual or group based on those attributes (employing the profile). The GDPR definition, however, narrows down this scope to automated processing of personal data (Bygrave, 2020a).

448. Recital 71, GDPR, provides details on automated decision-making based on profiling with legal or similarly significant effects and states, at the end, that this *should not concern a child*. At first, this could lead to the understanding that being a child, in itself, would be enough for decisions based solely on automated processing to meet the significant effects threshold (Bygrave, 2020b, p. 534). This means that human intervention should always be employed when dealing with children's data.

449. However, it could also mean that decisions based on automated processing concerning children could be carried out, as long as it does not produce any legal effects for or similarly significantly affects the child (Lievens; Verdoodt, 2018, p. 276). Given that the legislator likely included this phrase for a specific purpose, particularly considering that the rule already applies

to all data subjects, it is essential to analyze Recital 65 in its entirety and examine its interconnection with other recitals to gain a comprehensive understanding.

450. Regarding the structure of the recital itself, it first states that data subjects have the right not to be subject to a decision, which may include profiling, based solely on automated processing and which produces legal effects or similarly significantly affects them. After providing some examples and explaining the definition of profiling, the recital includes exemptions when this kind of decision-making is allowed and appropriate safeguards that should be implemented. Only then, it says that such measures should not concern a child. Therefore, this could be interpreted in a way that the exemptions would not be applicable to children.

451. Recital 38 also clarifies that a specific protection for children's data would, "in particular, apply to the use of personal data of children for the purposes of marketing or *creating personality or user profiles* and the collection of personal data with regard to children when using services offered directly to a child". This reinforces this second interpretation, as it foresees profiling as a possibility.

452. This second view is also supported by the Committee on the Rights of the Child (2021), which demands that states ensure that "automated processes of information filtering, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment" (para 61) or are used to affect or influence children's behavior or emotions or to limit their opportunities or development (para 62).

453. WP29 was of the opinion that this could not be interpreted as a prohibition because it is stated in a recital, which is not binding. However, it recommended that, "as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it" (WP29, 2016, p. 28). An exception would be when "solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children [… is used] to protect their welfare. If so, the processing may be carried out on the basis of the exceptions in Article 22(2)(a), (b) or (c) as appropriate" (WP29, 2016, p. 28).

454. In any scenario, one could argue that automated decisions based on profiling in the educational setting would indeed fall within the scope of what constitutes a legal or similarly significant effect. In terms of legal effects, it could hinder the right to education, when it is used for providing access to educational institutions or for assessing students. When it comes to

similarly significant effects, recital 71 mentions the example of e-recruting practices without human intervention, which could also use educational data.

455. WP29 (2016, p. 21) defines what can significant affect individuals as the decisions that have the potential to: "significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals". As described throughout this thesis, it can be argued that all these three situations could result from automated decisions based on profiling within the educational realm, which emphasizes the need for having human intervention at all times.

456. Specifically in relation to targeting advertisement, WP29 emphasized that "data controllers should not process children's data for behavioral advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing" (WP29, 2013, p. 26). The EDPB reiterated this idea in the endorsed guidelines on automated individual decision-making and profiling, stating that organizations should refrain from profiling children for marketing purposes (WP29, 2016). More recently, art. 28(2) of the DSA has introduced a prohibition on online platforms, barring them from displaying advertisements targeted at minors through profiling.

6.1.6 Data Protection Impact Assessment (DPIA)

457. Under the accountability principle, controllers are required to demonstrate compliance woththe GDPR, considering "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (art. 24(1), GDPR). For certain kinds of processing activities that are "likely to result in a high risk to the rights and freedoms of natural persons" (art. 35(1), GDPR), the GDPR mandates the undertaking of a DPIA.

458. The DPIA is "designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them" (WP29, 2017, p. 4). The operative text of the GDPR *per se* does not explicitly consider the processing of children's data as carrying a high risk (Hof; Lievens, 2018, p. 17). However, recital 75 explains that when personal data of vulnerable natural persons, such as children, are processed, this may result in risk to their rights and freedoms. WP29 also considered that the processing of data from vulnerable data subjects should be considered as one of the criteria

evaluated by the controller in order to determine if a DPIA should be undertaken "because of the increased power imbalance between the data subjects and the data controller" (WP29, 2017, p. 10).

459. It is also important to highlight the role of the principle of the best interest of the child as rule of procedure, that requires an evaluation of the positive or negative impacts of a decision on the child in every decision-making process that could affect them (Committee on the Rights of the Child, 2013a, parag. 6). Since several of the rights recognized by the CRC may be affected when processing children's data, it is crucial to perform a child rights-oriented DPIA (Hof; Lievens, 2018, p. 19) and leverage methodologies that already exist for CRIAs.

6.2 AI Act

460. At the time of completing this thesis, the EU Council and Parliament have reached an agreement on the AI Act (Council of the European Union, 2023a). As the final text is not yet available for analysis, I will use this section to provide a high-level overview of the fundamental ways in which the AI Act (European Union, 2021), as subjected to the analysis of the Committee of Permanent Representatives (COREPER) on 26 January 2024 (Council of the European Union, 2024), may impact the use of edtech. A thorough analysis of the impacts of the AI Act on edtech and on children's data protection will be essential once the final text becomes available, and this is intended to be carried out elsewhere.

461. The AI Act proposal was announced in April 2021 and aimed to be a technology-neutral, cross-cutting EU legislative instrument setting rules for the development, placing on the market, and use of AI products and services. The proposal was linked to many other policy and investment initiatives, such as the White Paper on Artificial Intelligence (European Commission, 2020d); the Communication on Fostering a European approach to Artificial Intelligence (European Commission, 2021b); the Coordinated Plan on AI (European Commission, 2021c); as well as the Horizon Europe and Digital Europe programs (European Commission, 2021a, n.p.). It is important to mention that the AI Liability Directive (European Commission, 2022b) is also intrinsically linked to the AI Act, but will not be discussed in this thesis.

462. Based on arts. 114 and 16 of the TFEU, the main purpose of the regulation is to ensure the harmonization and proper functioning of the single market, preventing fragmentation and providing legal certainty (recitals (1) and (2)). Recital 1 also emphasizes its aim to

> promote the uptake of human centric and trustworthy artificial intelligence while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy and rule of law and environmental protection, against harmful effects of artificial intelligence systems in the Union and to support innovation.

463. The regulation also supports the objective of the EU to become a global leader in the development of secure, trustworthy and ethical artificial intelligence.

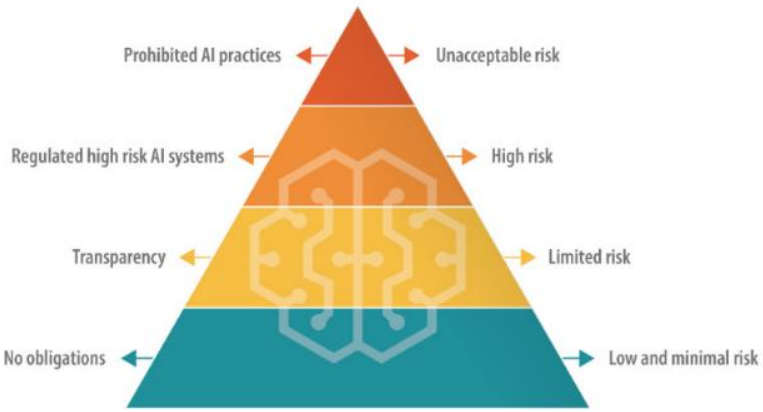
464. It applies to all AI systems impacting people in the EU, across all sectors, and contains certain extraterritorial measures affecting AI systems that impact people within the EU. The definition of AI system was aligned with the recently updated definition used by the OECD:

> [a]n AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

465. The AI Act adopts a tiered risk-based approach, whereby different obligations are defined according to the legal, economic and ethical risks that AI systems can pose to society. Recital 14a recalls, however, the 2019 Ethics Guidelines for Trustworthy AI and its seven non-binding ethical principles for AI, emphasizing their role in promoting trustworthy and ethically sound AI.

466. As shown in the figure below and explained in its recital 14, the AI Act distinguishes between a) unacceptable risk—which are banned—b) high risk—which are more heavily regulated by a new set of obligations—c) limited risk—which are subject to a set of transparency rules—and d) low or minimal risks—which could be freely developed and used in the EU. General-purpose AI (GPAI) systems follow a separate framework which will be discussed below.

Figure 3 - AI Act risk-based approach - pyramid of risks



Source: Madiega (2023, p. 4)

467. Title II establishes a list of prohibited AI, which includes practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness; exploit vulnerabilities of specific vulnerable groups, including due to their age, disability or a specific social or economic situation; and infer sensitive data through biometric categorization. More specifically related to edtech, it prohibits the use of AI systems to infer emotions in educational institutions, except when put in place or into the market for medical or safety reasons.

468. Title III lays down specific requirements for what is considered high-risk AI, which carries most of the compliance obligations within the AI Act. Instead of providing a definition of what is considered high risk, the AI Act provides a list of these systems in its art. 6 and Annexes II and III. The Commission retains the possibility of expanding this list in the future as long as some specific conditions are met. No explanation has been provided as to why these specific systems and not others are listed. Moreover, no analysis has been carried out to assess whether the high risks posed by these systems are necessary and proportionate according to art. 41, CFR.

469. Included in the lists are AI systems used as safety components or a product covered by EU harmonization legislation, such as medical devices, motor vehicles and civil aviation. Annex III also includes different contexts where AI systems are applied, posing significant risk of harm to health, safety, or fundamental rights.

470. Recital 28a explains that the adverse impacts caused by the AI system on the fundamental rights protected by the Charter are of particular relevance when classifying an AI system as high-risk. More specifically, the recital highlights that

> children have specific rights as enshrined in Article 24 of the EU Charter and in the UN Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being.

471. In this regard, two of the categories within Annex III are relevant to this thesis. First, it includes some AI systems used for education and vocational training, i.e., AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels; AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels; AI systems intended to be used for the purpose of assessing the appropriate level of education that individual will

receive or will be able to access, in the context of/within education and vocational training institution; and AI systems intended to be used for monitoring and detecting prohibited behavior of students during tests in the context of/within education and vocational training institutions.

472. Recital 35 explains that these systems should be considered high-risk because they

> may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood. When improperly designed and used, such systems may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination.

473. The comprehensiveness of AI systems mentioned under this category of Annex III is welcomed and would encompass most the technologies mentioned by this thesis.

474. In Annex III of the AI Act, another significant category of AI systems pertains to accessing and enjoying essential private services and public services and benefits, which could include educational services. While access to education is already covered by a specific category, the addition of the term "enjoyment" holds particular importance in the context of education. This inclusion encompasses systems such as student behavior monitoring and other edtech that could potentially impact the complete enjoyment of the right to education beyond monitoring and detecting prohibited behavior. Additionally, AI systems used in employment settings are pertinent, encompassing recruitment systems that may process personal data gathered during a child's school years.

475. There are some exceptions to this high-risk classification. AI systems will not be considered high-risk, based on art. 6(2a), if they are intended to perform a narrow procedural task; improve the result of a previously completed human activity; detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

476. In relation to the obligations established by the regulation for high-risk AI systems, art. 9 mandates the establishment of a risk management system, which should be understood as a continuous iterative process, planned and run throughout its entire lifecycle (art. 9, (2)). It must comprise a series of steps, such as identification and analysis of the known and reasonably foreseeable risks; estimation and evaluation of the risks that may emerge; evaluation of emerging risks based on post-market monitoring; and the adoption of appropriate and targeted risk management measures designed to address the risks identified in the previous steps. The risk management system should not only consist of documentation, but also of a testing phase

according to art. 9(5). Art. 9(8) also determines that when implementing the risk management system described in paragraphs 1 to 6, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

477. The risk management system is then at the core of the AI Act approach. The quality and comprehensiveness of the identification and classification of the risks will set the tone for the mitigation measures that will be implemented. The AI Act leaves, however, a lot of discretion to the AI provider in determining which measures must be taken to deal with the identified risks and at which point they are considered enough (Smuha *et al.*, 2021). According to art 9(4), the provider will have to determine what is a relevant residual risk and if the measures taken are enough to make them reasonably acceptable. The residual risks should be communicated to the deployer.

478. It is commendable that children's specificities have been included in this provision. However, considering their vulnerability, it does not seem appropriate for actors who will themselves face the consequences of enforcement to determine the required mitigation measures and what qualifies as an acceptable yet relevant risk. If a provider intends to introduce a product to the market or into service within the EU, it is unwise to assume that they could act in a way that might conflict with their commercial interests. At the very least, stakeholders who are subject to the AI system, particularly children who have the right to be heard, should be consulted about what level of risk may be considered acceptable (Smuha *et al.*, 2021). Children also have the fundamental right to have their interests taken into consideration in every decision that affects them, and we cannot be sure if this will be the case with this procedure, especially because the results would be only shared with the user (art. 9(4)).

479. General obligations related to high-risk AI systems include implementing appropriate data governance and management practices for training, validating and testing data sets to be used in AI systems. These practices must consider, for example, design choices and possible biases that can negatively impact fundamental rights or lead to prohibited discrimination. Data sets are also required to be sufficiently representative, free of errors, and take into account the geographical, contextual, behavioral or functional setting within which the system is intended to be used.

480. These are very important requirements to be considered when it comes to edtech, especially due to their capacity to limit children's opportunities in life. However, some challenges still remain in their application, especially due to the broad discretion that AI

providers enjoy, as explained above when faced with open expressions such as “appropriate” and “sufficiently representative”. Moreover, the provider is not necessarily in a good position to define the broader context in which the system will be deployed so it could be taken into account when gathering the data set. Since AI is an umbrella term for different technologies, context makes a tremendous difference in the risks they pose (Smuha, 2023b).

481. Other obligations include maintaining technical documentation and record-keeping; being transparent and providing information to users; enabling and conducting human oversight; and complying with standards for accuracy, robustness and cybersecurity. High-risk AI systems must also be as resilient as possible regarding errors, faults or inconsistencies.

482. Deployers of high-risk AI systems must also comply with certain obligations, such as carrying out a fundamental rights impact assessment (FRIA) if they are a public body or private entity providing public services; implementing human oversight; ensuring that input data is relevant to the use of the system, among others. This would be the case of schools, for example, that deploy AI systems for the purposes established in point 3 of Annex III.

483. Finally, for certain AI systems that are not prohibited nor considered high-risk, the AI Act establishes transparency obligations (Title IV). For example, AI systems intended to interact with natural persons should be designed and developed in such a way that people are informed that they are interacting with an AI system. Companies developing such systems are also invited to commit to codes of conduct on a voluntary basis.

484. When it comes to GPAI[18], the AI Act also adopts a tiered approach, differentiating between high-impact GPAI with systemic risk and other GPAI models. The latter should comply with limited transparency obligations, such as keeping up-to-date and making available, upon request, technical documentation, as well as providing certain information and documentation to downstream providers for the purpose of compliance with the AI Act. The former should also perform model evaluation; make risk assessments and take risk mitigation measures; ensure an adequate level of cybersecurity protection; and report serious incidents to the AI Office and national competent authorities.

[18] According to art. 3(44b) of the AI Act, “‘general-purpose AI model’ means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.”

485. The AI Act is expected to be approved by the European Parliament and the Council and published in the Official Journal in early 2024. The current agreement foresees a phased timeline for enforcement, starting with prohibited AI systems and progressively extending to other AI systems until 2028.

6.3 EU policy on digital education

486. According to art. 165, TFEU, the primary responsibility for education lies with EU MS, leaving the EU with only a supporting role. The Commission believes that education is the "foundation for personal fulfilment, employability and active, responsible citizenship" and "is essential to the vitality of European societies and economies" (European Commission, [*s. d.*], n.p.) A European Education Area would thus help MS develop education and training systems that are more resilient and inclusive (European Commission, [*s. d.*]).

487. At the 2017 Social Summit in Gothenburg, Sweden, European leaders first endorsed the idea to create a European Education Area (European Commission, [*s. d.*]). Between 2017 and 2020, the Commission has taken three important steps to lay down its vision for its establishment (Chircop, 2021).

488. First, in November 2017, it issued the Communication "Strengthening European Identity through Education and Culture" (European Commission, 2017c) as its contribution to the Summit. The Commission identifies several challenges in the areas of education and culture, including digitization, automation, artificial intelligence, as well as the future needs for specific skills and competences. Therefore, it sets out the vision of a European Education Area—building on the New Skills Agenda for Europe (European Commission, 2016a), as well as investing in Europe's youth initiatives (European Commission, 2016c, 2016b, 2017b, 2017a)—as a "driver for jobs, social fairness, active citizenship as well as a means to experience *European identity in all its diversity*" (European Commission, 2017c, n.p., emphasis in the original). The solutions identified by the Commission encompassed mutual recognition of diplomas, boosting the Erasmus+ program, defining benchmarks for digital competences and lifelong learning, and "prepare a new *Digital Education Action Plan* in order to *promote innovative, personalised and digital teaching methods* and technologies that will help improve learning outcomes" (European Commission, 2017c, n.p., emphasis in the original).

489. Two months after the Summit, in January 2018, the Commission launched three initiatives to improve key competences and digital skills of European citizens, and to promote

common values and pupils' awareness of the functioning of the EU (European Commission, 2018c). The proposals fed into the first European Education Summit. The initiatives included two Council Recommendations on key competences for lifelong learning (Council of the European Union, 2018a), and on common values, inclusive education and the European dimension of teaching (Council of the European Union, 2018b). A third initiative was the Digital Education Action Plan (DEAP)—which outlined ways to make better use of digital technology for teaching and learning; develop the digital competences and skills needed for living and working in an age of digital transformation; and improve education through better data analysis and foresight (European Commission, 2018b).

490. Another package of measures in 2018 was described by the Communication "Building a stronger Europe: the role of youth, education, and culture policies" (European Commission, 2018a). This communication highlighted that 44% of Europeans were still considered to have low or no digital skills and that more attention needed to be devoted to education, training and culture to unlock their full potential to support the European project (European Commission, 2018a, p. 2). The Commission then announced the Youth Strategy, the New European Agenda for Culture, and three proposals for Council Recommendations on "Mutual Recognition of Diplomas", improving the "Teaching and Learning of Languages" and on "High Quality Early Childhood Education and Care Systems".

491. Finally, a third communication of 2020 set out the vision to achieve the European Education Area by 2025 and presented more concrete steps to deliver it (European Commission, 2020c). It was followed by two Council resolutions in 2021 on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) (Council of the European Union, 2021a) and on the strategic framework's governance structure (Council of the European Union, 2021b).

492. As part of the European Education Area enabling framework, the first DEAP (2018-2020) was important in promoting cooperation and dialogue on digital education. However, due to its short duration and limited budget, the actions' full potential and expected impact could not be achieved, according to the Commission (Binder, 2023; European Commission, 2020a). A second DEAP (2021-2027) was then adopted in September 2020 (European Commission, 2020b) and, in comparison to the 2018-2020 action plan, this DEAP has a lengthier duration, lasting from 2021 to 2027 and a more expansive scope, as it also encompasses informal and non-formal education, based on a lifelong learning approach (Binder, 2023).

493. The plan understands that there are two aspects that need to be focused on when it comes to digital education. First, it is necessary to assess the deployment of the vast and growing array of digital technologies. Second, there is the need to equip learners with digital competences (knowledge, skills and attitudes). The priority areas set out by this DEAP are: 1) Fostering the development of a high-performing digital education ecosystem; and 2) Enhancing digital skills and competences for the digital transformation. The DEAP also highlights some guiding principles, which include that digital education should be high quality, and protect personal data and ethics (European Commission, 2020b).

494. The development of a high-performing digital education ecosystem has several layers, and they are reflected in the actions outlined under this area. A very important one involves ensuring proper access to internet connectivity and digital technology. On average, 5% of European children lack access to computers at home. Although this percentage may initially appear small (especially when compared to Brazilian children), significant disparities exist among MS. For example, while only 0.7% of Estonian children face this issue, the figure rises dramatically to 23.1% for Romanian children (Niestadt, 2022).

495. Action 4, therefore, help reduce these disparities by supporting Gigabit connectivity and 5G coverage in certain areas and action 5 aims at supporting teachers on developing their digital competences (Binder, 2023). Finally, the development of ethical guidelines on the use of AI and data in teaching and learning for educations was also part of the first area as per action 6.

496. The second area directly supports the Skills Agenda, as it establishes objectives related to the uptake of digital competences. It includes the creation of a common European Digital Skills Certificate (EDSC) and the uptake of the European Digital Competence Framework to include AI and data skills (Muraille, 2020).

497. The implementation of the DEAP is synergetic with several other EU initiatives. It supports the European Skills Agenda (European Commission, [*s. d.*]) by ensuring that 70% of 16 to 74-years-olds have at least basic digital skills by 2025. The European Year of Skills 2023 seeks to strengthen synergies between skills policies and EU initiatives on training, such as the DEAP and the European Education Area (European Parliament; Council of the European Union, 2023). When it comes to the 2030 digital compass and the Digital Decade policy program (European Commission, [*s. d.*]), the plan helps implementing the goal of a digitally skilled population and highly skilled digital professionals. It also supports the Commission's "A Europe fit for the digital age" (European Commission, [*s. d.*]) priority, contributes to the

Next Generation EU (NGEU) recovery instrument (European Commission, [*s. d.*]), and is related to the new European Strategy for a better internet for kids (BIK+).

498. Finally, it is also important to mention the development of a Data Spaces for Skills within the Data Strategy. In addition to foreseeing the issuing of new legislation such as the Data Governance Act (DGA) and the Data Act (DA), the Data Strategy also includes investment in common European data spaces in strategic sectors through the Digital Europe Programme. According to the Data Spaces Support Centre (DSSC) (2023, p. 6), a data space is "a distributed system defined by a governance framework, that enables trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and supports one or more use cases."

499. The Data Space for Skills would then be a framework for sharing data related to qualifications, learning opportunities, jobs and skills. The purposes for the data sharing include

> analytical and statistical purposes to policy development or reuse in innovative applications, as well as at providing easy, cross-border access to key datasets. The European skills data space will also aim to reduce the skills mismatches between education and training systems on the one hand and labour market needs on the other. Besides improving skills intelligence, this data space will deliver services to its users, with recommendations of learning opportunities to support their upskilling efforts, tailored to the information on their skills profiles (European Commission, 2022a, p. 32–33).

500. Considering the novelty of the concept of data spaces and the fact that they are still ill-defined, the full array of effects this may have on children's rights are still unknown. The benefits of a large amount of data "on the market" for fundamental rights are not adequately proven. However, it is already well-known that widespread data sharing can have serious consequences for protecting personal data and, consequently, other fundamental rights. The data strategy may be reinforcing a narrative of commodification of personal data which might contradict the main aim of the GDPR to protect fundamental rights. It could also affect children's rights not to be subject to economic exploitation.

501. The interplay and overlap between the data strategy and the new data regulation with the GDPR is also still not fully assessed, and new conflicts can arise while implementing them. An area of potential friction between the objectives of the strategy and the GDPR lies, for example, in the principles of purpose limitation and data minimization (Fernandes; Sas, 2023). While the goal of the creation of a data space is to make data available for further use, these principles should be, according to the WP29, interpreted more strictly when it comes to children (WP29, 2013).

Chapter 7. Brazil's relevant legal frameworks

502. Before the enactment of the LGPD (Brasil, 2018b))[19] in 2018, which marked Brazil's first data protection law, its legal framework contained some data protection rules scattered across various regulations. They were included, for instance, in the Internet Bill of Rights (Brasil, 2014), the Consumer Protection Code (Brasil, 1990), the Access to Public Information Law (Brasil, 2011a), the Civil Code (Brasil, 2022a), the Good Payer's Registry Law (Brasil, 2011b) and Interception of Telephone Communication Law (Brasil, 1996)**.**

503. This patchwork of legal frameworks proved insufficient to adequately safeguard the rights of data subjects. For many years, various stakeholders advocated for a comprehensive data protection law. The development of LGPD was significantly influenced by Convention 108 of the CoE, the DPD, and the GDPR. Similar to the GDPR, LGPD applies to both the public and private sectors, employs an ex-ante protection system, and emphasizes the accountability approach. It establishes a minimum set of principles and rights for data subjects, which must be adhered to in all personal data processing activities and requires a legal basis for data processing.

504. The enforcement of LGPD falls under the purview of the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados* – ANPD). Originally conceived as an independent body, the creation of this new agency in Brazil was deemed unconstitutional by the president of the republic at the time. The Presidency argued that only the executive branch had the authority to establish such an entity. Consequently, while the president sanctioned the LGPD, it vetoed the provisions related to the ANPD and immediately after issued Provisional Measure (Medida Provisória - MP) No. 869/2018[20], which positioned the ANPD as an entity subordinate to the Presidency of the Republic. This move eliminated the financial and political autonomy of the authority. The ANPD only began its operations in November 2020, following the appointment of its first directors.

505. In 2022, another MP altered the LGPD and transformed the ANPD into a "special nature autarchy" (Brasil, 2022b), granting it autonomy and independence in its decision-making and normative publications. More recently, a Presidential Decree linked the ANPD to the Brazilian

[19] For an English translation of the law, see Lemos *et al.* (2020).
[20] Transformed into Law n. 13.853/2019 (Brasil, 2019).

Ministry of Justice and Public Safety, thus ending its direct affiliation with the Presidency of the Republic (Brasil, 2023a).

506. The Brazilian Federal Constitution (*Constituição da República Federativa do Brasil* – CRFB) (Brasil, 1988) also contains significant provisions for the protection of personal data. It provides for the right to privacy in its art. 5º, X; the right to the secrecy of correspondence in its art. 5º, XII; and the *habeas-data* in art. 5º LXXII, a constitutional remedy that guarantees individuals the right to know whether a public entity is processing their data and, if necessary, the subsequent rectification.

507. Since 2020, data protection has been recognized as a fundamental right in Brazil, following a landmark decision by the Brazilian Supreme Federal Court (*Supremo Tribunal Federal* – STF). In 2022, the Constitution was amended to include the right to the protection of personal data as a fundamental right in the Brazilian legal order (art. 5º, LXXIX), separate from the right to privacy. This provision also grants an exclusive federal competence to organize, oversee and draft bills on the right to the protection of personal data and data processing.

7.1 The Brazilian General Data Protection Law (LGPD)

508. This section outlines specific issues that affect the processing of children's data according to the LGPD, particularly within the school environment. Due to the significant similarities between the GDPR and the LGPD, many of the comments made in the context of GDPR remain valid. Therefore, to avoid redundancy, I will strive to elaborate on the similarities and differences between the laws in each section and provide commentary only on the aspects that differ.

509. The LGPD is a horizontal law, applicable to both the public and private sectors. The exceptions for application are limited and provided for in its art. 4°. The law establishes the foundations and principles of personal data protection, an exhaustive list of applicable legal bases, important definitions, obligations for controllers and processors, as well as rights for data subjects.

7.1.1 General Principles for Data Processing

510. While the GDPR provides seven principles for data processing, the LGPD offers eleven. Apart from minor differences in the wording of the provisions, the principles contained in both

laws are purpose limitation; data minimization and storage limitation (both covered by the principle of necessity, in LGPD); accuracy (data quality, in LGPD); integrity and confidentiality (security, in LGPD); and accountability. The principle of lawfulness, fairness and transparency, in the GDPR, is encompassed by several other principles in LGPD, namely adequacy (compatibility of the processing with the purposes informed to the data subject, according to the context of the processing), prevention (adoption of measures to prevent harm due to the processing of personal data), good faith and transparency. LGPD also includes the principles of free access (which guarantees data subjects easy and free consultation regarding the form and duration of the data processing, as well as the completeness of their personal data), and non-discrimination (which prevents controllers of carrying out the data processing for illicit or abusive discriminatory purposes).

7.1.2 Art. 14, LGPD

511. The LGPD dedicates art. 14 to the processing of children's and adolescent's data. This provision is broader than art. 8, GDPR, and encompasses more rules than the ones relating to consent. Art. 14 states that children and adolescents' data must be processed in their best interests, pursuant to this article and specific legislation. The initial concern arising from the examination of this provision lies in the differentiation between children and adolescents. As a signatory to the CRC, Brazil should adopt a broad interpretation wherein the term "children" encompasses all individuals under the age of eighteen. However, the Child's and Adolescent's Statute (*Estatuto da Criança e do Adolescente* – ECA), which came into force in July 1990 and elaborates on art. 227, CRFB defines a child as an individual under the age of 12 and an adolescent as someone between the ages of 12 and 17.

512. Given the widespread use and recognition of the ECA's terminology, particularly within the legal field, the LGPD legislator decided to emphasize that data concerning adolescents should also be processed in accordance with their best interests. This differentiation becomes particularly pertinent when interpreting the paragraphs of this article, which establish specific rules for situations in which the data subject falls under the definition of a child according to the ECA, as elaborated below.

513. The CRC as a whole must be considered when interpreting any provision that affects the rights of children. However, emphasizing the importance of applying the principle of the best interests reinforces its critical role as a filter in any processing of personal data involving children and adolescents. While the article may not address all the issues arising from the

processing of their data in the digital environment, the inclusion of this principle directly in the provision has the potential to enhance the effectiveness of all the fundamental rights of this group (Henriques, 2023, p. 255).

514. Finally, the heading also mentions that processing children's data according to their best interest should take into consideration the other rules within its paragraphs, as well as in relevant legislation. This will certainly include any pertinent provision within the Brazilian legal system that may, in some way, affect this data processing. More specifically, this mainly includes the CRFB, the ECA, the CC and the CDC.

515. More specifically, the right to privacy is also recognized by art. 17, ECA, which provides that the right to respect consists of the inviolability of the physical, psychological, and moral integrity of the child or adolescent, including the preservation of image, identity, autonomy, values, ideas and beliefs, personal space and personal objects.

7.1.2.1 Children's consent and applicable legal bases for processing children's data

516. Art 14, §1º, LGPD states that children's data must be processed based on specific and explicit consent given by at least one of the parents or the legal representative. This rule should also be interpreted according to the broader Brazilian legal system.

517. The Brazilian CC presents two tiers of legal capacity. The so-called capacity of right can be considered a consequence of personality inherent to the condition of being a person (Menezes; Rodrigues; Bodin de Moraes, 2021). On the other hand, the capacity to act is linked to the ability to validly exercise civil life acts by oneself without the need for a representative or the consent of an assistant (Pereira; Lara; Rodrigues, 2023). The core of the capacity to act lies in the concept of discernment, through which capacity is measured by the efficiency of the outcomes of a person's choices (Menezes; Rodrigues; Bodin de Moraes, 2021).

518. Art. 3°, CC, defines individuals under 16 as absolutely incapable, which means that their will is disregarded by the legal system, and representation is necessary. On the other hand, art. 4°, CC, defines individuals aged 16 and 17 as relatively incapable. This means that these individuals can perform some acts directly, while they will need assistance for others (the incapable person participates in the civil life act jointly with their assistant). The child's representative or assistant are their parents (art. 1,690, CC) and in their absence a guardian appointed by a judge (art. 1,728, CC). Despite the recognition of the evolving capacities of the

child by the CRC, a static model purely based on age prevails in the Brazilian system as in many others around the world.

519. Over time, several other provisions have sought to mitigate the CC's rigidity, presenting exceptions to the general regime of civil incapacity, especially when personality rights are involved[21] (Teffé; Fernandes, 2022). As presented above, the LGPD uses the ECA terminology of children and adolescents and not that of the CC. This led some legal scholars to argue that the LGPD should be interpreted in light of the CC, and parents' consent should be sought for processing data of every person under 16 (Gomes & Zappelini, 2020; Henriques *et al.*, 2020). However, considering that the LGPD is subsequent to the CC and the existence of other exceptions in the Brazilian legal system, it is possible to argue that the legislator has indeed introduced a new exception via *lex specialis*, allowing individuals aged 12 and older to consent to the processing of their personal data without representation or assistance (Densa, 2023; Fernandes; Medon, 2021; Teffé, 2020).

520. Just as consent given for the processing of sensitive data, the consent for processing children's data referred to in art. 14, §1º, LGPD, must not only have the same characteristics as the consent given for common data within LGPD (being freely given, informed, and unambiguous) but also be specific and explicit. Although the legislator has allowed adolescents to consent without parental representation or assistance, these two extra safeguards do not appear to be applicable to them.

521. Just as art. 8(2), GDPR, art. 14, §5º, LGPD, demands that the controller make all reasonable efforts to verify that consent had been given by the child's parents or legal guardian, considering the available technology. Here, two challenges arise, namely, what is considered reasonable efforts and what constitutes the available technology. Both challenges could be addressed through a case-by-case risk approach. The level of effort and technology used should be balanced with the processing of data that requires consent as a legal basis and with the best interests of the child as a whole, analyzing its necessity and proportionality. For example, if only the name and email of a child are going to be processed, it is not proportionate to use facial recognition technologies to verify consent, as this would entail much greater risk than the

[21] For example, art. 1,740, III, of the CC, determines that it is the guardian's responsibility to fulfil other duties that normally fall to parents, after hearing the opinion of the child, if the child is already twelve years old or older; and art. 28, II, of the ECA, which determines the need for consent for adoption for people over twelve years old.

original processing activity. On the other hand, if the original activity is related to a child's health, for example, the threshold for verification should be higher.

522. It is important to mention that the provision of art. 14, §1º, has also raised several questions in relation to the legal bases applicable to the processing of children's data. Since it states that children's data must be processed based on specific and explicit consent given by at least one of the parents or legal guardians, many scholars would interpretate it as if consent was the only possible legal basis to process children's data.

523. This interpretation would be problematic for two main reasons. First, because art. 14, §3º, itself, as will be described below, provides two other legal bases for processing children's data for specific situations when consent could not be obtained. Second, this interpretation would not cover factual situations in which the best interest of the child needs to be enforced and where consent would not be applicable, such as in cases of legal obligation or when vital interests are at stake. Therefore, by using the best interest as an interpretative principle, it must be considered that other legal bases included in arts. 7º and 11 of the LGPD can and should be used (Fernandes, 2020).

524. In a preliminary study focused on the topic, the ANPD (2022a) also recognized many hurdles to implement a stricter interpretation. The DPA pointed out the illusion of control when consent is used in many cases; the excessive burden placed on parents or legal guardians; the impossibility of free consent in some instances (such as when there is a legal obligation to process data, as in education); the obstacle that it could create for children to have access to digital participation; the fact that parents are not always aware of all the risks for data processing; and the concern that it could be seen as creating a hierarchy between legal bases.

525. Art. 14, §3º stipulates that children's data can be collected without consent, when necessary to contact their parents or legal guardian (used only once and without storage) or for their protection. In neither of these two cases can the collected data be shared with a third party without parental consent. Thus, it is evident that these two specific legal grounds for processing children's data are reserved for highly specific and exceptional situations.

526. There is still no adequate and official understanding of what would constitute the protection of the child and the limits of the use of this legal basis. One possible way to interpret this basis would be to understand it in terms of "comprehensive protection", which is the object and scope of the ECA (art. 1). Considering that the ECA is the consolidation and elaboration of art. 227, CRFB, comprehensive protection could be understood as the duty of the Brazilian

State, the family, and society to promote all the rights of children and adolescents with absolute priority.

527. However, this interpretation would overly broaden the scope of art. 14, §3º, and this does not seem to have been the legislator's intention. It is possible to argue that the rule was formulated within a narrative of exceptionality. This becomes evident when considering that data to contact parents should only be used once and without storage or when, in both cases, data cannot be shared with third parties until consent is obtained (i.e. when the exceptional situation is remedied). Therefore, it is crucial to interpret this legal basis within the context of an extraordinary situation, encompassing protection against more immediate threats to the child's life and health.

528. Beyond the more restrictive interpretation of art. 14, §1º, as described above, another group of scholars argued that data concerning children and adolescents should be considered sensitive (Henriques *et al.*, 2020; Requião & Mendonça, 2023). It is important to highlight that, under the LGPD, sensitive data enjoy a special regime and a specific set of legal bases outlined in art. 11, which are different from the legal bases for the processing of general data found in art. 7º, LGPD. Unlike the GDPR, the bases provided in art. 11, LGPD are used on their own, without the need to combine them with a basis for processing common data.

529. Understanding children's and adolescents' data as sensitive data has the inherent advantage of automatically recognizing a stricter regime for the processing of this kind of data. However, Fernandes and Medon (2021) argue for the necessity of first considering whether all data concerning children can indeed be classified as sensitive before assessing the consequences of recognizing them as such and, more importantly, whether such classification is necessary.

530. First, the list of sensitive data includes specific categories of data and not of data subjects. In this regard, sensitive data includes, for example, those concerning racial or ethnic origin, religious beliefs, political opinions, etc., as per art. 5, II, LGPD. Therefore, the authors raise the question whether allowing children's vulnerability to justify treating all their data as sensitive, would not create the necessity of extending this understanding to the data of the elderly people and people with disabilities, for instance.

531. Secondly, the classification of data as sensitive is also tied to its potential for discrimination. However, a proper interpretation of the best interests principle has the potential to protect children's data much more broadly, as it demands comprehensive protection of children's rights, not solely limited to non-discrimination (Fernandes; Medon, 2021).

532. Lastly, this interpretation would hinder the possibility of creating an extra layer of protection for children's data that falls into the original classification of sensitive data, which could probably be considered "hypersensitive" (Fernandes; Medon, 2021; Teffé, 2021). In this regard, it seems evident that data concerning the religion, sexual orientation, and biometrics of these individuals, for example, should be protected even more rigorously than the same data concerning adults. Revisiting Luna's (2009) theory, we could identify two different layers of vulnerability, the one related to age and the one related to the processing of personal data which is potentially discriminatory.

533. Based on the issues described above, Fernandes and Medon (2021) suggest using children's best interests as an interpretative filter that should be applied *a priori* to determine which legal basis is appropriate to process children's data. In this regard, two legal bases could be seen as problematic: legitimate interest and credit protection (which will be further explained below). These are highly flexible legal grounds that may jeopardize, for example, the necessary transparency in assessing the best interest in each case. When it comes to legitimate interest, there is a need to balance rights in the specific case, which is done by the data controller. It would be the responsibility of the ANPD or the judiciary to conduct a *post hoc* analysis of the suitability of this legal basis, which increases the risk of violating children's fundamental rights. Regarding the legal basis for credit protection, it is evident that its purpose is strictly to protect financial interests, which may not align with the best interests of children.

534. This interpretation was adopted by two amendments to MP No. 1124/2022, which suggested transforming the ANPD into a special autonomous agency and initiated the process of independence for the authority (Mendonça; Rielli, 2022). The amendments were not included in the final text of the MP, and the situation was solved through an official interpretative statement by the ANPD.

535. In September 2022, the ANPD called for a public consultation regarding the possible legal grounds for the processing of children's data. In order to stimulate the discussion, the ANPD released a preliminary study (ANPD, 2022a), as previously mentioned, in which it recognizes three possible interpretations, disregarding the last one described above: (a) the application of consent as the only legal basis for processing children's data; (b) the application of the legal bases outlined in art. 11 to children's data; and (c) the possibility of applying all existing legal bases in the LGPD, as provided in arts. 7º and 11, depending on the data category.

536. In the study itself, the ANPD expressed a preference for the last hypothesis. This understanding remained unchanged even after several opposing positions from civil society and was released as an official Statement[22]. The same understanding was published in another Statement stemming from the IX Civil Law Conference[23], recognizing that art. 14 of the LGPD does not exclude the application of other legal bases, when applicable, as long as they observe children's best interests.

537. In the study, the ANPD highlights that even when more flexible legal bases are permitted to process children's data, they should be used with an additional layer of caution, considering children's vulnerability and the risks to their fundamental rights (ANPD, 2022a, parag. 64). This interpretation does not prevent the ANPD from establishing restrictions in the future related to the processing of children's data in specific situations, including with regard to the use of certain legal bases (ANPD, 2022a, parag. 73).

538. This was the case of the legal basis of legitimate interest, whose use was interpreted more restrictively by the authority in a specific guideline. According to the ANPD, legitimate interest should be used as a legal basis in a residual manner for the processing of data concerning children and adolescents in cases where there is: (i) a prior and direct relationship between the data subject and the controller, (ii) the processing aims to ensure the protection of the rights and interests of the involved child(ren) and/or adolescent(s), and (iii) when data processing is necessary to enable the provision of services that benefit the data subject (ANPD, 2024b).

7.1.2.2 Transparency obligations

539. Art. 14, §2º and §6º define specific transparency rules applicable to the processing of children's data. Art. 14, §2º states that when processing data related to art. 14, §1º, i.e., children's data processed based on parental consent, information about the types of data that are collected, how they are processed, and how the data subject rights in art. 18 can be exercised should be made public.

---

[22] A Statement (Enunciado, in Portuguese) is a type of deliberative instrument with the purpose of interpreting the LGPD, which has binding effects on the ANPD. The aim of issuing a Statement is to promote legal certainty in relation to controversial issues (ANPD, 2023).

23 The Civil Law Conferences are legal conferences held by the Brazilian Federal Judiciary with the aim of fostering debates among judges, scholars, and legal experts on unresolved issues in civil law and consolidating key doctrines through the formulation of statements that represent the majority of the members of each of the various committees (Aguiar Júnior, 2012; Conselho da Justiça Federal, [*s. d.*]). Although the statements are not binding, they are widely used as a reference by Brazilian authorities and the judiciary.

540. On the other hand, while the other paragraphs of art. 14 refer directly to art. 14, §1º, focusing on children as defined by the ECA, art. 14, §6º, applies to both children and adolescents since it refers to information about data processing mentioned in this article as a whole (which includes art. 14's heading on processing data in the best interest of children and adolescents). The information must be provided in a simple, clear, and accessible manner, taking into account the physical, motor, perceptual, sensorial, intellectual, and mental characteristics of the user. When appropriate, audiovisual resources should be used to ensure that the information is understandable for both parents or legal guardians and children.

541. This rule is of utmost importance within the context of the LGPD. Unlike the GDPR, the LGPD does not have a specific provision addressing transparency rules and mandatory information to be provided to data subjects. Art. 6º, VI establishes the principle of transparency, defining it as the guarantee of providing clear, accurate, and easily accessible information to data subjects about the data processing process and the controllers and processors of the data processing activity while respecting trade and industrial secrets. Therefore, art. 14, §6º, goes further and requires that the information provided about data processing be not only clear and accessible but also simple. Additionally, the controller must take into consideration the evolving capacities of the child and use other resources, such as audiovisual aids, to provide the information. This is especially important not only for children, as even when their parents or legal guardians consent on their behalf they are still considered the rights holders. It is also important for adolescents who may consent on their own according to the law and need information appropriate to their level of understanding and discernment.

7.1.2.3 Purpose limitation and data minimization requirements

542. Art. 14, §3°, stipulates that controllers are prohibited from making the participation of data subjects, as defined in art. 14, §1º (i.e., children according to the ECA), in games, internet applications, or other activities contingent upon the provision of personal information beyond what is strictly required for the activity. Its main objective is to discourage the "all or nothing" policies, where the user must either accept all the ToS or cannot use the application, which is common in standard form contracts (Teffé, 2020).

543. As previously mentioned, the LGPD includes in its art. 6º, III, the principle of necessity (i.e., data minimization), which, as defined by the law, entails restricting data processing to the minimum necessary, relevant, proportionate, and not excessive data required to achieve the

specified purposes. However, beyond reinforcing this principle, it is possible to argue that art. 14, §3º goes even further by using the expression "strictly necessary for the activity."

544. Therefore, merely mentioning other purposes in the ToS is not sufficient to collect data beyond the main purposes of the application. Indeed, the LGPD determines that the principle of necessity is closely linked to the principle of purpose limitation: as long as it is a legitimate purpose, it is sufficient to announce it transparently, find an appropriate legal basis, and process the necessary data for it. In the case of children, however, it is necessary to refrain from purposes unrelated to the basic functioning of the application (Fernandes; Medon, 2021).

545. As an example of the practical application of this rule, consider that for a child to create an account in a particular application, only the essential information for the running of the game should be required. In other words, data collection should be reserved for enabling gaming, and it would not be possible to process data, for instance, for targeting advertising (Fernandes; Medon, 2021). Similarly, edtech should not be used to economically exploit children's data for advertisement and for obtaining insights into children's economic behavior. Therefore, the personal data collected must strictly adhere to (i) what is indispensable and (ii) what is justifiable (Zanatta; Valente; Mendonça, 2021).

546. This is an extremely important rule within the scope of the LGPD, which protects children's data from the moment of collection and prevents them from being collected on a large scale for purposes unrelated to the main aim of the application or game in which the child is involved.

7.1.3 Other legal bases for processing children's data

547. To process common data, the LGPD provides 10 legal bases in its art. 7º, which is four more than the GDPR. It can be said that the legal bases of consent, performance of a contract, protection of vital interests, compliance with a legal obligation, and legitimate interest are essentially the same in both laws. The legal bases unique to the LGPD are: Conducting studies by a research body, ensuring, whenever possible, the anonymization of personal data; the regular exercise of rights in judicial, administrative, or arbitral proceedings; protection of health, in a procedure conducted by health professionals or health entities; and when necessary for "credit protection," such as in credit analyzes.

548. Furthermore, there is also a difference concerning the legal basis that can be used by public bodies. While the GDPR's legal basis is broader and includes the performance of a task

carried out in the public interest or in the exercise of official authority vested in the controller, art. 7º of the LGPD only includes processing carried out by the public administration for the execution of public policies provided for in laws and regulations or supported by contracts, agreements, or similar instruments. In a significant ruling in Brazil, the STF decided that the execution of public policies was the only permissible legal basis from art. 7º and 11 that could be used for the purpose of sharing data by the public administration. The court understood that specific provisions in Chapter IV of the LGPD would provide additional legal bases for the processing of personal data by the public sector. For instance, art. 23 of the LGPD would allow the processing of personal data for the execution of legal competences or attributions of public services.

549. However, a recent guideline published by the ANPD on data processing by the public sector establishes that any of the legal bases defined in the LGPD, whether in art. 7º or art. 11, can be used by the public sector. When it comes to consent and legitimate interest, the examples provided are related to activities that have no direct correlation with public functions. Beyond the legal basis of executing public policies, the ANPD has determined that the fulfilment of a legal or regulatory obligation is a relevant and applicable legal basis for data processing by public authorities.

550. As previously mentioned, unlike the GDPR, the LGPD does not mandate controllers to find a legal basis in art. 7 and art. 11 for processing sensitive data. Instead, the legal bases outlined in art. 11 are considered sufficient on their own. Besides some minor textual discrepancies, the one present only in the LGPD is to ensure the prevention of fraud and to promote the security of the data subject in the processes of identification and authentication of registration in electronic systems (art. 11, II, g). In the case of the GDPR, it also provides some legal bases that are not present in the LGPD, namely when processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body (art. 9(2)(d), GDPR); and where the processing relates to personal data which are manifestly made public by the data subject (art. 9(2)(e), GDPR).

551. When it comes to schools, the same general guidance in relation to which legal basis could be employed under the GDPR is also applicable to the LGPD. However, two specific issues must be highlighted. First, during the public discussions regarding the LGPD, there was great pressure for consent to be waived in cases related to credit risk analysis. Intense lobbying led to the inclusion of a specific legal basis for credit protection. The authorization brought by

this legal basis is extremely broad and does not require specific safeguards, as is the case with legitimate interest, for example.

552. Rhere is no precedent for this in other data protection legislation worldwide, and the ANPD has not yet issued any commentary on the topic. Consequently, there is no official guidance regarding the utilization of this legal basis for processing children's data. In its study on hypotheses for processing children and adolescents' data (ANPD, 2022a), the ANPD reinforced that, in its understanding, all the legal bases of art. 7 and 11 are possible to be used, but mentioned that there is a possibility that in future guidance, specific rules for the use of each basis will be defined. Thus, it is possible to use the best interests principle as an interpretative guide to preliminary state that since the primary aim of this legal basis is to protect financial interests, it should not be used to process data from children and adolescents in Brazil.

553. Second, the LGPD also provides for another legal basis not included in the GDPR when it comes to sensitive data, namely the prevention of fraud and to promote the security of the data subject, in the processes of identification and authentication of registration in electronic systems (art. 11, II, g, LGPD). This legal basis could be used, for example, to process biometric data for authentication purposes in the use of edtech. Given the great sensitivity of these data, especially when it comes to children and adolescents, an in-depth analysis of necessity and proportionality needs to be carried out in each case.

7.1.4 Data subjects' rights

554. The data subjects' rights in the LGPD are fairly consistent with the ones in the GDPR. However, there are some differences and, in general, the LGPD provides fewer details regarding their exercise, considering that most of them are outlined in a single provision (art. 18).

555. For example, in relation to the right to erasure, this can be invoked when data are no longer necessary for a specific purpose, are excessive or non-compliant with the LGPD. Data processed based on the consent of the data subject must also be erased upon request, except in cases where the data are necessary for compliance with a legal obligation; for a study by a research agency, ensuring, whenever possible, the anonymization of personal data; transfer to a third party; or exclusive use by the controller, provided that the data are anonymized.

556. Another difference is encountered in the right to object to data processing. In the LGPD, a general right to oppose to the processing only applies when there is non-compliance with the law and there is no right to object to direct marketing.

557. Regarding the right to data portability, the LGPD merely states that it must be exercised according to guidance issued by the ANPD, which has not yet been published. The regulation of data portability in the LGPD does not restrict its scope to the data provided by the data subject, nor does it limit itself to specific legal grounds or the processing of data through automated means (Negri; Korkmaz; Fernandes, 2021).

558. Finally, it is important to mention that the LGPD does not grant data subjects a general right to object to solely automated decision-making. Art. 20, LGPD, only stipulates that data subjects have the right to request a review of decisions made solely based on automated processing of personal data that affect their interests. This includes decisions aimed at defining their personal, professional, consumer, and credit profiles, as well as aspects of their personality. It is worth noting the challenges brought about by the amendment of the LGPD by Law 13.853 of 2019, which removed the legal requirement that the review must be carried out by a natural person (Negri; Korkmaz, 2021).

7.1.5 DPIA

559. The DPIA is described in the LGPD as the documentation from the controller that contains the description of the data processing activities that could generate risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms for risk mitigation (art. 5°, XVII, LGPD). While the GDPR specifies cases where a DPIA is required more clearly, the LGPD sets rules in a more scattered way.

560. The LGPD lists high-level situations in which the DPIA *may* be required by the ANPD, such as: in processing operations carried out for the exclusive purposes of public security, national defense, State security or investigation and prosecution of criminal offenses (art. 4, §3º); when the processing is based on the legal basis of legitimate interest (art. 10º, §3º); for public sector agents, including determination regarding the publication of the DPIA (art. 32); for processing involving sensitive data (art. 38).

561. While comprehensive guidance has not yet been issued, the ANPD specifies on its website that a DPIA must be conducted in any context where personal data processing operations may pose a high risk to the guarantee of the general principles of personal data protection outlined in the LGPD, as well as to civil liberties and fundamental rights of the data subject, in accordance with art. 5°, XVII, and art. 55-J, XIII, LGPD.

562. It also stipulates that controllers may, where appropriate, adopt as a parameter the concept of high-risk processing defined in art. 4° of the Application Regulation for small processing agents, approved by Resolution No. 2/2022 of the ANPD (2022b, 2023). This article includes the processing of data pertaining to children and adolescents as a scenario where high risk would be identified. This was also reaffirmed in a recent glossary developed by the authority (ANPD, 2024a).

563. In any case, assessing the impact of any decision on children's rights more broadly is already demanded by the principle of best interests itself. As already explained above, one of the aspects of this principle is its role as a rule of procedure, which demands that in any decision-making involving a child, a group of children or children in general, an assessment of its possible impact (positive or negative) on them should be carried out (Committee on the Rights of the Child, 2013a). In this sense, the evaluation must be used to explain how the best interests were considered in the decision, on what criteria it is based and how the best interests were weighed against other considerations (Fernandes; Medon, 2021).

7.2 The right to education

564. Art. 6, CRFB, guarantees the right to education, which is elaborated upon in arts. 205 *et seq*. According to arts. 205 and 206, CRFB education must be promoted and encouraged with the collaboration of society, aiming at the full development of the individual, their preparation for the exercise of citizenship, and their qualification for work. Its provision must follow basic principles such as equality of conditions for access to and permanence in school; freedom to learn, teach, research, and disseminate thought, art, and knowledge; pluralism of ideas and pedagogical concepts, and the coexistence of public and private educational institutions; the provision of free public education in official establishments; among others.

565. Primary education is free and compulsory for individuals aged four to seventeen. While the responsibilities for providing education are concurrent among the Union, states, and municipalities, the Constitution clearly defines the primary roles of each federative entity. The Union is tasked with organizing the federal and territorial education systems, funding federal public educational institutions, and serving a redistributive and supportive role through technical and financial assistance to the states, the Federal District, and the municipalities. The states and the Federal District oversee primary and secondary education, while municipalities

focus mainly on primary and early childhood education (as stipulated by art. 211, CFRB). The right to education is also guaranteed by ECA in its arts. 53 *et seq*.

566. The Guidelines and Bases of National Education (Lei de Diretrizes e Bases da Educação Nacional - LDB, 1996) is the primary legislative framework regulating both the public and private educational systems in Brazil, spanning from primary education to higher education. The law mandates that educational content, methodologies, and assessments must incorporate online activities to ensure that students grasp the scientific and technological principles underlying modern production (art. 35-A). Art. 80 also highlights the need to promote the development and dissemination of distance learning programs.

567. The Ministry of Education (*Ministério da Educação* - MEC) is the key Brazilian governmental agency responsible for formulating educational policies. At the federal level, the National Education Council **(***Conselho Nacional de Educação* - CNE) contributes to the development of educational policies. Additionally, Brazil is committed to promoting the right to education under the UDHR (art. 26), the CRC (arts. 28 and 29), and the ICESCR (art. 13).

7.3 The Brazilian Artificial Intelligence Bill

568. Just like in the case of the AI Act in Europe, this section aims to simply outline the debate regarding AI regulation in Brazil. The discussion below will mainly focus on the content of bill 2,338/2023, which is still undergoing legislative proceedings in the Brazilian Congress and is still subject to modification.

569. AI governance has been under discussion in Brazil for some time now. In April 2021, the Brazilian Artificial Intelligence Strategy (*Estratégia Brasileira de Inteligência Artificial* - EBIA) was published by the Ministry of Science, Technology, and Innovation (*Ministério da Ciência, Tecnologia e Inovação* - MCTI), establishing nine thematic axes for the development of AI in the country. However, the document was considered by many as vague, not delving into essential topics such as planning and governance (Gaspar; Mendonça, 2021).

570. Regarding legislative initiatives, noteworthy are bills 5,051/2019, 21/2020, and 872/2021, which were filed in parallel with policy initiatives. In February 2022, the president of the Brazilian Federal Senate established a Committee of Jurists responsible for writing a draft bill on artificial intelligence in Brazil. After 240 days of work, which included hearings and public consultations, the final report with the draft was published, intending to replace the

three bills mentioned above. In May 2023, the draft bill was converted into a bill, the 2,338/2023 (Brasil, 2023c).

571. Bill 2,338/2023 reinforces the idea that there is not necessarily a trade-off between protecting fundamental rights and promoting innovation, seeking to align a risk-based with a rights-based approach. Apart from stablishing rules for the development and deployment of AI systems in Brazil, it also encompasses rules for civil liability of AI systems.

572. In particular, art. 2° stands out for establishing the foundations on which AI should be developed and implemented, such as the centrality of the natural person, respect for human rights and democratic values, and the free development of personality. Art. 3° also enshrines basic principles, including self-determination, human participation, and non-discrimination. Chapter II contains various sections outlining the rights of individuals affected by AI systems, which apply horizontally to all cases. Of particular note is the extra attention accorded to vulnerable groups in art. 7°, §3°, which mandates that AI systems intended for their use must be developed in a manner that enables these individuals to comprehend their operations.

573. The bill also emphasizes the need to adapt the AI governance debate to the specific needs of the Brazilian reality (Bioni; Garrote; Guedes, 2023). The project acknowledges that asymmetries and structural inequalities permeate the country, and it includes, for example, definitions for direct and indirect discrimination derived from the Inter-American Convention against Racism. It also presents specific rules for the adoption of AI in the public sector, particularly in situations where individuals who are socioeconomically more vulnerable may be affected.

574. On the other hand, similarly to the AI Act, bill 2,338/2023 also contains specific rules that depend on the risk imposed by the AI system. This classification must be assessed by the AI system provider before placing it on the market or into service. Section II of Chapter III addresses AI systems that pose excessive risks and should be prohibited in the country. In comparison to the AI Act, the list is shorter, but the situations can be considered more comprehensive. In particular, emphasis is placed on the prohibition of the implementation and use of AI systems that exploit any vulnerabilities of specific groups of natural persons, such as children, in order to induce them to behave in a manner harmful to their health or safety, or contrary to the principles presented in art. 2° of the bill, including access to education (art. 2°, X).

575. Section III of the same Chapter addresses high-risk AI systems. Just like the AI Act Proposal, the Brazilian bill lists various categories of AI systems that may be considered high risk in its art. 17 and does not clearly define what can actually be regarded as high risk. Art. 18 determines that the competent authority can update this list based on a series of criteria, which include the impact on vulnerable groups. Within the list in art. 17, systems used for educational or professional training purposes stand out, including those that determine access to educational or professional training institutions or for assessing and monitoring students.

576. Art. 19 establishes governance structures and internal processes applicable to certain AI systems, such as transparency measures in the case of systems used in interaction with natural persons and for the mitigation of potential discriminatory biases. Apart from the requirements established in art. 19, high-risk AI systems must also comply with specific rules in arts. 20 and 22. They include conducting algorithmic impact assessments, keeping specific documentation, carrying out tests to assess reliability levels, establishing data management measures to mitigate and prevent discriminatory biases, and adopting technical measures to enable the explainability of the system's results.

7.4 Brazilian policy on digital education

577. The LDB states that distant learning can only be applied to primary education as a supplementary learning tool or in the case of an emergency (art. 32, §4º). With the COVID-19 pandemic, Law 14040/2020 (Brasil, 2020) was enacted to allow schools and higher education institutions to use online learning to meet the minimum workload required for their courses during the pandemic.

578. Regarding policies, the National Education Plan (*Plano Nacional de Educação* – PNE) was established by Law 13.005 in 2014, setting guidelines, goals, and strategies for educational policy from 2014 to 2024. Throughout the plan, several goals related to the implementation of ICT in education are mentioned, such as the development of pedagogical technologies that consider special education, rural schools, and indigenous and *quilombola* communities (Goals 2.6 and 5.4); the development and dissemination of educational technology, preferably open educational resources (Goals 5.3 and 7.12); and the promotion of full internet connectivity and access to computers in schools (Goals 7.20 and 7.22).

579. Goals 5.3 and 7.12 mention the need to give preference to free software and open education resources. In this vein, the MEC published Ordinance 451 (2018), which delineates

criteria and procedures for the production, evaluation, and distribution of open or free educational resources for primary and secondary education within official MEC programs and platforms. Art. 7º stipulates that educational resources created with financial support from the MEC for primary and secondary education must always be open educational resources.

580. It is also important to mention the Brazilian Strategy for Digital Transformation (Ministério da Ciência, 2018), which underlies the National System for Digital Transformation (*Sistema Nacional para a Transformação Digital*), established via Decree 9319, 2018 (Brasil, 2018a). This strategy extensively discusses open educational resources and highlights their potential to enhance access to quality education, thereby fostering innovative educational practices driven by digital culture (Amiel; Gonsales; Sebriam, 2018).

581. Also noteworthy is Commitment 6 of the 3rd Action Plan of the Open Government Partnership (2016-2018), co-created by the MEC and members of civil society, which aims to integrate the potential of digital culture into educational policy and to foster autonomy for use, reuse and adaptation of digital educational resources, valuing the plurality and diversity of Brazilian education (Ministério da Transparência, 2016).

582. Finally, in January 2023, the National Policy on Digital (Brasil, 2023b) was promulgated. The approach adopted by the policy is to coordinate programs, projects, and actions from different government levels to maximize the outcomes of related public policies. The PNED prioritizes actions aimed at the most vulnerable populations and is structured around four main pillars: digital inclusion; digital education in schools; digital training and specialization; and research and development (R&D) in ICT.

583. Regarding the digital inclusion pillar, the policy emphasizes various actions related to the development of digital skills, such as raising awareness, using tools for self-diagnosis of digital skills, training, developing platforms and repositories of resources, certifications, as well as the implementation and integration of connectivity infrastructure for educational purposes.

584. The pillar of digital education aims to integrate digital education into school environments, which encompasses acquiring knowledge about the digital world, computational thinking, digital culture, digital rights (including the protection of personal data), and assistive technology. In the pillar of Digital Training and Specialization, the twelve strategies are primarily geared towards higher education institutions and vocational education. The predominant aspect is the direct linkage of education to the demands of the workforce market.

585. Lastly, the R&D in ICT pillar aims to develop and promote accessible and inclusive ICT. This pillar lists six priority strategic actions, including fostering the development of low-cost ICT focused on education; promoting international partnerships; promoting open science and sharing digital resources among Scientific, Technological, and Innovation Institutions.

586. The LDB was also amended by the PNED to incorporate digital education and the provision of internet connectivity as part of the state's obligations concerning education in all public educational institutions (art. 4º, XII and sole paragraph).

587. The PNED will still be regulated by the federal Executive branch and does not have its own budgetary resources. It should be included in the multi-year national plan and in the budget laws in force until 2030 (Agência Senado, 2023). This means that the budgetary allocation for the PNED will have to compete with the already small portion of the education discretionary budget (the part not linked to mandatory expenses or programs whose funding sources are legally foreseen but allow for budget withholding or reallocation) (Seki; Venco, 2023).

588. Furthermore, the law also provides for state funds to finance actions related to the plan, such as the Telecommunications Services Universalization Fund (*Fundo de Universalização dos Serviços de Telecomunicações*), and the Fund for the Technological Development of Telecommunications (*Fundo para o Desenvolvimento Tecnológico das Telecomunicações*). Private entities will be able to enter into agreements with the public authorities for the implementation of the plan, in accordance with the regulation that will still be set by the executive branch (art. 11, sole paragraph).

589. The enactment of this law shows how the policy regarding digital education in Brazil has been shifting over the years, aligning with a more neoliberal approach. Several elements should be highlighted, such as the new state's spending cap, which reduces general public spending on education; the lack of inclusion in the law of specific budget for its implementation; its focus on promoting the use of "low-cost" digital technologies; and the encouragement of public-private partnerships. These elements demonstrate that a highly probable solution for the implementation of the plan regarding the digital technology infrastructure for education is the establishment of partnerships with foreign technology companies that offer their products for free or at a low cost due to their DDBM.

590. In the early 2010s, Brazil became internationally known for its strong engagement in the open educational resources community through laws and public policies that encouraged the use of licensed technologies in an open model in education and mandated public entities to

ensure that technologies developed with public funds were freely accessible (Amiel; Gonsales; Sebriam, 2018; Sebriam; Gonsales, 2017).

591. As will be discussed in the conclusion of this thesis, the focus on the development of open source technologies that consider local specificities is an interesting alternative to relying on big tech companies, which comes at a low cost but often at the expense of children's data protection. However, the coup d'état suffered in the country in 2016, the economic crisis, and the constant cuts in the education budget have made these policies increasingly hollow, which was further exacerbated by the COVID-19 pandemic. Without the necessary investment, it is more challenging to develop and procure sovereign technologies that are aligned with national interests and the best interests of children.

PART III. CHALLENGES INTRODUCED BY EDTECH TO CHILDREN'S RIGHTS TO PRIVACY AND TO THE PROTECTION OF PERSONAL DATA

592. This thesis asserts that, akin to all types of technology, it is imperative to maintain a critical and scientific perspective regarding both the opportunities edtech afford for humanity's advancement and the risks they entail. We have briefly seen in the introduction different ways in which edtech holds the potential to promote access to information, enhance accessibility—especially for children with disabilities—and optimize the efficacy and efficiency of learning. Nonetheless, apart from the absence of robust scientific evidence concerning the actual efficacy of the majority of current edtech in achieving their stated objectives, they may also be reinforcing problematic pedagogical practices (such as behaviorism and a learning-centric approach to education) and engendering adverse effects, such as the violation to children's rights to privacy and data protection.

593. Part III will use the research synthesized thus far to delineate the challenges introduced by edtech to these rights. Chapter 8 will concentrate on conducting a comprehensive mapping exercise of these challenges, divided into two main areas. The first part of the chapter will focus on horizontal challenges AI technologies pose, considering their prevalent role in contemporary edtech and data processing. The second part will delve into specific challenges introduced by three types of edtech included in the typology: personalized learning, student monitoring technologies, and learning analytics.

594. Chapters 9 through 11 will subsequently present a case study on the application of Google Workspace for Education in the EU and in Brazil to provide a concrete and more in-depth example of how children's fundamental rights can be at risk when using edtech. Chapter 9 focuses on understanding what Google Workspace for Education is, how it works, and what its role is within Google's business model. Chapter 10 discusses the implications of employing this technology to children's privacy and data protection in the EU and in Brazil. I will begin by analyzing decisions of authorities within the EU concerning this technology. This methodology was selected considering the audit and analysis capabilities of certain competent authorities, notably DPAs, allowing for a more in-depth understanding of the issues, which the mere assessment of ToS and Privacy Policies would not afford. This is also significant given the average data subject's inability to verify the validity of a company's claims within its policies.

595. Subsequently, I seek to understand the implementation of Google Workspace for Education in Brazil. The ANPD has not yet focused on the issues resulting from the application of this technology. Thus, in addition to a formal analysis of the ToS and Privacy Policies applicable to Google Workspace for Education in the country, secondary data obtained through a literature review were used for the assessment. This included research examining these documents in previous versions and also empirical research carried out via information requests to education secretariats in Brazil.

596. Finally, Chapter 11 undertakes a broader analysis drawing from the data collected in both jurisdictions to grasp the systematic operation of Google Workspace for Education through the lens of data colonialism. It also analyzes the extent to which the current data protection legal frameworks in the EU and in Brazil address these challenges.

Chapter 8. Mapping the challenges introduced by edtech

597. This chapter is dedicated to mapping the main challenges stemming from the use of data-driven edtech to children's rights to privacy and data protection. Considering that data processing predominantly occurs within AI systems nowadays, the first part of this chapter will concentrate on the overarching challenges presented by AI-powered edtech. Where possible, examples have been integrated into the text, supplemented by use cases in text boxes, to illustrate how these particular issues can be or have already been identified within edtech.

598. The second half of the chapter will focus on specific challenges related to three popular employed edtech, aligned with the typology developed in Chapter 1. We have discussed that technologies can be used for *providing education*—supporting educational institutions, teachers and learners—and for *learning about education*. Considering that many of the examples provided within the first part of the chapter pertain to technology that supports institutions (such as admissions or scholarship distribution algorithms), the second part of the chapter will focus on specific challenges brought about by personalized learning technologies (mainly focused on supporting students), student monitoring technologies (mainly focused on supporting teachers), and learning analytics (developed for learning about learning).

8.1 Datafication

599. As explained in Chapter 2, the measurement movement in education greatly benefited from the increased datafication enabled by digital ICT. Datafication can be understood as a way to put phenomena "in a quantified format so it can be tabulated and analyzed" (Mayer-Schönberger; Cukier, 2013, n.p.), which should not be conflated with digitalization—the process of converting analogue information into digital information. Data are "produced by abstracting the world into categories, measures and other representational forms—numbers, characters, symbols, images, sounds, electromagnetic waves, bits—that constitute the building blocks from which information and knowledge are created" (Kitchin, 2014, p. 1).

600. To capture something from the analogue world and transform it into digital data, it is necessary to measure and record it for analysis and value creation. Data are then often understood as the *representation* of a phenomenon2, but it can also be "implied (e.g., through an absence rather than presence) or derived (e.g., data that are produced from other data, such as percentage change over time calculated by comparing data from two time periods)" (Kitchin, 2014, p. 1).

601. With the increased possibility of dataifying new aspects of human life, the amount of data to be processed and evaluated by computers is enormous. Thus, the term big data started to be employed to refer to operations that "one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value […]" (Mayer-Schönberger; Cukier, 2013, n.p.). AI systems, in particular analytics, started to be used to make sense of these big datasets, which would be impossible for humans.

602. The software model that is built on these data has three main characteristics: mapping (i.e., it is a projection, it is based on an original—reality); reduction (i.e. it reflects only a relevant selection of the original's properties); and pragmatic (i.e. it is usable in place of the original for some purpose) (Kühne, 2005, p. 2). Indeed, a model is not a copy. Taking the development of a car as an example, if a copy is used in a crash test, a real test run would be performed, not a model simulation**.** Using a model has the advantage of being cheaper, but the drawback of often being inaccurate (Kühne, 2005, p. 3)**.** If what is being datafied is human behavior and social relations, this copying exercise can be even considered impossible due to their complexity, instability and unpredictability**.**

8.1.1 Reduction and abstraction

603. Since datafication presumes measuring and quantifying complex phenomena of reality, it naturally captures only what is possible to measure with the current state of technology. It also entails reducing these phenomena into something that can be shared, analyzed and stored. The software model merely offers a limited representation of reality, and the decision regarding which data to collect for a specific purpose rests with the software engineers (Selwyn; Gašević, 2020, p. 530). The inevitable consequence is that these representations can fail to capture granular details from reality and important points of contrast.

604. What cannot or is hard to be directly measured, either because of a lack of technology or because it is too expensive or time-consuming, can be alternatively translated into usable data by proxies. A proxy is a variable or set of variables used as a substitute or approximation for a variable that a data scientist would like to measure. Proxies work through correlations, which will be better explained in section 8.2, *infra*.

605. Learning, for example, is hard to objectively measure because of its inherent complexity. It entails a multidimensional individual and collective process, involving, i.a., cognitive, affective, behavioral, and social factors. Several proxies could be used to evaluate learning, such as correct answers (and number of attempts to reach it) on exams, competition rates of lessons, participation in discussion fora, engagement metrics like click rates or time spent on a specific content, self and peer assessments etc. In a digital test situation, for instance, "rapid response times, alongside declining test performance may be associated with disengagement and guessing" (Wise, 2020, as cited in Maddox, 2023, p. 6).

606. The reduction of aspects of reality is closely related to the concept of abstraction, which refers to the process of removing information from its original context to be aggregated and processed (Pangrazio *et al.*, 2022, p. 262). This means that other information previously available in its original context that could help make sense of the data is removed or not even considered significant (Pangrazio *et al.*, 2022, p. 263). Again, which data are removed is related to the decision of which data are important for the model, which depends on the purpose of the collection and the pragmatic feature of software models discussed above. That means that using the data in other contexts is challenging and can lead to unintended consequences.

607. Removing the context from the collected data is inherently related to the idea that *what* is more important than *why* (using correlation instead of causation, as explained below). Therefore, datafying and modelling human life, especially within the school environment, has

to be done very carefully and for very specific purposes. The purpose of the model directly influences the aspects of reality that are integrated and those that are excluded, making it very difficult to extrapolate this model to other situations. This creates a significant problem, for example, when the data production has as a final target its widespread sharing (such as in the development of "data products"), as there is a greater risk to misinterpreting the data in a different context.

608. Furthermore, we must consider the problem itself of quantifying education, as briefly discussed in Chapter 2. When it comes to education more broadly, certain aspects are simpler to quantify, such as learning content, leading edtech to prioritize these areas while overlooking crucial aspects that are not easy to measure, such as creativity, critical thinking, and social-emotional skills. This reduction of education to a mere compilation of skills and competences may result in decisions like narrowing the curriculum and favoring data sciences over humanities and the arts, given the greater difficulty in quantifying the latter (Holmes, 2023).

609. Within AI-driven edtech, students are also reduced to their digital twins, transformed into "calculable persons" who are assessed and evaluated based on their data (Lupton; Williamson, 2017, p. 787). Students are seen by AI systems as a model as well, which becomes a

> make-believe substitution which can then be used to inform how the teacher approaches that student, or how an algorithmically personalized learning program assigns her tasks. As such, the substitute profile built out of the data takes an active ontological role in shaping the 'real life' of the student—a process that could always have been done otherwise, with different real world results. The data play a part in 'making up' the student (Williamson, 2019, p. 217).

8.1.2 Data collection for AI systems operation

610. The current operation of AI systems relies on the access to and utilization of a tremendous amount of data. Data are essential for training AI systems, and subsequently, it plays a crucial role in maintaining its relevance and facilitating adaptation for specific situations such as through profiling.

611. The massive collection of personal data in itself can be considered problematic not only due to the heightened risk of data breaches but also the potential for increased surveillance. As demonstrated earlier, when technology mediates all human behaviors and interactions, facilitating data recording, it enables various uses such as drawing inferences, creating profiles, conducting experiments, and influencing behavior for commercial and political ends (Sartor, 2020). In essence, what is fundamentally at stake (a focal point of the theory of data

colonialism) is human and collective autonomy and flourishing. Having information about the entire society confers immense power upon the social quantification sector, which actually lacks democratic legitimacy.

612. Therefore, before discussing whether algorithms and datasets are fair, biased, or accurate, we should weigh the societal costs against the advantages of technology. We must deliberate on which systems merit development, who should oversee their creation, who holds the authority to determine their functions, what accountability mechanisms are necessary, and how individuals can participate in this process (Powles; Nissenbaum, 2018).

613. One example is data commodification and whether society deems data worthy of consideration as a tradable asset in the market, even in the absence of monetary exchange. This specific mindset surrounding of data, as we have seen in Chapter 3, creates market incentives to collect increasingly larger amounts of data and extend market's influence into more and more aspects of human life. This is exacerbated when issues related to the market dominance of big tech companies are discussed within a competition framework, as the solution often revolves around incentivizing data sharing and increasing the volume of data circulating in the market.

614. Apart from the massive collection of personal data in itself, we must also consider tha challenges posed by the data sources used for training algorithms. When it comes to the data source, data may be collected explicitly for the purpose of training algorithms, repurposed if previously collected in other contexts, or scraped from publicly available sources on the internet. Each of these scenarios presents specific challenges, including ensuring compliance with the appropriate legal basis according to regulations such as GDPR or LGPD, meeting transparency obligations, ensuring compatibility for further data processing, and upholding data subjects' rights (Solove, 2024). Data scraping is particularly problematic, as even when the personal data being extracted is accessible in the public internet, it remains governed by data protection laws. It, therefore, raises concerns related to transparency and appropriate legal bases for processing data.

615. Finally, another important challenge relates to the tension between training AI systems and complying with key principles of data protection laws, such purpose limitation and data minimization. These principles mean that only data necessary for specific purposes should be processed and this should be defined prior to the data collection. However, when data are collected for training AI systems, the exact purposes for processing them are often unforeseen by the AI developers. Considering that the GDPR and LGPD give more focus on establishing

rules for the collection of personal data (which serves as input for the inferences made by AI) rather than on the outputs of this process (Wachter, Mittelstadt, 2017), it becomes difficult to perform meaningful purpose limitation or data minimization for data used to train AI systems, especially when dealing with general purpose AI (Wolff *et al.*, 2023).

8.2 Data Generation

616. A second challenge related to AI systems is related to how they produce knowledge based on the data they are fed with, and data analytics plays an important part in this process. *Analytics* is a field of computer science that uses ML techniques through mathematical and statistical algorithms to find meaningful patterns in data and, thus, insights. Davenport (2014) distinguishes three phases in the analytics history. The initial era of analytics 1.0 started in 1954 in the USA and was characterized by small, structured and internal data sources. At this time, data was stored in large companies' warehouses or marts before analysis, and the analytical activity was mainly descriptive.

617. In the early 2000s, the exploitation of online data by companies such as Google, Yahoo! and eBay started the analytics 2.0 phase. Although in the beginning the analytical efforts were still mainly focused on internal and structured data, they started informing not only internal decisions but also customer-facing products and processes. Gradually, data began to be externally sourced, and the sets became either very large or unstructured, also being stored in parallel servers. That was the start of the so-called data-driven economy and the use of big data (Davenport, 2014).

618. Analytics 3.0 combines characteristics of the two previous eras. It is defined as the combination of "large and small volumes of data, internal and external sources, and structured and unstructured formats to yield new insights in predictive and prescriptive models" (Davenport, 2014).

619. Data analytics includes different technologies that can be clustered in many ways. It is not the intention of this thesis to present all the possible ways data analytics can be used and described, but some definitions are important for the discussions that will carried out. Based on the outcomes of the analysis, for instance, data analytics algorithms could be descriptive, which means that they try to understand data from the past and provide solutions to influence the future. On the other hand, it can also be predictive, meaning that it tries to understand the present situation to predict the future.

620. Data analytics algorithms can also be clustered by their purpose. Educational analytics, for example, are understood as the use of analytics in education, which can serve different goals. If the goal is to optimize learning, this could be tackled by learning analytics, which is often defined as "the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs" (Siemens *et al.*, 2011, p. 4). The technical, ethical and pedagogical dimensions are explicitly integrated in this domain (Laet *et al.*, 2018).

621. Academic analytics, in turn, uses learners, academic and institutional data to improve organizational processes, resource allocation, workflows and institutional measurement (Siemens *et al.*, 2011). It focuses on strategic policy decisions and on how learning and educational results can be improved. It concerns, for example, figures on study success and drop-out rates (Laet *et al.*, 2018). More recently, the concept of student analytics has also emerged, which primarily targets students themselves and study career counsellors. Its goal is to provide a personal and data-based student guidance by analyzing data factors for study behavior or success (Laet *et al.*, 2018).

622. Finally, educational data mining is yet another different technique for gaining insight into learners' activities. Unlike learning analytics, which "adopts a holistic framework seeking to understand systems in their full complexity […, educational data mining] adopts a reductionistic viewpoint by analyzing individual components, seeking for new patterns in data and modifying respective algorithms" (Papamitsiou; Economides, 2014).

623. It is important to highlight, however, that there are no clear boundaries among these concepts. Institutional strategies directly affect learning, and learning results affect how institutions make decisions. Similarly, through a topic modelling of abstract data from articles on learning analytics and educational data mining, Lemay *et al.* (2021, p. 8) state that the difference between the two topics seem to be more a matter of degree than kind:

> [b]oth fields were focused on student performance and learning platforms, and in modelling student behavior. [Learning analytics] papers focused more on student engagement, teaching tools, and social network analysis whereas [educational data mining] papers focused more on techniques and methods of data analysis.

624. As mentioned above, data analytics are used to recognize patterns or correlations among the data. After recognizing a pattern, the next step would be to extrapolate or deduce additional conclusions or predictions about causality based on the observed correlation. Therefore, this process does not adhere to classical scientific methodologies focused on identifying causation; instead, it relies on methods aimed at uncovering correlations.

625. “[A] correlation quantifies the statistical relationship between two data values. A strong correlation means that when one of the data values changes, the other is highly likely to change as well” (Mayer-Schönberger; Cukier, 2013, n.p.). With correlations there is never certainty, only probability. Statisticians will often choose a proxy and run a correlation analysis to discover how strong the proxy is. In order to first choose a proxy, they could use hypotheses based on theories, i.e., abstract ideas about how a phenomenon works. If they fail, the hypothesis or the theory it was based on needs to be revisited (Mayer-Schönberger; Cukier, 2013, n.p.).

626. It is also possible to use data mining, i.e. unsupervised/bottom-up data mining algorithms that are designed to identify relationships among data points without developing initial hypotheses. These algorithms do not rely on training data or predefined solutions (Hildebrandt, 2015, p. 24), and the patterns “discovered” by the algorithms can reveal specificities of certain groups. This has important implications, especially for vulnerable people. An interesting example provided by Barocas and Selbst (2016, p. 691) in the context of employment can also be translated to the context of education. By providing more attention and opportunities to employees who are predicted to excel in a task, employers might unintentionally treat members of certain groups unfairly. This happens because the qualities that make employees attractive can be less common in these groups.

627. The focus on correlation instead of causation can also directly impact decisions made about students. For example, students who excel academically often allocate more time to the library or actively participate in the LMS. These behaviors can be associated with diligent studying, as high-achieving students typically engage in extensive preparation. However, encouraging other students to increase their LMS usage or time spent in the library, for instance, might not necessarily result in enhanced academic performance. Similarly, some of the outcomes generated by the data can be interpreted in different ways. If the algorithm identifies, for example, that students do not strictly adhere to the course schedule, with some studying ahead and others slightly behind the calendar, this can be understood at the same time as a problem or as an integral aspect of the adaptable and inclusive curriculum design (Weller, 2020, p. 145–146).

628. Understanding the reasons why some patterns exist is, in the case of big data analytics, often an afterthought. According to Mayer-Schönberger *et al.* (2013, n.p.), it is easy to get

> caught in a web of competing causal hypotheses. But our attempts to illuminate things this way only make them cloudier. Correlations exist; we can show them

> mathematically. We can't easily do the same for causal links. So we would do well to hold off from trying to explain the reason behind the correlations: the why instead of the what. […] [B]ig data itself aids causal inquiries as it guides experts toward likely causes to investigate [and i]n many cases, the deeper search for causality will take place after big data has done its work.

629. The instrumentalized "knowledge" generated by big data analytics can be seen, therefore, as representing a reversal of the values associated with the ideals of rationality and scientific inquiry (Kohl, 2021, p. 14). Subject matter expertise and domain-specific knowledge start to lose their significance, leading to a shift where computer and data scientists, rather than professionals like physicians, biologists, or sociologists, are increasingly seen as the primary protagonists (Rieder; Simon, 2017, p. 90).

630. It also directly affects the rights to privacy and to the protection of personal data by creating new data about people through inferences. These inferences, which include profiling and making predictions, often inform decisions that can directly impact people's fundamental rights. The issues surrounding decision-making based on inferences will be explored further in subsection 8.3. However, it is first important to map the challenges related to generating new data itself, such as the presence of bias in the training data or design of the algorithmic code, as well as the lack of control of one's personal data.

8.2.1 Bias

631. Bias can manifest in various forms within AI systems, and given that data is sourced from society, where human bias abounds, it is difficult to think of a dataset without it. Data used to feed the system may be incorrect, partial or nonrepresentative, meaning that certain people or groups could be disadvantaged when decisions are based on these data (Barocas; Selbst, 2016). Prejudice could have played a role as valid examples to learn from, and the system will reproduce them.

632. Second, bias can also be imbued in the choices made by data scientists, either in the selection of the data that are included in the model, or in designing the algorithm code itself. The data that is left out of the analysis "is particularly problematic in educational datafication, since many of the issues that schools face have origins in structural inequalities that are not captured by, or considered in, data about student learning or teacher effectiveness" (Pangrazio *et al.*, 2022, p. 263).

633. Apart from defining which data to collect or not, the labelling process of the data by data miners or even users can also include bias in the system. Even when an AI model is "ready"

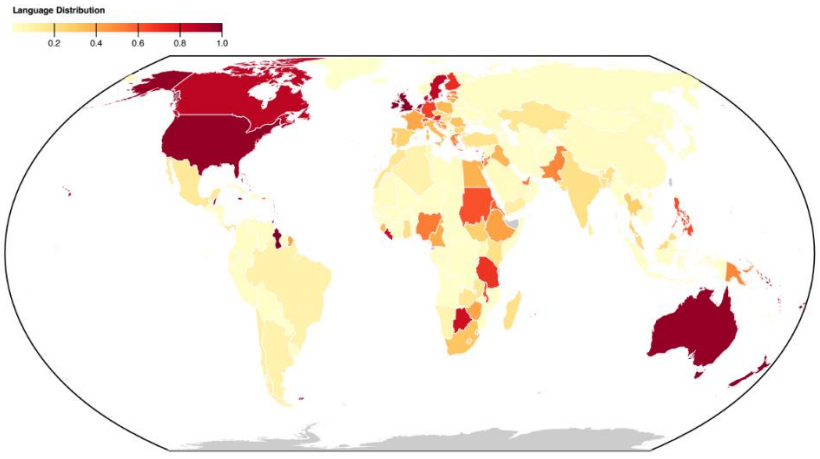
it can continue learning with the user's behavior, which means that the prejudices and users' biased behaviors will also influence it (Barocas; Selbst, 2016, p. 682). In this sense, O'Neil (2016) argues that the choices made by data scientists are not just about logistics, profits, and efficiency but are fundamentally moral.

634. When it comes to the algorithm code, it can also be biased depending on how the data scientist designed it. For example, in a globalized world, edtech gets exported and used in contexts completely different from the ones where they have been developed. The constraints of a technology will be aligned with the ones of its designers, who are usually based on developed western countries (Pinkwart, 2016, as cited in Miao *et al.*, 2021). If the designers are a homogeneous group of people with the same background and worldview, this will often create bias and injustices, as they are less familiar with the educational necessities of other regions.

> EdTech is neither 'borderless, gender-blind, race-blind or class-blind'. The framing of the curriculum, as well as automated delivery in the mode that brooks no discussion, marginalizes the knowledge of students—both indigenous and experiential—and reinforces existing epistemic injustices (Sarwar, 2022, n.p.).

635. One illustrative example is the dominance of the English language, which is frequently mandatory to participate in the digital environment. A recent research by Longpre *et al.* (2023) has developed a heatmap (reproduced below), which illustrates the extent to which the spoken languages of each country are reflected in the composition of natural language processing (NLP) datasets. It indicates that English-speaking and Western European nations are better represented when compared to other countries around the world.

Figure 4 - Global heatmap measuring how well each country's spoken languages are represented by the composition of natural language datasets



Source : Longpre *et al.* (2023, p. 12)

636. Within NLP, “coloniality can be connected to unstructured data, annotations, models and software. […] In turn, these technologies reinforce and amplify coloniality beyond the social systems that created them” (Held *et al.*, 2023, p. 1–2). This limits and shapes a student’s experience, even when the content itself is translated, as language is intrinsically attached to a specific culture and epistemology. This dominance can also hinder digital literacy, an important factor for an efficient edtech (Sarwar, 2022, n.p.). Algorithms focused on personalized learning are also frequently biased towards “high income countries’ cultures and languages, which can result in a reinforcement of cultural hegemony and a suppression of local languages and cultures” (Holmes, 2023, p. 66).

637. Finally, it is important to mention that discrimination does not only occur when traits that are traditionally defined as potentially discriminatory are taken into account (such as data considered to be sensitive). Algorithms can also introduce new forms of discrimination that were not previously anticipated (Solove, 2024). For instance, if an algorithm establishes a random correlation between a person’s dominant hand and their academic performance, new types of discrimination may arise.

638. When it comes to edtech that aims to help educational institutions, one popular application is aiding in the student admissions process. In this context, an early and significant example of its adoption can shed light on the existence of bias in the training data, which is described in Table 2 below.

Table 2 - Franglen’s Admissions Algorithm

639. From 1982 to 1986, St George’s Hospital Medical School used a program to automate part of their admissions process. The algorithm was developed in the 1970s by St. George’s vice dean Dr. Geoffrey Franglen, with the main motivation being to make the process more efficient and fairer because students would be subject to the same evaluation. After a double-test by human assessors and the program in 1979, the latter proved to be aligned with the panel’s decision 90-95% of the time, and was put to use (McGregor, [s. d.]; Schwartz, 2019).

640. However, some lecturers recognized the lack of diversity among students and decided to conduct an internal review of the program. They concluded that irrelevant factors such as name and place of birth were being considered by the system, discriminating against women and people of color. The case was brought before the United Kingdom (UK) Commission for Racial Equality, which found the school guilty of discrimination. It identified that the biases

already existed in the admissions process, with the algorithms merely learning from biased examples (Schwartz, 2019).

8.2.2 The challenge of controlling inferences based on personal data

641. As described in section 8.2, new knowledge generated by algorithms can take the shape of inferences, which, when made about people, can interfere in their rights to privacy and to the protection of personal data. Inferences can be drawn about basically any human attribute, state or behavior, including political opinion, emotional state, sexual orientation, shopping preferences, socioeconomic status, cultural background, dietary preferences, medical conditions, and location. Within the educational environment, inferences can be related to a student's attention and engagement levels, academic performance and potential for success, learning disabilities, study habits, attendance patterns, personality traits, etc.

642. The operation of big data analytics presents a formidable challenge in discerning how data has been used to produce new information, directly affecting the control over one's personal data (Solow-Niederman, 2022, p. 361). This is tied to epistemic limitations of algorithms, i.e., constraints or shortcomings in the way they produce knowledge or "understand" a particular subject or phenomenon. Mittelstadt *et al.* (2016) propose three main epistemic limitations arising from the use of algorithms: i) inconclusive evidence, which underscores the probabilistic yet uncertain nature of knowledge derived from inferential statistics; ii) inscrutable evidence, which refers to the lack of clarity regarding how the different data points contributed to the generated conclusion; and iii) misguided evidence, which highlights the notion that he reliability of conclusions is contingent upon the quality of the input data.

643. From the individual's perspective, whether data was collected or produced by the algorithm is irrelevant; the ultimate outcome remains that new information about them has been produced that they might not have anticipated and might be used to make decisions that affect them. It can also uncover details that people do not intend to reveal or make wrong assumptions about them (Solove, 2024). Data is speaking on behalf of people, posing risks to the rights to their privacy, identity, development of personality, freedom of expression, reputation and self-determination.

These inferences, especially when people are not aware of them, persist over time and affect future opportunities and equal treatment (Mittelstadt, 2017), which can particularly affect

children. The procedural approach of data protection laws have generally not been able to deal in a comprehensive way with these kind of challenges, as controllers are not obliged to disclose or justify the criteria and methods used to draw inferences. This led Wachter and Mittelstadt (2019) to argue, for instance, for a right to reasonable inferences as an accountability mechanism, which would offer additional protection against inferences that can cause reputational damage, violate privacy, or have low verifiability.

Table 3 - Inferring pupils' attention through brain waves

644. In 2019, some schools in China made headlines worldwide for implementing devices that monitored pupils' brainwaves. These headbands, provided by the company BrainCo, would sit across the students' forehead to infer their attention and was similar to devices used for detecting brain waves of patients in hospitals for medical assessments. They claim to be able to inform teachers and parents about how focused students are on their studies by detecting their brain signals—with different colored lights displaying the students' varying levels of concentration (Standaert, 2019).

645. While many parents and teachers see them as tools to improve grades, negative reactions from the public led the school to halt the experiment (Savillo, 2019). This case illustrates the expanding breadth of inferences that can be (allegedly) drawn from human beings, extending to the realm of human cognition.

8.3 Decision-making

646. After collecting the data, finding patterns, and creating new data, AI systems can be used to make automated decisions or aid in the human decision-making process. Automating decisions is often seen as a solution to streamline administrative tasks and help educators focus on more important issues, with the "bonus" of "remov[ing] politics and ideology from decisions" (Schildkamp; Kuin Lai, 2013, p. 2).

647. Nevertheless, students' lives can be profoundly impacted by decisions made based on data-driven technologies, particularly AI systems, potentially limiting their future opportunities (Jarke; Macgilchrist, 2021, p. 3). This section will concentrate on the primary challenges posed by the deployment of big data and AI systems to either automate decision-making or assist educators in making decisions regarding students. It will delve into specific types of inferences and the decisions based on them, such as profiling and future predictions, as well as scenarios

where the human element directly intersects with the challenges posed by technology. Furthermore, it will address special situations where edtech is employed based on the typology adopted in Chapter 1.

8.3.1 Profiling

648. One way to infer data about people and make decisions based is to use profiling techniques. Algorithms use personal data and big data to analyze individuals' past preferences, behaviors, networks, and activities to create a profile of who they *were*. This information is used to infer their behavior, what may persuade them, such as a specific movie or advertisement, or their future actions and likes (inferences related to the future, i.e., predictions, will be dealt separately in the next subsection). As already explained above, profiling occurs when 1) a set of aspects about a person or group is inferred (a profile is created), and 2) the person or group is targeted based on these aspects (the profile is applied) (Bygrave, 2020a). Profiling raises concerns because of its very nature, as it involves "the pre-selection and pre-emption of individual choices by those who have access to big data sets and profiling technology" (Kohl, 2021, p. 5).

649. Although it may sound as if the individual is the focus, individual profiling involves classifying a person based on group attributes, which are used to place them into a specific micro-category (Kohl, 2021, p. 7). Cohen (2019, p. 69) argues that calling the process individualization is not entirely accurate. Individuals are probabilistically defined based on their past actions and undergo a process of rather singularization. Individuals are not adjusted to their unique characteristics by the profiler; instead, after providing some initial data, they are conformed to the profiler's standardized patterns (Kohl, 2021, p. 19).

650. In order to further unpack this process, it is first important to understand what "target variables" and "class labels" are within the data science language. Data analysis is a very broad that encompasses many different ways of understanding data. Simple forms of data analytics can produce records or summary statistics. Data mining, however, aims at locating statistical relationships, or patterns, in a dataset. "The accumulated set of discovered relationships is commonly called a 'model,' and these models can be employed to automate the process of classifying entities or activities of interest, estimating the value of unobserved variables, or predicting future outcomes" (Barocas; Selbst, 2016, p. 677). This is the process of finding correlations, as previously discussed. These qualities of interest are called *target variables* (i.e.,

what data miners are looking for), while the mutually exclusive categories that divide these outcomes are called *class labels* (Barocas; Selbst, 2016).

651. Translating a problem from reality to a question about the value of some target variable so that a computer can understand it is a very subjective process and it is possible to occur in a way that disadvantages specific individuals or groups. When the categories the algorithm is looking into are not mostly uncontroversial (such as what is fraud or spam), they will always involve a value judgment (Barocas; Selbst, 2016).

652. Take, for example, the analysis of student excellence for admission to a university in a scenario where admission tests are not possible, as in the case of the COVID-19 pandemic. Calculating a student's grade can be carried out in several ways, such as through school records, curriculum, motivation, teacher recommendations, averages of similar students from the school they attended in previous years, evaluation of activities in the current year, etc. What is excellent, then, will be defined in ways that can be measured, but all of these options are just part of an almost infinite number of possible definitions of excellence.

653. The choice made can then have different impacts on different individuals or groups. In this sense, "[w]hile critics of data mining have tended to focus on inaccurate classifications (false positives and false negatives), as much—if not more—danger resides in the definition of the class label itself and the subsequent labeling of examples from which rules are inferred" (Barocas; Selbst, 2016, p. 680).

654. Therefore, the distinction between the individual and the group is likely to be misunderstood as they constantly and mutually influence each other: "[i]ndividual data feeds into population data sets and these sets produce, through correlations, knowledge about populations, that is patterns and groups within them (inductive), which in turn are instructive about the individual (deductive)" (Kohl, 2021, p. 8). The deductive process is related to distributive profiles (or universal generalizations), when the attributes are shared by all the members of the group (for example, in the category bachelor, all people share the fact that they are not married). On the other hand, non-distributive profiles "are framed in terms of probabilities and averages and medians, or significant deviances from other groups. They are based on comparisons of members of the group with each other and/or on comparisons of one particular group with other groups." (Vedder, 1999, p. 277).

655. However, distributive profiles may also be understood in comparison with other groups when it comes to what they are *not* (e.g., the group *university staff* can be compared with *police*

or *hospital staff*). This blurs the boundaries between the different types of profiles, and the certainty associated with distributive profiles becomes illusory (Kohl, 2021, p. 8). Ultimately, they can be considered as two different ways of looking at the same group or constructing groups.

656. When it comes to profiling and comparisons to group data, one frequent objection is the process of stereotyping, which occurs when people are evaluated or treated based on their membership in a particular group rather than recognizing their unique qualities and achievements as individuals. Take, for example, the use of academic credentials in hiring decisions. Employers

> tend to assign enormous weight to the reputation of the college or university from which an applicant has graduated, even though such reputations may communicate very little about the applicant's job-related skills and competencies. If equally competent members of protected classes happen to graduate from these colleges or universities at disproportionately low rates, decisions that turn on the credentials conferred by these schools, rather than some set of more specific qualities that more accurately sort individuals, will incorrectly and systematically discount these individuals. Even if employers have a rational incentive to look beyond credentials and focus on criteria that allow for more precise and more accurate determinations, they may continue to favor credentials because they communicate pertinent information at no cost to the employer (Barocas; Selbst, 2016, p. 689).

657. This indirect profiling is opposed to direct profiling, which is based on data only about individuals themselves and is sometimes understood as a better way to profile individuals (Kohl, 2021, p. 10). However, arguing that direct profiling is more legitimate assumes that a person's past actions and preferences can accurately predict their future behavior and preferences. This perspective also implies that a person's identity is fixed over time. Direct profiling, like indirect profiling, is also inherently comparative and thus involves the social aspect of human life. Understanding individuality requires comparing it to a presumed "normality" that provides a context for individual differences (Kohl, 2021, p. 10–11).

658. Finally, even if the two processes are considered not so different from each other, there is still the discussion on stereotyping *per se* and its morality. Kohl (2021, p. 11) argues that stereotyping, or making non-universal generalizations, is a natural and necessary aspect of human knowledge and judgment, provided that it is based on empirical evidence and that certain historically disadvantaged groups are protected by anti-discrimination laws. This behavior, using shortcuts and proxies, is not inherently irrational or unethical and it is based on an acceptance of inaccurate results in particular cases (Kohl, 2021).

659. Hildebrandt (2008, p. 26) observes that to survive, all living beings must consistently analyze and profile their surroundings to adjust themselves or their environment. Therefore,

big-data driven profiling and individualization can be criticized for *undue* stereotyping and for mistaking the reduction process for the totality of social knowledge (Pangrazio *et al.*, 2022, p. 262).

8.3.2 Predictions

660. Making predictions about the future is inherent to human nature. We do it all the time to mitigate the risk of uncertainty and the unexpected. With big data and the increase in data processing capacity, statistical techniques have become increasingly powerful and affordable. When it comes to predicting human behavior, what was initially more restricted to the finance sector (with the use of algorithms to predict whether a person would pay back a loan, for instance) has spread to all areas of life in society, including education.

661. Children are still evolving, and education itself is the implementation of human and economic resources betting on the development of individuals and society as a whole. Thus, predicting the future would facilitate anticipating challenges such as dropout rates, identifying areas for improvement, tailoring interventions regarding each child's educational path, resource allocation, etc.

662. However, unlike other types of algorithmic inferences, predictions are special because they involve the element of time, creating a unique set of problems. Decisions are made regardless of the prediction's accuracy and human rights violations can occur even when conclusions were right. As a projection of a possible future stemming from past or present perspectives, algorithmic predictions rely on certain assumptions that give rise to particular concerns. These assumptions are that i) the past repeats itself and the future will resemble it; ii) individuals will maintain consistent behaviors over time; and iii) groups with shared characteristics will share similar actions (Matsumi; Solove, 2023).

663. Matsumi and Solove (2023) cluster the problems arising from these assumptions and the use of algorithmic predictions based on personal data in categories. I will adapt them in this subsection while applying them to edtech.

8.3.2.1 Crystallization of the past

664. This issue is mainly based on the assumption that the past repeats itself. When algorithmic predictions are made about students based on past data about them, their families, their schools and their peers, it can perpetuate existing inequalities and limit their ability to

explore and even think of alternative educational pathways and opportunities. These interventions can lock children into stereotypes, impede their social mobility, and influence their educational and other life opportunities.

665. Consider a student who is unable to attend classes due to her need to care for her ill mother. Hwe low attendance may influence predictions about this student's performance. However, if her mother's illness is cured, this aspect may not necessarily be factored into the decision-making process for her situation. Similar circumstances could arise when a student shows disruptive behavior at school due to family issues or bullying. Even if these underlying challenges are solved, decisions made solely based on a snapshot of a particular period in the child's life, rather than considering the entirety of their experiences and the potential for change, can lead to significant problems.

666. This is described by Williamson (2016, p. 137) as a "new form of 'up-close' and 'future-tense' educational governance", which transforms students into centers of anticipation. This kind of anticipatory governance "abducts subjects in specific habits; governs subjects through provided memories; and (dis)-orients subjects for calculable futures" (Webb; Sellar; Gulson, 2020, p. 2). This process is facilitated by data infrastructures that emphasize a linear, teleological, and quantifiable understanding of time, resulting in the synchronization of educational cultures.

667. Indeed, education policy has always been concerned with preparing individuals for an uncertain future and facilitating societal change. However, this form of anticipatory governance raises questions about whether future possibilities are truly knowable and how this could limit human agency. Rather than viewing educated individuals as having untapped potential waiting to be realized through education, they can be reduced to datafied subjects with predetermined paths. This approach restricts the range of possible educational futures, as they become mere continuations of past and present rearrangements (Webb; Sellar; Gulson, 2020).

668. This is especially problematic regarding children, as childhood is known to be a period of experimentation. Children test their limits all the time in order to get to know the world, inevitably making mistakes along the way. This does not mean that they will necessarily happen again in the future. On the contrary, we must recognize that most people change over time, particularly when they mature, and that it is unfair to view their past actions as determinants of future potentialities.

669. A study on errors of AI models predicting students at risk of not submitting their assignments can illustrate this. The researchers examined two categories of errors: false negatives, i.e., students who were anticipated to submit their assignments and did not, and false positives, i.e., students not expected to submit their assignments who yet did. The findings underscored the importance of unforeseen events that can influence students' behavior and cannot be anticipated or accounted for in predictive algorithms, such as shifts in family and work obligations, unforeseen health concerns, and technical issues with computers (Hlosta *et al.*, 2022).

670. The dominance of chronological anticipations also obscures the ways in which the habits and memories of educated individuals are governed. In other words, the logic of time based on chronological order conceals how artificial intelligence determines future outcomes based on its own non-human algorithmic "learning". The concept of aionic time[24], which encompasses different conceptions of time beyond the human perspective, is rarely discussed within education policy processes and practices (Webb; Sellar; Gulson, 2020).

671. Finally, when we zoom out from the individual to society, we realize that fossilizing the past necessarily maintains the status quo. The collected data tell a very specific narrative about the past, inherently limited to what was possible to gather and, more specifically, quantify. This leads to the oversight of underlying contexts and reasons, perpetuating existing inequalities.

8.3.2.2 Unfalsifiability and preemptive intervention

672. Two other very related problems described by Matsumi and Solove (2023) in relation to predictive algorithms are the impossibility of falsifiability and the problem of preemptive intervention. It is not possible to assert whether a prediction will ever occur in the future, meaning that individuals affected by decisions based on these predictions cannot effectively challenge them. Even though it is possible that the accuracy of the predictions can be determined in the future, decisions are often made before this time.

673. This creates another issue known as the preemptive intervention problem. Decisions based on the prediction interfere with the sequence of events in a particular narrative, making it impossible to know if the future event would have actually occurred or not. Consider an educational institution that implements a student retention program using algorithmic

[24] "Aionic conceptions of time stress the quality of duration (e.g., 'eternal', endless, cyclical) and differ from chronological conceptions of time that stress sequencing of events and binary teleologies that extend backwards or forwards (e.g., past and future)" (Webb; Sellar; Gulson, 2020, p. 6).

predictions. If a student's probability of dropping out in the next semester exceeds a certain threshold, the student will be enrolled in additional support programs. A student is at high risk of dropping out, so the institution provides them with extra academic and counseling support and they complete the semester]. In this scenario, it is impossible to know if the initial prediction was wrong or if the institution has just timely intervened in the situation. A narrative arguing that the algorithm prevents dropouts is thus challenging to refute.

674. This presents specific challenges regarding accountability and data control, akin to those discussed in section 8.2.2 above. However, these challenges are exacerbated due to the element of time and the inability of individuals to provide counterevidence to the prediction. When it comes to inferences about the present, it is easier to be verified (think of a person's political affiliation, for instance), but inferences about the future are always speculative (Matsumi; Solove, 2023).

8.3.2.3 Performativity

675. As discussed above, unsupervised algorithms use a bottom-up approach to identify relationships among data points and create clusters. This means they will try to find patterns among the data that were not previously thought of. The very nature of clustering algorithms introduces uncertainty regarding whether the generated groups accurately represent the data's underlying structure or if artificial groupings have been created. Different clustering algorithms with distinct properties can yield different results, and selecting a clustering criterion further influences the outcomes, as different criteria can impact the created groups (Perrotta; Williamson, 2018, p. 10).

676. This means that patterns are not just "found" by algorithms but actively constituted. The concept of "performativity" is relevant here, as it suggests that social practices, knowledge forms, objects, and analytical tools are not mere representations of reality but are involved in reproducing it (Perrotta; Williamson, 2018, p. 4). Selwyn (2015, p. 72) argue that using a digital data lens can lead to the idea that complex (and mostly unsolvable) social problems within schools can be seen as complex (but solvable) statistical problems. Therefore, data analysis starts to shape educational settings in the same way that educational settings produce data.

677. Floridi (2011, p. 30, emphasis in the original) explains that information can be understood in three ways: "information *as* reality (e.g. as patterns of physical signals, which are neither true nor false), also known as environmental information; information *about* reality (semantic information, alethically qualifiable); and information *for* reality (instructions, like

genetic information, algorithms, orders, or recipes)". This means that information can deeply impact reality by changing the knowledge about it, constituting it, or changing it (Purtova; Maanen, 2023, p. 10). The extent of this impact depends on the intricate interplay of various factors that underly the process of datafication and the use of algorithms, including interests, choices, and technical considerations.

678. Algorithmic predictions may crystallize a student's perceived status and result in, for example, low expectations, which leads to a self-fulfilling prophecy of failure. This is known as the Pygmalion or Rosenthal effect, which refers to a psychological phenomenon where high expectations leads to improved performance. When certain behaviors are anticipated from others—due to any specific bias, be it good or bad—human actions tend to influence the likelihood of those expected behaviors occurring (Perera, 2023). The labels created to categorize students are internalized not only by them but also by their educators. This influences both behaviors towards what was initially expected and not necessarily to a child's full potential.

679. Studies show, for example, that increasing the amount of a scholarship (or conversely, increasing the amount of debt) directly increased graduation rates. Additionally, scholarships can influence a student's attitude and commitment towards college (Engler, 2021). This evidence suggests that using predictive algorithms, which rely on past data to award scholarships—a practice increasingly observed in universities—might overlook this effect and directly impact individuals' likelihood of graduating.

680. The table below illustrates two similar cases highlighting the issues with predictive algorithms. It demonstrates how these algorithms, used to assess students, crystallized past situations; made it impossible for students to counterprove the results; and, if their use were not discontinued, they could potentially begin shaping reality, influencing how schools teach students or organize themselves to better align with the algorithm's assessment criteria.

Table 4 - Ofqual's algorithms for evaluating students' performance

a) England

681. In England—with a similar situation taking place in Scotland (Scottish school pupils have results upgraded, 2020) —algorithms were used for evaluating students' performance in secondary school. Due to the cancellation of all secondary education exams as a result of

the COVID-19 pandemic, an alternative method had to be developed for assessing students' achievements. The Office of Qualifications and Examinations Regulation (Ofqual) initially requested that teachers predict their students' grades, but it was worried that they might be too optimistic. Therefore, an algorithm was also implemented to standardize grades.

682. The model was complex and encompassed various layers of assessment. According to Bedingfield (2020, n.p.), first, it created a historical profile of grades achieved by students in each subject at each school over the past three years. The algorithm then generated three sets of grades, comparing the distribution of grades from previous years to predict distributions for past and current students based on national averages for similar prior attainment.

683. The algorithm calculated the difference between the predicted distribution for current and previous students, adjusting the actual distribution of earlier students to give a distribution for current students. Grades were assigned based on a ranking provided by teachers. Even if a student was predicted a certain grade, they could still receive a lower one if the pupil ranked at the same level the year prior received a lower grade. While the percentage of "A" grades reached a record high of 27.9%, the algorithm reduced nearly 40% of the A-level grades forecasted by teachers. Many students failed to meet university entry requirements, and neither the International Baccalaureate Organization (IBO), which offered the algorithm, nor Ofqual have properly explained how the final grades were awarded (Cyndecka, 2020).

684. This model was problematic for various reasons, such as for penalizing excellent schools and students because of the national average; penalizing great students in underperforming schools; privileging independent, smaller and richer schools because cohorts that averaged smaller than five were given only their teacher's predictions; and lacking accuracy and transparency in its testing (Bedingfield, 2020, n.p. Dark, 2020). Digital rights' organization Foxglove threatened to take legal action against Ofqual on the bases that the algorithm was evaluating schools instead of students and this automated decision would violate art. 22 of the UK GDPR (Dark, 2020). In the end, students protested against the use of the algorithm and only the grades predicted by teachers were used. This does not mean that problems such as incorrectly estimating the performance of black students did not occur (Cowan; Arboine; Alemoru, 2020).

b) Norway

685. The same algorithm provided by IBO was used in Norway and was investigated by *Datatilsynet*, the Norwegian DPA. The DPA has received several inquiries related to reports issued by Norwegian media regarding students who believed their final grades were not accurate. According to the DPA's request for information letter sent to IBO in July 2020, some students believed that using historical prediction data from the schools would lead to being evaluated similarly to their peers of previous years, even when individual differences existed. Being this an automated decision-making process, it would be prohibited, unless exceptions of art. 22(2), GDPR, applied (Datatilsynet – Norwegian Data Protection Authority, 2020c).

686. In the following month, the DPA issued an advance notification of order to rectify unfairly processed and incorrect personal data to IBO. The DPA intended to decide that a) IBO refrained from using "school context" and "historical data" in awarding grades to students, as this would violate the fairness principle in art. 5(1)(a), GDPR, and lead to the processing of incorrect personal data in violation of art. 5(1)(d), GDPR; and that b) IBO rectified grades awarded under these criteria (Datatilsynet – Norwegian Data Protection Authority, 2020a). This action led to some students receiving higher grades. However, the DPA did not have the competence to challenge them further. The IBO's main office was in the UK, which was still part of the European Economic Area (EEA) at the time, meaning that the Norwegian DPA could not take further actions (Holmes *et al.*, 2022)**.**

8.3.3 Human mis-interpretation and mis-use of data

687. Human interpretation of data within the school environment can result in wrong and unfair decisions, creating new or perpetuating old inequalities. After misinterpreting the data and making incorrect assumptions, educators could focus on improving the wrong issues (Lai; Schildkamp, 2013, p. 18). If a student is performing poorly, for instance, educators may try to interpret the causes of their academic outcomes (Bertrand; Marsh, 2015, p. 864) (although, as already discussed, causation is not the approach to data taken by algorithms). Schools could, attribute students' performance solely to their categorization by an algorithm (such as identity, services received or test scores). They can assume inherent deficiencies (e.g. the student's outcome in English is not excellent because of its migration background) instead of reflecting on historical inequalities, their own instruction or considering how the school can better support

these students. When educators use data ignoring their context or rely on personal assumptions about students or their families, it can reinforce pre-existing biases and the unjust context that shapes student outcomes (Bertrand; March, 2021). It also prevents them from getting to the root of the problem and making the right decision to improve educational processes.

688. There is also the challenge of placing too much trust in technologies, often leading to overshadowing educators' reasoning and experience, even when evidence suggests otherwise. Research has shown, for example, that people tend to obey instructions from a robot in a simulated fire emergency, even when they are informed that the robot was malfunctioning and the guidance provided was evidently incorrect (Wagner; Borenstein; Howard, 2018). This means that educators will require training and assistance to comprehend how and when they must apply their own judgment (Cardona; Rodríguez; Ishmael, 2023, p. 32).

689. This is also linked to what is currently known as the dashboard effect. After the data are analyzed by a specific system, the information is often presented to educators through a dashboard or other type of visualization technique. This effect means that individuals or organizations make decisions solely or mostly based on the information presented in a dashboard or visual display of data without considering the broader context or additional information. It is easy to become overly reliant on the simplified and summarized information provided in a dashboard, potentially overlooking important details, nuances, or underlying complexities.

690. Even if people were to become aware of the context and all the information needed to interpret the data—which is very difficult due to algorithms' black-box feature (Laet *et al.*, 2020)—dashboards, as well as the data embedded on them, rather than being impartial representations of reality, are shown to construct compelling narratives. These narratives have the tendency to portray teachers as managers, students as varying degrees of risk, and reduce the complexity of students' social interactions to quantifiable data points (Jarke; Macgilchrist, 2021, p. 3).

691. The use of dashboards in edtech, as well as other kinds of data visualization, "makes data about children into a form of value that can be exchanged by them for rewards such as upgrades and personalized features, transforming classrooms into little digital economies and calculative spaces where personal data have exchange value and utility" (Lupton; Williamson, 2017, p. 787).

692. Dashboard views also "create a false sense of autonomous control over learning while nudging teachers' interpretations and pedagogical actions through particular views. […] They are] always biased reductions of learning—and not in any way neutral representations […]" (Kerssens; Dijck, 2022, p. 295). The increasing reliance on data-driven decision-making may affect educators' pedagogical assessment and intuition, as their importance can rapidly be diminished compared to the digital devices that students are required to use (Hillman *et al.*, 2023).

693. This effect can certainly be identified both in descriptive and predictive analytics. Although research on predictive systems in education is limited, the existing ones indicate that teachers and other users can modify their behavior based on dashboard outputs. This raises ethical concerns, as exemplified by a user questioning whether they should advise students labelled as "high risk" to pursue alternative paths instead of college (Hartong & Förschler, 2019, as cited in Jarke; Macgilchrist, 2021, p. 3).

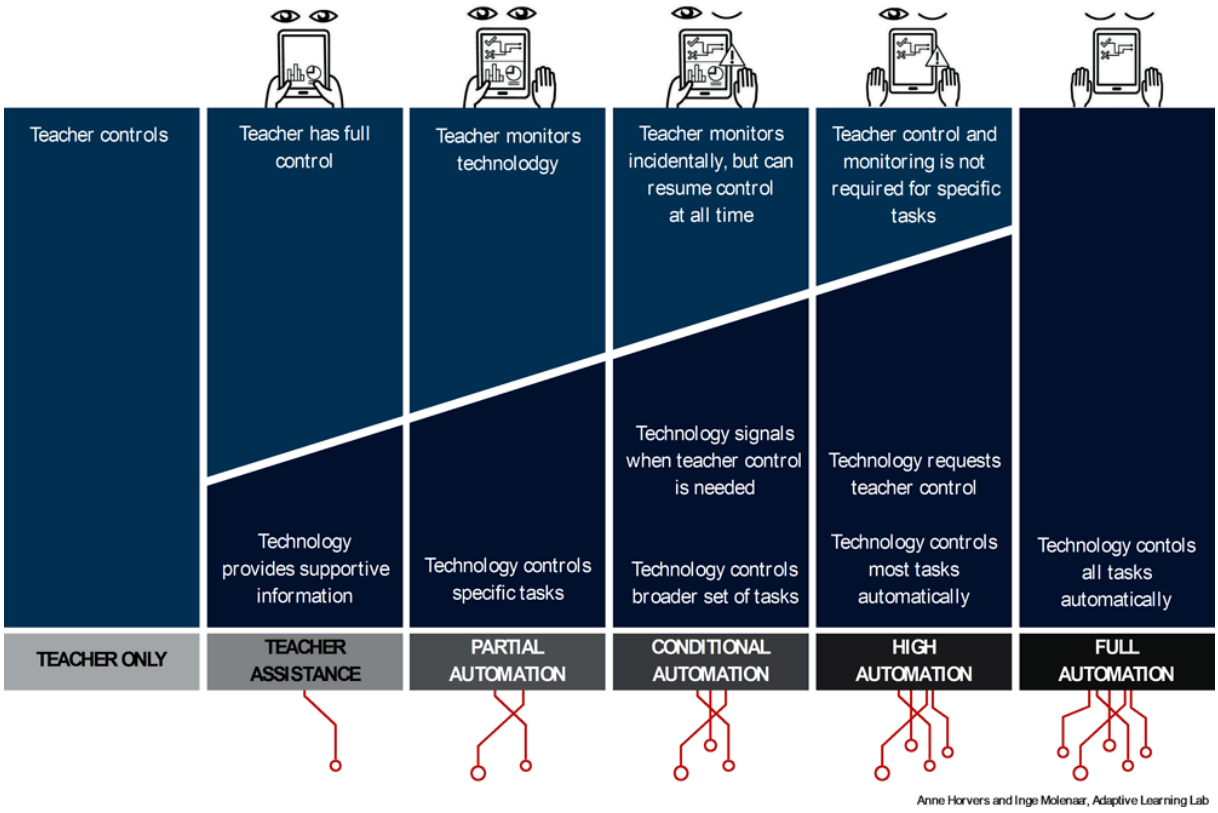
694. They can thus also play a role in undermining educator's professional autonomy and expertise. Educating a child is highly nuanced and context-dependent, which requires flexible and adaptive approaches. Relying on predefined metrics and algorithms, especially when these are seen as more "objective", can limit the ability of educators to make informed decisions that are also based on their knowledge, experience, and instinct (Zeide, 2020).

695. To understand the level of automation and teacher participation within personalized learning technologies—which could also be used here to discuss how edtech can impact educators' autonomy—Molenaar (2021) suggests six levels of automation defined by the car industry to the field of education (see Figure 5 below). Here, we can clearly see how industry standards and epistemologies (as discussed in Chapter 2) are increasingly being applied to education.

696. According to the original model's explanation (Molenaar, 2021, p. 59),

> [t]he lines under the model represent the expectation that increasingly more data streams will be used in the transition towards full automation. These data streams can support more accurate detection and diagnosis of learners and their environment. At the top of the model, the level of human control is visualized across the levels. The hands on the tablet represent the level of teacher control. Full teacher control with two hands on the tablet, partial control with one hand and no hands symbolizes no or incidental teacher control. The eyes represent the required level of teacher-monitoring, ranging from full, partial, incidental to no monitoring. The warning triangle indicates the ability of the AI to notify the teacher to resume control at critical moments.

Figure 5 - Six levels of automation of personalized learning



Source: Molenaar (2021, p. 60)

697. These possibilities create several tensions around teacher's control. A scenario where the technology is in full control with no teacher involved would rarely be desirable, but the middle ground is full of nuances and gives rise to different challenges. We might need to establish guidelines that would vary on a risk-based approach. More caution should be taken when handing over control of critical decisions, such as determining a student's placement in their next course or managing disciplinary referrals (Cardona; Rodríguez; Ishmael, 2023, p. 31).

698. Similarly, these decisions may also require a very granular understanding of what it means to have humans in the loop or in control. This could include always requiring teachers' input establishing protocols for further intervention of principals, municipalities, or student associations where necessary, as well as granting students due process rights. However, it is also important to recognize that including teachers in the loop might also create more work than what they previously had, which mitigates the initial attempt to make their job easier (Cardona; Rodríguez; Ishmael, 2023).

699. Finally, another situation where data could be misused is by trying to "game the system" (Laet, 2023, p. 52). This would involve the attempt to be successful in the educational digital learning environment by exploiting its social-technical properties, instead of using it as a tool to achieve the previously defined educational goals.

700. Schools might manipulate student data to boost their own performance metrics; emphasize short-term achievements, compromising the long-term learning process; tailor the course content or focus only on some students in order to improve score tests at all costs (Lai; Schildkamp, 2013); focus on hacks to master standardize tests, etc.

8.3.4 Personalized learning

701. In a traditional classroom, students follow the same curriculum and perform the same tasks. Credits are generally awarded based on "seat-time", regardless of what is actually learned, and the focus is on the development of the average student, not the full potential of each individual. Even in this traditional scenario, however, everyday interactions within the classroom already include some degree of personalization, such as when teachers provide extra support to students who are struggling to make progress, which requires educators to have a deep awareness of the needs of each student (Holmes *et al.*, 2018).

702. Personalized learning is thus not a straightforward concept. It can encompass a wide range of approaches and there is no universally accepted definition, with different educators and experts interpreting and implementing personalized learning in different ways. It is also often conflated with other concepts such as individualized learning, competency-based learning and differentiated learning, whose meaning will often depend on the one defining it.

703. Although complex and very much contextual, it is possible to map some common features of personalized learning from the existing understandings. According to Holmes *et al.* (2018, p. 16), these features would involve multiple continua related to micro and macro decisions taken by the network of actors within education. The more agency learners have in relation to designing their own learning process, the more personalized the learning process can be. These continua include:

> Personalisation of why something is to be learned (the learning aims); Personalisation of how it is to be learned (the learning approach); Personalisation of what is to be learned (the learning content and learning pathway); Personalisation of when it is to be learned (the learning pace); Personalisation of who is involved in the learning (the learner or learning group); Personalisation of where the learning takes place (the learning context).

704. As we have seen above, the idea of personalized learning is not a new one and started to be discussed well before the development of existing technologies. It is at the core of progressive education traditions, which emphasize tapping into students' interests and passions, providing them with individualized opportunities to ask questions, explore, and take risks to facilitate learning. This approach is related to the work of the American educator John Dewey over a century ago, for instance, and is commonly found in schools that prioritize project-based learning (Herold, 2019, n.p.).

705. However, personalizing learning was also very important to behaviorist approaches at the beginning of the twentieth century. Behaviorism is a psychological theory that emphasizes the study of observable behaviors, rather than internal mental processes. According to behaviorists, behavior is shaped by environmental factors, such as rewards and punishments, and can be modified through conditioning techniques.

706. Human beings are understood as "organisms" that should be observed in order for psychologists' work to be considered scientific. The loss of the human inner world's importance (as it would be exempted from scientific inquiry) and the understanding that the environment determines human behavior have several consequences for autonomy and free will. What is viewed as outcomes of free will should be seen just as the accidents in the world of physics (Zuboff, 2019).

707. The behaviorist approaches to learning, for example, seek to reinforce desired behaviors and shape them through systematic instruction and practice. Mastering academic content could be fostered by identifying what each child needs to learn, assessing what they already know, and then creating an optimal path for them to learn the rest. As detailed in Chapter 1, the implementation of this approach can be traced back to the 1950s when the behaviorist B. F. Skinner experimented with "teaching machines", which allowed students to answer questions and immediately receive feedback (Herold, 2019; Watters, 2021).

708. As can be expected, the problem with this theory is that it views personalized learning not only as rooted in a measuring and testing rationale but also as completely detached from the development and significance of students' autonomy. It fails to encourage self-knowledge, thereby hindering individuals to understand their capabilities and difficulties, as well as the best path towards integral human development. This approach merely identifies, through observable behavior (which can be embedded in biased interpretation and correlations), what the students

know and need to know, guiding the learning path from one point to another through behavioral steering techniques.

709. Understanding this history is important because technologies can reflect different understandings of learning and different pedagogical theories. Many argue that the way personalized learning is embedded in today's edtech is mostly based on behaviorist and instructionist knowledge-transmission approaches, rather than on educating by projects, collaborative learning, guided discovery learning or productive failure approaches (Miao *et al.*, 2021; Watters, 2021).

710. If the learning process is narrowly conceived as the transmission of pieces of information, that will eventually build into knowledge and skills, then automation would be a way to enhance the efficiency of this process. If the goal, however, is to enable children to understand concepts from within and encourage them to find answers to their own inquiries about the world, then their approach to learning is somehow already unique and diverse (Kohn, 2015).

8.3.4.1 Technologies for Personalized Learning

711. Although personalized learning can be perceived as an interesting and pedagogically sound approach, it is challenging to implement in traditional, large classrooms. It requires training, specific resources, time, and alignment with the educator's own approach. Ideally, it demands a democratic discussion on who decides what, and where a school lies within each of the personalized learning continua mentioned above.

712. Technologies are historically seen as an important tool to support personalization (see, for example, the development of teaching machines described in Chapter 1). With advanced tracking capabilities, it has become easier to monitor students' learning plans and progress with greater precision, while enabling a wider range of instructional opportunities (Pane, 2018, p. 3). Other developments such as the availability of one device per student in many countries and a deeper integration of technology into daily school practices have also played an important role (Molenaar, 2021).

713. Intelligent Tutoring Systems (ITS)—also known as intelligent interactive learning environments—, for example, "provide step-by-step tutorials, practice exercises, scaffolding mechanisms (e.g. recommendation, feedback, suggestions and prompts) and assessments, individualized for each learner, through topics in well-defined structured subjects such as

mathematics or physics" (Holmes *et al.*, 2022, p. 5). When the ITS is based on dialogues about the subject instead of an individualized sequence of material or activities, it is also called Dialogue-Based Tutoring System (DBTS).

714. ITS can come in many shapes and is sometimes implemented in LMS such as Moodle, Open edX and platforms like Khan Academy (Miao *et al.*, 2021). They mainly involve several AI models, such as a domain model (knowledge about the topic to be learned), a pedagogy model (knowledge about effective approaches to teaching) and a learner model (knowledge about the student). Some ITSs also involve a fourth model called open learner, which aims to provide information to teachers and learners on what has taken place within the system and the decisions made (Holmes; Bialik; Fadel, 2019, p. 102–107).

715. Making use of a learner model, i.e., a hypothesized knowledge state of a student, is actually what really differentiates AI-driven ITS. It incorporates thousands of data points from the user, such as which tasks they have answered correctly and what challenges them, what is clicked on the screen, what is typed, how rapidly they move the mouse, as well as their emotional state. Through data analysis, this is integrated with the knowledge about other students and their interactions to predict the suitable pedagogical approach and domain knowledge for a specific student at any stage of their learning (Holmes; Bialik; Fadel, 2019, p. 105). These data are also used to update the model, and the cycle starts again.

716. As mentioned in the definition of ITS, these systems are better suited for well-defined domains such as mathematics and physics. One reason for this is that imprecise problems would generally require students to apply other more complex skills and the contexts would be more dynamic and uncertain. The lack of structure challenges the definition of learning paths and the provision of feedback (Holmes; Bialik; Fadel, 2019, p. 108–109). An alternative to ITS is Exploratory Learning Environments, which adopt a constructivist approach. In these systems, students actively build their knowledge, but the challenge of not having clear definitions of correct behaviors to provide the necessary guidance still remains (Holmes; Bialik; Fadel, 2019, p. 127).

717. The type of technology used for implementing personalized learning will greatly depend on the learning objectives and what kind of governance decision will be affected. Therefore, we can also mention smart learning management systems, learning network orchestrators and digital games-based learning as other existing examples among the myriad of available technologies (Holmes *et al.*, 2018, p. 37–40).

718. Technologies have the potential to effectively implement personalized learning, and their promise is worth pursuing. However, they should not be considered a silver bullet that can solve all problems of current education systems, especially when they are still based on poor pedagogical approaches. All the current challenges they present should be taken into consideration within the decision-making process. Below, I will highlight the main challenges to children's rights to privacy and to the protection of personal data resulting from implementing personalized learning technologies within education.

8.3.4.2 Lack of robust evidence of their effectiveness

719. The efficacy of personalized learning tools has been demonstrated in some short studies, usually restricted to some contexts and universities (Holmes *et al.*, 2022). In the case of ITS, some meta-analysis concluded that, compared to one-to-one teaching, there was a negative effect size of -0.19, while compared to whole-class teaching it had an average effect size of 0.47 (Holmes; Bialik; Fadel, 2019). However, robust and independent evidence, especially focused on different groups and long-term effects, is still not available (Braun *et al.*, 2020; Dijck; Poell; Waal, 2018; Holmes *et al.*, 2018; Hooper; Livingstone; Pothong, 2022; Stringer; Lewin; Coleman, 2019).

720. On the contrary, some technologies might even reinforce poor pedagogical practices. While analyzing the 124 most-downloaded edtech mobile apps, for example, Meyer *et al.* (2021) highlighted that the majority showed lower-quality design, being distractive and repetitive, and provided minimal learning value. The research indicated that free applications scored lower due to disruptive advertisement and frequent, reward-driven feedback, which affected children's attention and learning.

721. Many edtech products replicate performed educational processes that were flawed since the beginning, incorporating those imperfections into their design: "a child recalls facts and answers; an application diagnoses and displays the outcome on a digital dashboard. Learning is recorded on some kind of scale as some kind of learning achievement" (Hillman, 2022, p. 7).

722. Kucirkova *et al.* (2023) highlight some reasons why edtech companies might refrain from designing their products according to evidence-based, scientifically sound research. Edtech companies are generally driven by Key Performance Indicators (KPIs), levels of funds raised, profitability, customer retention and/or product scalability. Another contributing factor is the gap between edtech funding and development: "[w]hile the investor and funding

community typically value impact metrics that are guided by scientific research principles, they do not have a unified approach to guide these efforts" (Kucirkova; Brod; Gaab, 2023, p. 1)**.**

723. Therefore, based on the state-of-art and the current commercial incentives for personalized learning, there is little to substantiate the wide use in well-resourced classrooms apart from marketing pressure and groundless hopes by policymakers and administrators (Holmes *et al.*, 2022). In some regions, when there is a lack of qualified teachers, the argument for using these tools to support learning can be stronger. However, it should be viewed as a temporary measure, given that it addresses a consequence rather than the root cause (i.e. lack of appropriate investment in education) (Holmes *et al.*, 2022)**.**

724. Edtech could have a more positive impact on education if certain conditions were in place, such as the development in tandem with researchers and pedagogues, focusing on learning principles (Kucirkova; Brod; Gaab, 2023, p. 1–2). In any scenario, the costs of implementing these technologies for other human rights should not be disregarded, especially the ones related to the rights to privacy and data protection.

8.3.4.3 Limits to personalization

725. Although it may seem counterintuitive, personalized learning technologies often do not empower students to make meaningful choices about their education. While it is supposed to let students take responsibility for their own learning, they usually lack awareness of how their choices are organized within the technology design and have limited influence on other students' activities and the overall learning environment (Dishon, 2017, p. 282). Their choices are limited to when and how they will master a predetermined set of skills and personalization is restricted to the pathways to prescribed content (Miao *et al.*, 2021, p. 15). The learning outcomes are always the same and have been mandated by individuals who are often unaware of the student's specificities (Kohn, 2015). Finally, it presupposes an educational dynamic where children are constantly under surveillance and can do little to revert this situation (Couldry; Mejias, 2019, p. 176).

726. The students' learning path is not only constrained by the technology architecture but also by the interpretation of the data collected about them. In this context, the profiler does not necessarily adjust the learning paths to the student's unique characteristics. Instead, after providing some initial data, students are conformed to the profiler's standardized patterns. Personalization practices can then "homogenize" populations within sub-groups, and every student will be like others in fundamental aspects (Kohl, 2021). This is closely linked to the

debate on the individualization aspect of datafication and how the limits between individual and group data are blurred (see Section 8.3.1).

727. In the end, the mainstream available technology for personalized learning focuses on efficiently getting students to move quickly towards a learning outcome. “Real personalization, however, involves every student learning and achieving what they individually want to achieve, to what is called self-actualization. No current AIED system comes anywhere near helping students to achieve that” (Holmes, 2023, p. 62).

728. Another challenge is the way personalization is interpreted. As currently implemented, these technologies heavily emphasize the individual level of effort, which undermines the importance of both individual and social components of education. They tend to reduce the human contact among students and teachers and social interaction is often perceived as a secondary aspect (Miao *et al.*, 2021).

729. In a student-centered and project-based education, for example, children learn with each other by working together and developing their individual and collective autonomy. This means that while understanding concepts is undoubtedly a personal process, it is not limited to individual effort, and also requires working in a group (Kohn, 2015). This is essential for realizing a broader understanding of education, which includes community building and the development of social skills (Holmes, 2023, p. 62), as well as the cultivation of democratic citizens who are capable of shaping their learning environments and the larger society (Dishon, 2017, p. 282).

730. This is also related to the discussion on what level of standardization schools need to provide. One the one hand, personalization has the potential to address the complexity of learning and the specificities of each individual. On the other hand, some form of standardization might also be desirable to identify and narrow education gaps, as well as focus on collective achievements (Kucirkova, 2021).

8.3.4.4 Content filtering

731. Since personalization algorithms are based on inferences of users’ needs and interests, another possible result of this process may be filtering out some contents. In the words of Vaidhyanathan (2011, p. 182), “[l]earning is by definition an encounter with what you don’t know, what you haven’t thought of, what you couldn’t conceive, and what you never understood or entertained as possible. It’s an encounter with the other—even with otherness as

such". Personalized learning can thus often be considered "the educational equivalent of filter bubbles" (Dijck; Poell; Waal, 2018, p. 125).

732. This is what Kucirkova (2022) calls the like-like logic of recommendation algorithms embedded in social media platforms, whereby similar content is suggested according to the user's engagement. This works well when people are looking for a group that shares their niche interest, for example, but not necessarily for fostering new ideas and expanding viewpoints (Kucirkova, 2022, p. 225)**.** "The mission of education should be precisely the opposite—ensuring that children have access to many different areas of knowledge, and that they can experiment with all these areas in open-ended and non-discriminatory ways" (Barassi, 2020, p. 80). The difficulty of encountering the unknown affects not only the individual as such and the possibility of learning new things but also society more broadly, as accepting and understanding different people and viewpoints are essential for democracy.

733. While personalized learning is often hailed as a way to enhance learning by tailoring the educational experience to the individual needs of each student, determining which information holds relevance or which content should be reinforced remains highly subjective and dependent not only on the pedagogical methods but also on the designers' interests. Paradoxically, this has the potential to diminish student autonomy rather than enhance it. Finally, this logic also helps perpetuating power imbalances and inequities, further marginalizing underprivileged students (Holmes, 2023).

8.3.5 Student monitoring technologies

734. With the increasing adoption of digital technologies in schools, especially after the COVID-19 pandemic, it has become easier to monitor what kids do online and offline. This could be used, for example, to identify access to inappropriate content and online bullying, supervise students during an exam, ensure the safety of schools or monitor mental health, behavior or familiar issues. In this sense, a wide array of surveillance technologies have been increasingly deployed in schools, such as surveillance and facial recognition cameras, access control technologies, social media and student communication monitoring technologies, web filtering, weapon and metal detection etc.

735. Some enthusiasts argue that timely interventions could be implemented, for example, when students allow the sharing of conversations with advisors and professors. Special support can be provided to students dealing with dire situations, such as food insecurity. Personalized

emails could also be composed to help students with financial problems (Schaefer, [*s. d.*], n.p.). The edtech industry often markets these technologies based on two main narratives: that school and students' safety are at risk, which demands immediate attention, and that their products represent the optimal choice to solve the issue (American Civil Liberties Union (ACLU), 2023).

736. The emotional impact of fear on educators and the lack of resources and expertise to make decisions on the use of technologies can override statistics and science. There is still a lack of independent evidence about the efficacy of surveillance technologies in schools, and, in the case of surveillance cameras, there is already evidence showing that they actually do not prevent violence (American Civil Liberties Union (ACLU), 2023). The risks they pose to children's rights, however, are tangible, and the subsequent sessions will attempt to discuss some of them.

8.3.5.1 Behavior Monitoring

737. When it comes to behavior monitoring, a technology called Gaggle, widely used in the USA, could serve as an interesting example. Gaggle is a platform that uses a combination of AI technologies, such as ML, and human oversight to detect warning signs of potential crises among students, such as violence or self-harm, bullying, use of drugs, fighting, threats, or the presence of weapons on campus before they can escalate into tragedy.

738. Also on their list of worrisome words are LGBTIQA+-related ones such as "gay," "lesbian," and "queer." It can analyze every student's move, such as browsing history, social media notification, school email address, documents, interactions in the LMS, etc. (Haskins, 2019). By identifying these warning signs early on, Gaggle claims to help school administrators and teachers take preventative action and ensure the safety and well-being of their students (Who watches AI watching students? [Audio podcast episode], 2022).

739. A concrete example of its application was provided in the podcast "In machines we trust" (Who watches AI watching students? [Audio podcast episode], 2022). On a Friday evening, outside of school hours, a middle school student took out his Google Chromebook and began creating a document. The document contained the statement: "I'm tired of faking my feelings. I've got no one who loves me. Not even my family. My only choice left is suicide." Gaggle informed the school's principal of the situation, who then and contacted the student's home, while the assistant principal contacted the police. The student was later found walking towards a location where two other children had previously committed suicide by jumping in front of a train. All of this happened in just fifteen minutes.

740. Monitoring technologies like Gaggle typically work by analyzing and identifying students' online activities and content on school-provided devices, school networks, and especially on the adopted LMS. When monitoring software scans web traffic or specific applications, it can either scan the content and retain only the flagged material or keep all the material for future reference.

741. The algorithms can be based on natural language processing of keywords or phrases or use other types of AI. The service can also involve additional review layers, typically conducted by humans, as exemplified by Gaggle. In terms of response, it can vary depending on the system and what the school requires, ranging from content blocking and warnings to notifying parents, emergency services, and law enforcement agencies (Collins *et al.*, 2021, p. 4–6).

742. While these systems may seem promising in terms of identifying potential crises and ensuring student good behavior safety, "circumstances—in which there is a clear, imminent danger of a student about to harm themselves—are fortunately rare, and scanning for self-harm using monitoring systems often seeks to identify situations that are much more ambiguous" (Collins *et al.*, 2021, p. 4). These anecdotes must also be compared to the amount of erroneously flagged situations.

743. This prompts a discussion on how to accurately assess the success rate of such technologies. Since they are based on external behaviors, determining their preventive efficacy and long-term effects poses significant challenges.

> For example, in one description of an incident involving interception of a student suicide plan, Gaggle asserted that "[t]he student now realizes the importance of being cautious [with] how you express yourself in an email." One wonders, however, how much this student has been prevented from thoughts of self-harm as opposed to being deterred from ever again expressing her feelings about it in writing. If a student has other avenues to express her pain, she may get the help she needs; if, however, this particular means of communication was her only one, she may turn her negative feelings inward, internalizing the lesson that reaching out may yield only a police visit. What is more, the stigma and fear that a police visit may cause students is not discussed (Fedders, 2019, p. 1703).

744. Even in the USA, a country that leads the raking of school shootings[25], the chances of a student in primary or secondary education being shot and killed is 1 in 614 million, which is more than twice as unlikely as winning the top prize at the American lotteries Powerball or Mega Millions (American Civil Liberties Union (ACLU), 2023, p. 13). These statistics, together with the scant evidence that surveillance technologies are efficient to prevent violence

[25] According to Grabow and Rose (2018), the USA has had 57 times as many school shootings as the other major industrialized nations combined between 2009 and 2018.

and other undesired behaviors would already be enough to think twice before deploying them, especially when public resources are used.

745. However, on top of this, this kind of monitoring raises significant concerns regarding ethics, privacy and data protection issues, as well as the delicate nature of children's mental health. Although the intention behind such systems is usually noble, there are doubts about whether this approach is truly the most appropriate or effective in addressing the underlying issues students face.

746. For example, with filtering and blocking technologies, students can experience difficulties in completing assignments due to the lack of access to certain contents. Schools can also deploy subjective restrictions not always aligned with the promotion of human rights, such as filtering content related to LGBTQIA+ community, as stated before. Finally, there is always the risk of students circumventing the technology (Laird; Dwyer; Grant-Chapman, 2023).

747. One of the fundamental aspects of supporting children is establishing an environment of trust, where they not only feel comfortable confiding in adults about their struggles but are also able to seek for help elsewhere (American Civil Liberties Union (ACLU), 2023). By relying on surveillance mechanisms, there is a risk of creating a climate of suspicion and invasion of privacy, which could discourage children from seeking help or expressing their emotions openly. This constant monitoring can create a chilling effect whereby children avoid or limit their self-exploration. In the case of education, for instance,

> [t]his can lead to students who do not feel that they can ask questions when they are questioning the behavior of adults in their life or of abusive partners or peers, who do not feel like they can explore resources if they are questioning their own gender or sexuality, or who are afraid to do research to understand the nuances of complex issues in their own lives. This self-repression can be damaging to students' mental health and well-being (Center for Democracy & Technology (CDT), 2022, p. 2).

748. It is also important to mention that "escalating a student's mental health treatment by hospitalising them or calling the police can be risky [… and] could worsen a student's symptoms" (Fasulo, 2019, as cited in Haskins, 2019, n.p.). The involvement of law enforcement authorities often obstructs students from accessing medical treatment and needlessly entangles them in the criminal justice system. This reinforces existing inequalities and perpetuates the school-to-prison pipeline. Groups who are already marginalized, such as students of color, students with disabilities, LGBTQIA+ and non-binary students, undocumented students or low-income students are the ones most likely to be flagged by monitoring systems and disproportionately referred to law enforcement or being harmed in another way (American Civil Liberties Union (ACLU), 2023, p. 25 et seq.; Collins *et al.*, 2021, p. 20).

749. To create a sustainable and holistic impact on students' well-being and foster good behavior, it is essential to invest in resources that address the broader societal and environmental factors affecting children's safety and mental health. Surveillance technologies predominantly attempt to address the aftermath rather than tackling the underlying factors that contribute to issues students face.

Table 5 – Gaggle and its impacts on privacy and mental health

750. During the pandemic, a 13-year-old transgender person from Minneapolis, USA, experienced exacerbated gender dysphoria and emotional distress. This culminated in a suicide attempt, leading to hospitalization and subsequent outpatient psychiatric care. The student eventually improved and decided to reflect on this episode and how music therapy helped him cope in a school assignment. The document was flagged by the monitoring system Gaggle, especially because of the word suicide, and triggered school intervention. His mother was called to learn about the situation without considering the context of the student's mental state and the meaning of the assignment (Keierleber, 2021).

8.3.5.2 e-Proctoring

751. Apart from technologies used to monitor children's well-being and unwanted behavior online, other technologies to support teachers have been heavily introduced within the school environment, especially with the COVID-19 pandemic. It includes, for example, software to detect plagiarism and services that monitor students during online test-taking (e-proctoring). Proctorio, for example, is a well-known software that provides services such as identity verification, automated and live proctoring, plagiarism detection, and content protection. It uses

> gaze-detection, face-detection and computer-monitoring software to flag students for any "abnormal" head movement, mouse movement, eye wandering, computer window resizing, tab opening, scrolling, clicking, typing, and copies and pastes. A student can be flagged for finishing the test too quickly, or too slowly, clicking too much, or not enough. If the camera sees someone else in the background, a student can be flagged for having "multiple faces detected." If someone else takes the test on the same network — say, in a dorm building — it's potential "exam collusion." (Harwell, 2020, n.p.).

752. This information is then used to assess a student's conduct throughout the exam and detect any behavioral patterns that could be interpreted as cheating. For instance, the level of suspicion in relation to a student increases if their gaze deviates from the screen for an extended period. The algorithm, occasionally in collaboration with a human proctor, determines which

individuals are deemed suspicious and identifies who is considered to be engaging in cheating behavior (Watters, 2020).

753. According to some students, the system sometimes mistakes harmless actions like reading questions out loud or looking away as a response to thinking as signs of cheating. The possibility of failing can be an extra factor of anxiety, especially when it relates to movements the student cannot control. Professors have the power to decide which student behavior is monitored and choose to ignore the system's findings, but there is no guarantee. In a context where teachers have no direct access to the student's behavior, it is common to assume that the technology is objective and has greater monitoring capabilities, meaning that everything it detects aligns with reality. Therefore, in order to defend their honesty, students might have to prove that the technology got it wrong (Harwell, 2020).

754. Apart from the cognitive bias, the technology was also accused of not taking into account some student's living conditions—such as the fact that some live in dormitories or houses with many people—and of racial bias as it would not recognize black faces more than half of the time (Mitchell, 2021)**.**

755. Proctoring and other student monitoring technologies have in common the fact that the environment being created in schools is focused on control and mistrust, frequently using a narrative of care. The very place that should foster the exploration of knowledge about the world and oneself and cultivate ethical, responsible citizens prepared for the swift changes in society is, in fact, doing the complete opposite.

8.3.6 Learning Analytics and further use of data

756. The typology developed in Chapter 1 includes not only edtech used for providing education directly but also technologies used to *learn about learning*. The data and analytical techniques used for this purpose are generally the same as for providing education, but the focus is on understanding "how learners learn, learning progression, or which learning designs are effective […]" (Holmes *et al.*, 2022, p. 19). This is also called learning analytics.

757. As discussed above, personalized learning and other ways of implementing data-driven technologies for providing education collect an immense amount of students' data. A single session of interaction between a child and an edtech could generate around 5 to 10 million actionable data points per student, with education being considered the most "data-minable industry" (Data mining of school kids, 2012).

758. However, this digital footprint does not only help students learn better and personalize their experience. Apart from processing the collected data, AI tools will produce new data that could be fed again into the AI model (Laet, 2023, p. 50), especially data on how students learn and behave. By analyzing student behavior and engagement patterns, developers can train their AI models to make predictions about future trends that are considered more accurate. This information enables businesses to make informed decisions, such as forecasting demand for educational products and services, thereby informing strategic planning and resource allocation.

759. The constant data cycle presupposes this step in order to improve the algorithm and then personalize experiences based on group data. However, this also means that students' data could be used for other purposes not necessarily related to their learning process. Education data can provide insights into the knowledge, skills and competences of individuals and groups, as well as serve as proxies for various other situations. They can inform decisions across a wide range of areas and are valuable for different stakeholders, such as companies, data brokers, social scientists, political parties and the government (Chakroun *et al.*, 2022).

760. For instance, employers can use these data to make hiring decisions. A candidate's background and performance in school are often proxies for the candidate's suitability for the role and potential success. Applicant Tracking Systems (ATS) is one of the technologies used in a "talent acquisition" process, which has evolved to include "AI-based recruitment tools, skills assessments, candidate relationship management, onboarding, and even internal talent marketplaces" (Gallagher *et al.*, 2023, p. 7).

761. There is a growing interest in skills-based hiring in the market, meaning that prospective job candidates are assessed based on their skills rather than traditional degrees (Gallagher *et al.*, 2023, p. 16). These skills are usually captured and communicated through digital credentials, which "promise to make education more relevant by documenting learning in a way that empowers people to plan, track, and share their accomplishments in a secure and verifiable way" (Understanding Digital Credentials Building Value from an Ecosystem of Open Standards, [*s. d.*], n.p.).

762. Comprehensive Learner Records (CLR), for example, are digital portfolios that promise to provide a more holistic and accurate representation of a student's skills, knowledge and abilities. They not only focus on credits and grades but provide detailed information of student's learning experiences (Understanding Digital Credentials Building Value from an Ecosystem of

Open Standards, [*s. d.*], n.p.). CLR can include any kind of data related to a student's education or skills.

763. Commercial uses of education data are also of interest of edtech and other third-party companies. The profile built through data gathered by persistent identifiers that track children across multiple devices could be used for advertising or other commercial purpose. In a research carried out by Human Rights Watch that analyzed 73 edtech apps, 56% were found to collect children's advertising IDs[26], and none of them allowed children to opt out of the tracking activities (Human Rights Watch, 2022, p. 24–26). This clearly shows the surveillance element of these technologies in children's lives.

764. Fourteen of the analyzed applications also had access to information like the Wi-Fi Media Access Control (MAC) address or the International Mobile Equipment Identity (IMEI), "two persistent identifiers that are so strong that a child or their parent cannot avoid or protect against their surveillance even if they take the extraordinary step of wiping their phones or performing a factory reset" (Human Rights Watch, 2022, p. 27). Lastly, of the 163 apps examined by Human Rights Watch, 80% were found with embedded tracking technologies built by Google, which gives the company access to children's data from many different sources (Human Rights Watch, 2022, p. 86)**.**

765. The identifiers referred to above are just an example of the broader surveillance that children are put through because of commercial activities. Others include tracking where children are, who they know, how they deal with content online and what they do in the classroom often in an unnecessary and disproportional way. Many continue to track children outside the classroom, especially when the same device is used for other personal activities. Human Rights Watch also identified that "most EdTech companies did not disclose their surveillance of children and their data; similarly, most governments did not provide notice of these practices and their risks to students or teachers when announcing their endorsements of EdTech platforms" (Human Rights Watch, 2022, p. 41).

766. Even when children's data are not used for advertising purposes, other commercial interests can still be identified that would justify surveillance. First, children represent a

[26] "An advertising ID is a persistent identifier that exists for a single use: to enable advertisers to track a person, over time and across different apps installed on their device, for advertising purposes. For those using an Android device, this is called the Android Advertising ID (AAID). An AAID is neither necessary nor relevant for an app to function; Google's developer guidelines stipulate that app developers must 'only use an Advertising ID for user profiling or ads use cases'" (Android for Developers, as cited in Human Rights Watch, 2022, p. 24).

significant market segment with their own distinct needs. By trying to understand their behavior and preferences through data analysis, companies can tailor their products and services to better adapt them to this specific demographic.

767. Moreover, collecting children's data, or even being present in their lives early on, can contribute to building a loyal customer base for the future. By establishing a relationship with children at an early age and getting them used to their products, companies can potentially retain them as customers for many years, especially when the business model depends on scaling. This is particularly advantageous for companies offering products or services designed for children, such as toys or educational materials, and is especially the case when they are offered free of charge. Early experience with a brand or product could increase the likelihood of continued usage as children grow older and become more independent consumers. This is especially true when the brand creates a feeling of nostalgia in the user, which increases brand loyalty (Mondragon Ruiz, 2021).

768. Children also play a crucial role in influencing family purchasing decisions (Chaudhary, 2016). While parents often make the final choice, children strongly influence those decisions. They may request specific items, such as toys, clothing, or food, prompting parents to fulfil their wishes.

769. Education data can also be instrumental in enhancing products and services. Companies in the edtech sector can use data on student performance and behavior to develop new features that improve learning outcomes and engagement. Children's interactions with edtech are thus providing not only technical knowledge about how a product works but also business intelligence about how a product is used. These data can be used to improve edtech products and other offerings within the companies' portfolio, including job, health, and dating apps. Therefore, the remaining question is whether student data should be used for these purposes and whether the latter are being prioritized over children's educational goals and well-being.

770. Beyond the issues concerning how companies are using data, we should also reflect on the consequences of this transfer of knowledge from the public to the private sector. Indeed, this can directly impact children's future opportunities, determining the universities they will attend, the jobs they will secure, and the services they are entitled to. However, the amount of information that private actors have access to can also directly shape our economies and society, leading to an asymmetry of information and consequential power imbalance that can undermine democracy and the rule of law.

771. Due to the proprietary aspect of algorithms and the information they create (even if it is created with children's own data), states have less information about public education than the private actors themselves, which directly impacts public policies. Ultimately, it can lead to and reinforce the lack of digital sovereignty, reducing the autonomy of states to determine their digital destinies, the policies and legislation they will enact, and the technology they will have access to, which is at the heart of data colonialism practices.

Interim conclusion

772. This chapter aimed to provide an overview of the main challenges that edtech poses for children's rights, especially with regard to their rights to privacy and the protection of personal data. The first part of the chapter focused on horizontal risks presented by AI, given that these systems are present in the majority of today's edtech.

773. I started by examining the process of datafication itself and the issues stemming from reducing and abstracting reality into quantifiable variables. I discussed the operations of AI systems, noting the significant volume of data required for training and functioning, as well as the repurposing of data, which already poses challenges to the principles of purpose limitation and data minimization, as well as other basic data protection rules such as the need for a legal basis.

774. I have emphasized the concerns surrounding data generation within AI systems and how the inferences drawn can be tainted with bias and significantly affect individuals' control over their data. This calls for a greater focus on AI systems' outputs and the development of more tools for controlling personal data, such as the right to reasonable inferences.

775. The challenges related to decision-making based on the inferences made by AI systems have also been discussed, including those related to profiling, predictions and human interpretation of data. We have seen that algorithmic predictions have the potential not only to cement past circumstances, thereby impeding social mobility, but also to influence future outcomes, as patterns are not simply recognized but actively shaped by these predictions.

776. Building on the typology developed in Chapter 1, I also focused on some issues related to specific technologies, namely personalized learning, student monitoring technologies and learning analytics. After discussing its definition and historical context, I highlighted that although promising, personalized learning through technologies may still not be fit for purpose,

considering its risks. There is a lack of robust evidence demonstrating its positive impact on learning outcomes or other educational goals. Moreover, I emphasized how these technologies often overly focus on individual efforts at the expense of social components of education. I have also shown that the aspects that can indeed be personalized are limited, and these technologies can be, on the contrary, constraining student's learning paths and choices by predefined parameters, limiting their autonomy and potential for being whomever they want to be.

777. Although student monitoring technologies are often created with noble and legitimate aims in mind, such as dealing with student's mental health and preventing cheating, they frequently raise concerns related to surveillance. Surveillance mechanisms can create a climate of suspicion and invasion of privacy, hindering students from seeking help or expressing their emotions openly. It also creates a chilling effect that will affect children's development and learning (as have been discussed in Chapter 4). The focus on control and mistrust, under the guise of care, can paradoxically undermine the development of ethical, responsible citizens and perpetuate biases and inequalities, disproportionately impacting marginalized groups. This is even more serious when there is still scant evidence of these technologies' efficiency to tackle violence and other kinds of behavior within schools.

778. Lastly, I have also focused on the use of technologies for learning about education. I discussed how learning analytics analyze data from student interactions and AI models to generate new data that can inform the learning process, particularly regarding how students learn and behave. This enables companies to refine their AI models for more accurate predictions about future trends.

779. However, these data are often also used for purposes beyond the scope of education. There is a growing trend of using data for skills-based hiring and comprehensive learner records to provide a more holistic representation of student's skills and learning experiences. Students' data are also used for other commercial purposes, such as targeted advertising, creating a loyal customer base from an early age and developing other products. This raises concerns about limiting children's future opportunities, power imbalances, data protection and the erosion of digital sovereignty.

Chapter 9. Google Workspace for Education

780. This chapter aims to present what Google Workspace for Education is, its main features, and how it fits into the broader context of Google's business model. As described in the introduction, there are several reasons why Google Workspace for Education was chosen as a case study for this thesis. In summary, Google was a pioneer in DDBM on the scale that we currently know, which have been replicated across the digital environment, including by other edtech platforms; Google Workspace for Education is widely adopted worldwide; and Google is deeply involved in a broader network of data sharing, owing to its market power. Therefore, studying Google's dynamics can provide a framework to understand other commercial edtech platforms in the current digital economy and their impacts on children's rights to privacy and data protection.

781. With the COVID-19 pandemic and the further expansion of Google's deployment, a significant number of decisions made by competent authorities in Europe regarding its operations and the impact on personal data protection has surged. This is yet another reason to understand in greater detail the effects of this technology and gain insights from what has been found by the authorities.

9.1 What is Google Workspace for Education

782. On August 28, 2006, Google announced its web-based office suite named Google Apps for Your Domain combining various productivity tools (Statz, 2006). Although these tools were already accessible to individual customers, the package was primarily tailored to organizations aiming to provide them to their employees (Flynn, 2006). At the moment of its introduction, the suite encompassed GMail, instant messaging, Google Calendar, and a web page creation tool (Google, 2006b).

783. In October of the same year, Google announced Google Apps for Education, an initiative that would tailor the use of Google Apps for Your Domain for education institutions. This included new features such as the partnership with Blackboard—that would integrate Google enterprise search technology for schools and the Blackboard Learning System with Google Scholar—as well as the launch of an Application Programming Interface (API) that would simplify the process for organizations to integrate with Google Apps for Education (Google, 2006a). Later in 2006, Google purchased YouTube (Sorkin; Peters, 2006).

784. Over time, additional tools were introduced, including Google Spreadsheets, and Google Docs in 2007 (Google, 2007), as well as Google Presentations and Google Sites in 2008 (Google, 2008). In 2010, Google launched the Google Apps Marketplace that enabled Google Apps administrators to purchase integrated third-party cloud applications (McMullan, 2010). Google Drive was then introduced in 2012 (Johnston, 2012).

785. The beta version of Google Classroom was only launched in 2014 and was available for some selected schools (Magid, 2014). In 2015, a mobile version of Classroom was launched, together with the Google Classroom API, and a share button for websites (Perez, 2015). Google Apps for Education was renamed Google Suite for Education in September 2016 and later in 2020 as Google Workspace for Education (Google, 2020; Perez; Lardinois, 2016).

786. While it was not initially created to be an LMS (Lazare, 2021a), it constantly increased its features over time and teachers started to use it as a "hub" for educational content. Because of the pandemic, Google Classroom has increased from 40 million to 150 million users (Lazare, 2021b), making it one of the most used edtech worldwide. According to LearnPlatform, which publishes a regular Edtech Top 40 list of the most used edtech products in primary and secondary education in in the USA, Google products took 8 of the top 10 spots in 2022 (Palmer, 2022).

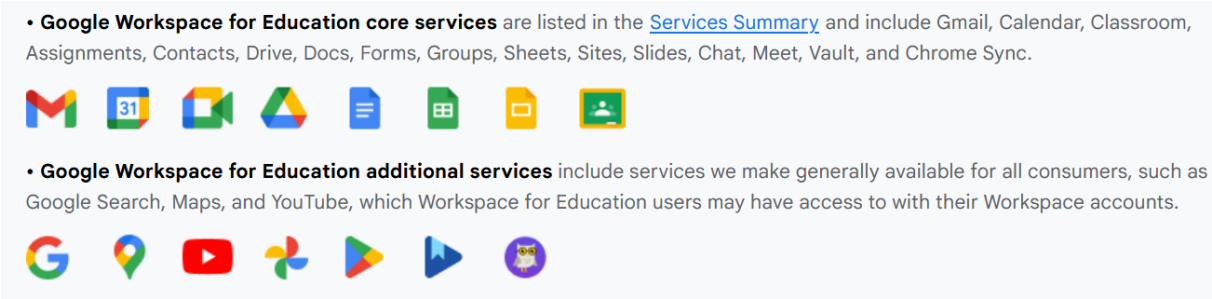
787. Anyone with a Google account can use Google Classroom, but to use Google Workspace for Education as a suite of applications, a school account is necessary. After being approved for Google Workspace for Education, schools can add users to their domains, set up the available apps, and use advanced features, such as mail migration.

788. Schools can choose from different editions of the application suite. With the Google Workspace for Education Fundamentals, they can access the core services, such as Classroom, Docs, Sheets, Slides, Forms, etc. The Google Workspace for Education Standard has the same features as the Fundamentals but also includes premium security and information technology features. The teaching and learning upgrade provides premium teaching and learning features to be added such as third-party add-ons, Microsoft Word support, call transcripts, YouTube Live Streams, among others. Finally, the Education Plus includes all features in the Standard version and the Teaching and Learning Upgrade. The Fundamentals edition is available at no

cost to schools, while the premium features demand annual subscriptions (Google, 2023b, 2023a). The main core[27] and additional[28] services are depicted in the figure below:

789.

Figure 6 - Google Workspace for Education's core and additional services



Source: Google (2023f)

790. Apart from the application suite, Google also provides Google Chromebooks for Education, a simple and affordable laptop based on web applications using Google Chrome browser (Google, 2023e; Magid, 2014; Upson, 2011), as well as smart whiteboards to use the Jamboard application (Google, 2023i).

791. Educators using Google Workspace for Education can participate in Google Educator Groups (GEGs), which bring together "teachers from the same region, in person or online, in a forum where they can share, collaborate and support each other to effectively leverage technology with students" (Google, 2023h, n.p.). Each group is organized by a volunteer GEG leader who despite not being formally linked to Google, acts as marketer for Google products (Sujon, 2019).

---

[27] The list of core services include: Client-Side Encryption, Cloud Identity Services, Duet AI for Google Workspace, Enterprise Data Regions, Gmail, Google Calendar, Google Chat, Google Cloud Search, Google Contacts, Google Docs, Google Sheets, Google Slides, Google Forms, Google Drive, Google Groups for Business, Google Jamboard, Google Keep, Google Meet, Google SIP Link, Google Sites, Google Tasks, Google Vault, Google Voice, Google Workspace Assured Controls, Google Workspace Migrate, Meet Global Dialing, Workspace Additional Storage, and Workspace Add-Ons (GOOGLE, 2023g).

[28] The list of additional services include: Applied Digital Skills, Assignments, Blogger, Brand Accounts, Campaign Manager 360, Chrome Canvas, Chrome Cursive, Chrome Remote Desktop, Chrome Web Store, Classroom, CS First, Early Access Apps, Experimetnal Apps, FeedBurner, Google Ad Manager, Google Ads, Google AdSense, Google Alerts, Google Analytics, Google Arts & Culture, Google Bookmarks, Google Books, Google Business Profile, Google Chrome Sync, Google Cloud, Google Colab, Google Developer, Google Domains, Google Earth, Google Fi, Google Groups, Google Maps, Google Messages, Google My Maps, Google News, Google Pay, Google Photos, Google Play, Google Play Console, Google Public Data Explorer, Google Read Along, Google Search Console, Google Takeout, Google Translate, Google Trips, Location history, Looker Studio, Managed Google Play, Material Gallery, Merchant Center, Partner Dash, Pinpoint, Play Books Partner Center, Programmable Search Engine, QuestionHub, Scholar Profiles, Search Ads 360, Search and Assistant, Socratic, Studio, Third-party App Backups, Tour Creator, and YouTube (GOOGLE, 2023g).

792. Google also offers training and certification programs to educators. Online training courses are available at no cost for teachers so they can learn the fundamentals of the tools. Educators can then become certified teachers by participating in two levels of exams designed to assess educators' abilities to use Google Workspace for Education (Google, 2023f). After getting certified as a Google Teacher, it is possible to become a certified trainer in order to train fellow teachers on Google tools (Google, 2023c, 2023l), as well as a certified innovator, which encourages teachers to lead so-called "transformative projects" proposed by Google.

9.2 The main features of Google Workspace for Education

793. As explained above, Google Workspace for Education is a suite of applications tailored for teaching and learning, which attempts to resemble the processes that occur face-to-face within schools. The central hub for activities within schools is the Google Classroom where other applications can be embedded or linked. Within Google Classroom educators can create and manage classes, assignments, and grades; give direct and real-time feedback; post announcements; engage with students in discussion fora; star video meetings; among others.

794. Google Workspace for Education and, more specifically, Google Classroom is increasingly adopting AI within its tools. "One notable application is the introduction of "Practice Sets", which leverages AI to transform teaching content into interactive assignments for personalized learning. Educators can input their own questions or select them in a database, with AI suggesting specific skills that would be emphasized in that activity. Teachers then select the most appropriate skills involved in that activity (such as solving equations or writing thesis statements) and students receive hints if they face any challenge in solving it. This can also be implemented in YouTube videos.

795. Students get real-time feedback "[a]nd when they get an answer correct, practice sets will celebrate their success with fun animations and confetti" (Kiecza, 2022). The application also includes an autograding tool, as well highlights on the students' performance, enabling educators to identify areas where students may need further support. Personalized learning is also implemented by the add-on read-along, which provides real-time feedback to children learning how to read (Sinha, 2023).

796. Classroom analytics provide educators with insights into assignment completion rates, grade trends, and Classroom adoption, with the possibility to delve into the individual student level to better provide support (Sinha, 2024). Additionally, generative AI is increasingly being

integrated into Google Workspace for Education. For example, Duet AI is designed to assist teachers across the suite's applications, aiding them in drafting lesson plans in Google Docs, generating images in Google Slides, or building spreadsheets in Google Sheets.

797. Although occurring through digital ICT, the educational processes enabled by Google Classroom still mostly reproduce a hierarchical classroom structure, as well as a behaviorist approach to learning (Gleason; Heath, 2021, p. 33). Within the pedagogical domain, the mechanisms and structures of formal schooling are said to be abstracted to fit a predefined template for participation. According to Perrotta *et al.* (2021, p. 107) this is done by the notion of a "doubly articulated pedagogy", which encompasses three main components:

> a) the role of Google, the platform proprietor, in establishing the strategic outlook and the 'rules of the game'; b) the various forms of integration enabled by a proprietary API, which simultaneously brackets and extends pedagogy; and c) the multiple divisions of labor which are enabled by the platform dynamics, and upon which the platform as a whole depends.

798. Even with Google stating that teachers should have a more significant role than technology (Langreo, 2023), these components mean that important decisions taken in relation to how the platform is designed and works are delegated to developers and often exclude educators (Perrotta *et al.*, 2021, p. 108). One illustrative example is provided by Jonathan Rochelle, the former director and product manager of Google, who was involved in the development of Google Classroom and other applications within the current Google Workspace for Education Suite. Referring to his children in a speech at an industry conference, Rochelle said: "I cannot answer for them what they are going to do with the quadratic equation. I don't know why they are learning it […] and I don't know why they can't ask Google for the answer if the answer is right there" (Singer, 2017)**.**

799. More than the content of the statement itself, what matters is what can be implied. The practice of memorizing facts is long criticized by more progressive pedagogies. However, more deeply, it suggests that Google has effectively become the arbiter of relevant knowledge and the ways to access it (Krutka; Smits; Willhelm, 2021, p. 427). It becomes able to determine whether something is useful and worth teaching or not, implying that any information obtainable through a Google search is deemed irrelevant to learning. Rather than prioritizing the process of critical thinking and the methods required to arrive at the correct answer, only the result is considered significant (Bäcke, 2022, p. 60), reinforcing the *learnification* of education paradigm. This concern might escalate with the increasing use of generative AI in education.

800. Moreover, especially with the dominance of its search engine, Google is influencing human memory, acting as an index and as a filter (Vaidhyanathan, 2011, p. 174–179). It changes what we humans choose to forget or remember, which can be a challenge when it comes to how people are educated and what kind of personal data are available not only for Google but also for third parties.

801. Google's role within education is only possible because of Google's broader role within the current society. Google's mission is defined as "to organize the world's information and make it universally accessible and useful" (Google, 2023j). Hillis, Petit, and Jarrett (2013, p. 6) argue that this power has given Google a consecrated status, both in the sense of being sanctioned by law, custom, or usage, and of something set apart by being hallowed, sacred, or divine. This "sacred" power and all the benefits that the technology provides mesmerizes educators, as well as public administrators.

9.3 The role of Google Workspace for Education within Google's business model

802. Efforts to quantify human behavior and use data to improve businesses have existed for centuries. Data have been used to inform internal decision-making processes and understand customers' preferences. Examples of early DDBM include selling customer profiles by data brokers, targeting with personalized direct mail campaigns, and customer loyalty programs.

803. Systematizing, understanding, and finding patterns in data was very labor intensive. However, advancements in the technological landscape (such as the advancement of computer processing capabilities, the spread of smartphones and connected devices, the rise of cloud computing technologies, and the improvement of AI systems) have made it more cost-effective to collect, store and process vast amounts of data, including personal data. Although the infringement of the rights to privacy and data protection was already an issue in the early adoption of DDBM, the so-called "data revolution" has taken it to another order of magnitude.

804. In this sense, Zuboff (2019) explains how Google had a key role in fostering the current DDBM, and compares their importance to how the Ford Motor Company and General Motors fostered mass-production-based managerial capitalism. Since the beginning, Google search queries produced a great amount of metadata (such as the number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location). Initially, these data were ignored by the company, but the work of Amit Patel led to the realization that "the continuous flows of collateral behavioral data could turn the search engine

into a recursive learning system that constantly improved search results and spurred product innovations such as spell check, translation, and voice recognition" (Zuboff, 2019, n.p.).

805. Through what the author calls the behavioral value reinvestment cycle, behavioral data were being used only to improve the user's experience in the form of improved services (Zuboff, 2019). At this stage, Google's vision of a search engine still repealed the use of advertisement for its funding, which was elaborated on a foundation paper written by its founders:

> [W]e expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers. Since it is very difficult even for experts to evaluate search engines, search engine bias is particularly insidious […] This type of bias is very difficult to detect but could still have a significant effect on the market. Furthermore, advertising income often provides an incentive to provide poor quality search results. […] [W]e believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm (Brin; Page, 1998, p. 18–19).

806. Nevertheless, with the implosion of the "dot-com bubble" and the need to find a business model to sustain Google's activities, these "collateral" data started to be used to improve the profitability of advertisement, what Zuboff (2019) calls the discovery of *behavioral surplus*. Advertisements have always been based on the idea of delivering "a particular message to a particular person at just the moment when it might have a high probability of actually influencing his or her behavior" (Zuboff, 2019, n.p.). Before the use of the behavioral surplus, advertisements on the internet were based mainly on the use of keywords or content, not on the specificities of a particular user. What Google presented as a solution was the increase of the "relevance" of advertisement based on deducing user's needs and wishes through their behavioral data. These data could be directly given by the user, observed, or inferred (Hof, 2017; Zuboff, 2019).

807. What is important for this thesis is that

> Google's invention revealed new capabilities to infer and deduce the thoughts, feelings, intentions, and interests of individuals and groups with an automated architecture that operates as a one-way mirror irrespective of a person's awareness, knowledge, and consent, thus enabling privileged secret access to behavioral data. A one-way mirror embodies the specific social relations of surveillance based on asymmetries of knowledge and power. (Zuboff, 2019, n.p.).

808. The internet, which in the mid-1990s was primarily perceived by companies as a marketplace for the sale of goods and services, evolved into the perfect place for harvesting user data, strengthening the development of tracking technologies, and leading the commercial web down a path of surveillance and dire power asymmetries (West, 2019).

809. Google is a pioneer when it comes to processing data for further use, especially for marketing, and it has influenced the creation of the current widespread business model in the digital environment. In order to scale and gather more data, so predictions were more "accurate", there was a need not only to attract more users but to be ever more present in users' lives through different means. Therefore, Google started to expand to other areas beyond search such as providing services for schools.

810. One of the characteristics that makes the use of Google Workspace for Education attractive is that it provides the majority of its services free of charge and some for an affordable fee. An interesting finding from the Privacy Company's DPIA within the Dutch case, which will be described below in Chapter 10, was that apart from the possibility to store specific consent data within the EU (which indeed is very important to comply with data transfer rules and foster digital sovereignty) and the provision of additional security management options, there were no other significant distinctions in data protection between the free and paid editions of Google Workspace for Education (Nas, Sjoera; Terra, 2021, p. 5).

811. In the beginning, Google would allow advertisements to be displayed within the suite, which were also based on students' and educators' email content. The scanning and indexing would happen even when advertisement options were turned off. However, after a lawsuit in 2014 that questioned whether Google's practices were in compliance with the Family Educational Rights and Privacy Act (FERPA - USA) (Herold, 2014), Google decided to permanently remove "the 'enable/disable' toggle for ads in the Apps for Education Administrator console", as well as "all ads scanning in Gmail Apps for Education" (Bout, 2014, n.p.).

812. The lack of advertisement within the suite and the non-use of collected data for advertising purposes on other platforms, however, do not pose a threat to Google's business model and the potential revenue derived from Google Workspace for Education. Although there may be little or no direct monetary exchange between end users and digital platforms, the former still have to give up on something to sustain the market.

813. O'Reilly *et al.* (2023) call this platform model Algorithmic Attention Rents. According to the authors, rents are related to control over a scarce factor of production, which allows its holder to profit above what would be normally achievable in a competitive market. Rather than the result of productive improvements to grow the economy, rents represent a reallocation of economic value from one party to another due to market power. In the case of digital platforms,

the scarce factor would be the attention of their users and this kind of rent would be linked to the ability to distort organic results. The allocation of attention within platforms will then drive value allocation. In the authors' understanding, data would be the means to more effective attention allocation and not necessarily an end in itself (O'Reilly; Strauss; Mazzucato, 2023, p. 4–5).

814. However, "[t]he current increase in rents is a major contributor to increased inequality, less vibrant entrepreneurial ecosystems, and lower levels of productivity growth and investment in modern economies" (O'Reilly; Strauss; Mazzucato, 2023, p. 3). What is mistakenly understood as "for free" or relatively cheap may be explored in the expense of individual and collective externalities that should also be factored in (Trzaskowski, 2022, p. 234), such as issues related to competition, data protection, procurement, and children's best interest more broadly.

815. One of the main arguments currently used by Google to promote its products is the absence of advertisements within Google Workspace for Education Core services, as well as the assurance that user data is not collected for advertising purposes. Consequently, delving deeper into this discussion is essential to grasp Google's economic motivations behind offering this suite.

816. After analyzing the institutional logic behind the involvement of the main transnational technology corporations in education, Patil (2023) concluded that financial gain was their main drive. This could take the form, for example, of brand recognition, market development, or workforce development and all these aspects can be recognized in the Google Workspace for Education case**.**

817. First, Google's marketing strategy heavily relies on brand loyalty and recognition. The focus then is not necessarily on immediate transactions but on profitable growth in the long term. The so-called customer lifetime value (CLV) is often used as a metric to measure, as the company puts it, "the total value a business receives from a single customer over their entire relationship, is an ideal way to acquire, develop, and retain the most valuable customers for business growth" (Fader; Hoyne, 2021, n.p.). This includes, for example, providing their services for free to attract new audiences, creating early exposure to the products to create familiarity, encouraging life-long learning, building community experiences, etc.

818. It also encompasses expanding their business to increasingly more areas. In the case of Google, the focus of their products go from search to education, shopping, patents, finance,

communication, productivity, maps, healthcare, and operational systems. Veliz (2022) contends that these are not necessarily products designed for people, but rather new ways to collect more and different data from them.

819. Second, Google Workspace for Education encompasses two different kinds of services, as explained above. Core services are the main services offered to schools and include, Google Classroom, Calendar, Docs, Sheets, and Gmail (Google, 2023k, 2023g). Additional Services, like YouTube, Google Maps, and Blogger, "are designed for consumer users and can optionally be used with Google Workspace for Education accounts if allowed for educational purposes by a school's domain administrator" (Google, 2023g, n.p.). This differentiation is crucial, as it determines how students' and educators' data will be processed by Google.

820. While within the core services no advertisements are shown and no personal data are processed for this purpose, additional services may display them. Personal data could also "be used to provide, maintain, protect and improve additional services, and to develop new ones" (Google, 2023g, n.p.). In this sense, if the educator uses one of the additional services within the classroom, personal data could be processed under less strict policies and advertisements can be shown to students.

821. It is unclear how students' data flow from one kind of service to another while being used throughout school activities, particularly when they are embedded within each other. As we will see in the case of the Netherlands, the agreement made between the schools and Google stipulated that when embedded in Google Classroom, YouTube videos would adhere to the same rules as the core services. However, it is not possible to ascertain whether this is also the case for other jurisdictions.

822. Google also encourages parents and guardians to create a second account for the child, which can be linked to the school account through the Family Link, as this would empower them to set parental controls across accounts (Hooper; Livingstone; Pothong, 2022). However, what remains unclear is that this action might inadvertently prevent the child from benefiting from the protective measures instituted by the school within the school account.

823. Therefore, the problems persist in the majority of products and the core services can be serving as a bait to acquire more users and as a pathway for children to move from privacy-friendly environments to data-harvesting ones (Hooper; Livingstone; Pothong, 2022, p. 55). A user experience study conducted by Hooper *et al.* (2022) discovered that the seamless user interface blurs the distinctions between core and additional services. This results in users easily

transitioning between them without being aware of the differences in terms of data protection and the associated consequences.

824. A third aspect that should be considered is that to support Google's commercial interests, data do not need to be processed only for targeted advertising. Google can use the data to refine and enhance their products and services. This involves analyzing user data to gain insights into consumer behavior, preferences, and trends. By understanding how users interact with their applications, Google can improve design, develop new features, and tailor their services to better meet the needs and desires of their (future) customers. Additionally, data can also be used for improving and training Google's AI tools. In this sense, children's data become valuable to understanding preferences within a specific generation, family dynamics, future trends, etc.

825. A fourth important aspect is that Google can access children's data indirectly, through data shared by other edtech, due to its dominance over the digital realm. In a study of 163 edtech products, Human Rights Watch discovered that 80% of them were found with at least one embedded Google software development kit (SDK). The NGO discovered that edtech companies would in some instances share children's data with Google's advertising division (Human Rights Watch, 2022). Its "vertically integrated chain of platforms and algorithms" (Couldry; Dijck, 2015, p. 4) facilitates this process, as Google currently dominates the advertising technology (adtech) market both in terms of selling advertising space on its own websites and apps and being an intermediary between advertisers and publishers that can supply advertising space. This is what led the European Commission to send a Statement of Objections to Google over abusive practices in June 2023 (European Commission, 2023a).

826. A fifth aspect to be considered is the integration of Google Workspace for Education with other applications through the Google Classroom API. Integration and interoperability are also fundamental for expanding Google's business model, maintaining its relevance, and increasing its adoption and customer retention. With the API, Google can attract developers and software providers, outsourcing the task of expanding the platform's functionalities to "'enrich' the classroom experience, as long as they remain aligned with the overarching data ontology" (Perrotta *et al.*, 2021, p. 103).

827. The amount of data that it has access to also increases. The use of the API "allows Google to monitor and regulate how data are being exchanged, and how functionalities and their associated practices are integrated in the Classroom experience" (Perrotta *et al.*, 2021, p.

103). This gives Google a powerful role of gatekeeper for the edtech industry, setting the rules for third-party providers to integrate with Google Classroom and share data between them (Williamson, 2021).

828. Finally, the provision of Google Classroom as a free and accessible edtech strategically aligns with Google's narrative of social responsibility. This builds a positive brand image and positions the company as an entity that cares for positive societal impact (Magalhães; Couldry, 2021).

Interim conclusion

829. To discuss the challenges posed by Google Workspace for Education regarding children's data in the following chapters, this chapter aimed to describe what it is and how it operates, as well as its relationship to Google's broader business model. It emphasizes the importance of understanding Google's dynamics as a framework for the wider landscape of commercial edtech platforms and their implications for children's rights to privacy and data protection.

830. Key milestones in the development of Google Workspace for Education, particularly within Google Classroom, have been highlighted. We have observed that the design of Google Classroom and the broader pedagogical possibilities within Google Workspace for Education are still tied to a traditional and hierarchical vision of the classroom, reinforcing a behaviorist and quantitative approach to education that benefits from the phenomena of datafication and the learnification of education.

831. More importantly, this vision is aligned with the specific needs of Google's business model. Even though the application suite is free, Google still has very specific commercial reasons for keeping children within its ecosystem, including brand loyalty and recognition; blurred boundaries between its services with varying levels of data protection; indirect access to children's data via other platforms; and the use of data for other commercial purposes, even if not for targeted advertising.

832. Overall, Google serves as an important case study precisely because it is typical and representative of the mainstream business model in the digital economy. It shows how big tech companies are increasingly influential in significant decisions in education, including what children should learn, how they should learn it, and with what tools. The growing integration

of AI in the educational environment reinforces this notion, and if not adopted critically and for specific purposes within a broader pedagogical strategy, it could render teachers increasingly irrelevant. This educational perspective and the technologies used to implement it directly impact the quantity and quality of data processed by edtech platforms.

833. This reinforces the notion that edtech should be regarded as a tool within broader educational objectives. These objectives should prioritize and acknowledge the significance of social interactions and the role of teachers; aim to equip children with critical skills for navigating an increasingly digital world; and safeguard them from commercial influences that could compromise their well-being and infringe upon their human rights.

Chapter 10. The use of Google Workspace for Education in the European Union and in Brazil

834. Google Workspace for Education is widely used worldwide, but it impacts different communities in different ways. This chapter will focus on analyzing the impacts Google Workspace for Education has had on children's privacy and data protection in two different jurisdictions: the European Union and Brazil.

835. With regard to the EU, given the technology's extensive adoption and the controversies outlined in Chapter 9, it is not unexpected that complaints have been brought to the attention of competent authorities. The multiple analyses of the technology by public authorities in Europe provide important insights for this thesis. The publication of DPIAs in certain cases and the authorities' auditing capabilities allowed an in-depth analysis of the features of Google Workspace for Education. This level of scrutiny would be unattainable solely through the information publicly disclosed by the company.

836. This chapter will thus focus on discussing the decisions taken by authorities within the EU MS related to Google Workspace for Education. The methodology used to identify the decisions was twofold. First, I conducted searches for decisions regarding Google Workspace for Education within the databases of DPAs in Europe that are part of the EDPB. This encompassed not only the DPAs in each of the EU MS (and, in the case of Germany, in each of its *Länder*), but also those in the three countries that are part of the EEA: Iceland, Liechtenstein, and Norway. This search was supplemented by cross-referencing with the GDPR Hub and GDPR Enforcement Tracker websites. Second, the literature reviewed for this thesis also unveiled significant decisions regarding the use of the technology in certain countries and regions that were not covered in the initial search, such as the decisions taken by other authorities in France and Belgium. Ultimately, decisions relevant to the scope of this thesis were located in Belgium, Denmark, Finland, France, Germany, the Netherlands, Norway, Spain, and Sweden. Each of the subsections below will describe the violations of the rights to privacy and to the protection of personal data encountered by each authority and the implemented solutions.

837. When it comes to Brazil, however, there are still no decisions concerning Google Workspace for Education made by the ANPD. Due to the absence of this initial filter to map potential challenges to children's rights to privacy and data protection in the country, a different methodology was employed. In the Brazilian context, the standard documents used by Google

for the implementation of the application suite were scrutinized. This examination was supplemented by similar assessments performed by other researchers on prior versions of the relevant ToS and Privacy Policies, along with a broader analysis of the platform's deployment in Brazil and its procurement by Brazilian public authorities.

838. The subsequent sections will thus delineate the decisions made by authorities in each EU MS, as well as the challenges identified in the Brazilian case. A comprehensive analysis of the convergence or divergence in these decisions, as well as the interrelation of the realities of the two jurisdictions and the gaps still identified according to the normative framework, will be conducted in Chapter 11.

10.1 Belgium

839. The *Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens* (VTC - Flemish Supervisory Commission) was established on 25 May 2018 with the Belgian GDPR decree. It replaces the Flemish Supervisory Commission for Electronic Administrative Data Traffic that was instituted by the e-gov decree and has been operational since 2010, being responsible for supervising the application of the GDPR by the Flemish administrative authorities (VTC, [*s. d.*]).

840. Due to the existence of other DPAs in the country, the role of the VTC was recently brought up in a parliamentary question (La Chambre des Représentants, 2023). It discussed a possible cooperation agreement between the Belgian DPA and the VTC due to different interpretations given to the GDPR, which could create legal uncertainty. The government responded by indicating that discussions are still ongoing regarding the powers of the VTC and its relationship with the Belgian DPA. However, it highlights that the Belgian DPA is the sole supervisory authority under the GDPR within the country. Although the GDPR does not exclude the existence of more than one supervisory authority in the same MS, the VTC would only be able to act as one if it fulfils the conditions set out in Chapter 4 of the regulation (see also decision 26/2023 of 16 February 2023, of the Belgium Constitutional Court (Grondwettelijk Hof, 2023)). The VTC is, therefore, only focused on the public authorities of the Flemish region and is in charge of providing them with advice on the matter of data protection.

841. In June 2021, the VTC published guidance on the procurement of software services and suppliers by public authorities in the Flemish region. It took note of the Flemish Government's

ambition to provide all pupils in the fifth and sixth years of primary education and the entire secondary education with an individual ICT device. However, it expressed concern about potential unintended side effects (VTC, 2021).

842. The authority highlighted that certain suppliers were unable to provide sufficient guarantees regarding the protection of children's data. This was particularly relevant for suppliers whose business model relied on the trading or commercial exploitation of personal data. Even if suppliers excluded the direct provision of advertising, there remained a risk that data could be used for other commercial purposes (VTC, 2021).

843. The VTC recommended that the government refrain from hastily purchasing such devices. It advised incorporating data protection criteria into the specifications of the public purchase, emphasizing adequate information security and limiting the use of data to the provision and organization of education. Furthermore, the VTC suggested selecting alternatives that offer the widest range of options for adjusting effective privacy settings effectively, ensuring that these settings are appropriately and thoroughly privacy-oriented. Finally, it urged the government to prepare the educational institutions that had already made investments in this regard for a transition aligned with these points of attention (VTC, 2021).

844. In June 2023, the VTC published a position on the use of Google Workspace for Education by primary and secondary schools in the Flemish region (VTC, 2023a). Referring to the previous guidelines mentioned above, it provided more details on this specific technology. The DPA highlighted the unequal relationship between Google and the individual schools and found it positive that the Department of Education and Training and the educational umbrella organizations have taken the initiative to enter into discussion with Google to negotiate better conditions for Flemish primary and secondary education, as happened in the Netherlands (which will be described in section 10.6). These Flemish authorities have then requested the VTC's opinion on the matter before agreeing to the proposal made by Google.

845. The VTC intended to first discuss Google Workspace for Education's privacy settings and, in a later consultation, the security vis-a-vis the supplier itself and third parties. Due to a Non-Disclosure Agreement, the authority had little knowledge about the actual terms of the agreement and had to seek information from Google itself, whose answer was considered not transparent enough (VTC, 2023a). Below are some highlights related to Google's answers and the respective comments issued by VTC (VTC, 2023a):

i. The VTC found it concerning that ambiguities still existed regarding the roles and responsibilities of Google and schools within the GDPR. It should be evident when Google has any influence over the means and purposes of the data processing activities, potentially leading to its classification as a controller. The fact that this could change without schools' knowledge was also troubling, given Google's ability to unilaterally alter its ToS and Privacy policies. The VTC considered it unrealistic for schools to be regarded as controllers in certain data processing activities, taking into account the widely varying and sometimes limited expertise they have.

ii. When schools are considered controllers, they are required to conduct DPIAs in accordance with art. 35 of the GDPR, concerning their intended use of Google Workspace for Education. The VTC also observed this requirement to be challenging and impractical, given that the majority of schools lack the necessary resources and expertise, as well as visibility into the risks dependent on Google's actions. Furthermore, conducting a DPIA does not guarantee that the essential technical and organizational measures, including the implementation of suitable privacy settings, have been effectively addressed.

iii. Google stated that it would address the concerns of Flemish schools if they were similar to those of the Dutch public sector. The VTC noted that this assumption relies on schools being aware of the concerns of the Dutch public sector and that Google should bear the responsibility for developing appropriate solutions.

846. The authority highlighted that the solutions in the Netherlands are not guaranteed to be sufficient in the Flemish case (VTC, 2023a). It was of the opinion that the developments in the Netherlands case must be followed up and that similar concessions and guarantees must be obtained for Flemish education. Based on this, it advised that:

i. Flemish schools using a limited number of Google applications should discontinue them unless adequate protective measures are taken, if at all possible.

ii. For schools that have their ICT structurally embedded in Google, its use must cease by September 1, 2024, unless adequate protective measures are implemented, which should be at least equivalent to the safeguards negotiated

in the Netherlands. The VTC expects an exit plan to be drawn up in the meantime.

iii. All schools using Google should be guided to achieve minimal data protection impact.

iv. Switching to Google or new applications is not permissible until conclusive guarantees are provided that ensure effective management and protection of data in compliance with the data protection framework.

v. Alternatives can be provided by the education umbrellas with support from the ministry.

10.2 Denmark

847. The Helsingør municipality in Denmark distributed Google Chromebooks installed with G-suite for education (now Google Workspace for Education) for its schools. While accessing YouTube with their school's accounts, students' full names, school, and class were displayed in their posts, unless aliases were used by the school, which prompted a complaint to the Danish DPA in December 2019. On 29 January 2020, Helsingør Municipality reported a personal data breach to the Danish DPA (Datatilsynet - Danish Data Protection Authority, 2021, 2022c). The Authority has also received other complaints related to this and other Municipalities, highlighting the absence of parental consent for the creation of the Google account and the parents' inability to correct or anonymize the information displayed while using it.

848. The Municipality argued that another legal basis was used rather than consent, i.e., the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It also stated that it was not aware of the changes made in 2019 to Google's ToS, when several add-ons, including YouTube, were made available through the school account. In the Municipality's opinion, the information shared with YouTube was ordinary and Google had already access to it through G-Suite, which would not demand a DPIA (Datatilsynet - Danish Data Protection Authority, 2021).

849. The Danish DPA's September 2021 decision clarified that the Municipality could use art. 6(1)(e), GDPR, to justify the provision of Chromebooks and core Google Workspace for Education applications, as well as the processing activities related to the creation of the individual user. However, data disclosed to other controllers to be used for their own purposes,

such as the collection of metadata for marketing and profiling, would not be covered by the Municipality's exercise of authority (Datatilsynet - Danish Data Protection Authority, 2021).

850. The authority emphasized that the core services could have been configured in a way that: a) the processing activities do not exceed what is permissible under the Danish Primary and Lower Secondary Education Act; b) students' information would have been reduced to aliases; c) only the authorized profiles would be able to access data; d) data was not processed outside the EU/EEA (Datatilsynet - Danish Data Protection Authority, 2021).

851. Based on the above, the authority found that the Helsingør municipality has violated:

a) Art. 4(12), GDPR, because in several cases students' full name were used, where an alias could have been applied instead;

b) Art. 5(1)(a), due to the lack of lawfulness of the processing activity;

b) Art. 5(1)(c), 5(1)(f) and 5(2), GDPR, because of the lack of documentation of the considerations of risks to data subjects' rights and the assessment of the processing carried out. Furthermore, it failed to demonstrate which system configuration was used and whether safety measures were ensured at that time of the data processing;

c) Art. 32(1), by not having taken appropriate organizational and technical measures to ensure a level of security appropriate to the risks posed by the processing of data, especially within the context of additional services such as YouTube;

d) Art. 33(1), GDPR, by not having notified the DPA within 72 hours after the municipality had become aware of the personal data breach;

e) Art. 35(1), GDPR, because the use of new complex technology, especially in the field of education where children's data are processed, would entail a high risk to their rights and freedoms. This is particular pertinent when part of Google's business model is rooted in data collection and sale, as well as targeting advertisement.

852. The municipality was then ordered to bring the processing under compliance (Datatilsynet - Danish Data Protection Authority, 2021).

853. After assessing the new efforts and documentation provided by the municipality, the DPA found, in July 2022, that the processing of students' data did not meet the requirements of the GDPR and should be banned. Although Helsingør Municipality was considered to have done a significant and proficient job of mapping out how personal data is used in primary schools, the DPA highlighted how easy it is that data protection issues arise with the approaches

used by major tech companies (Datatilsynet - Danish Data Protection Authority, 2022c). The authority referred to its overarching work on the use of Chromebooks and Google Workspace for Education in Danish municipalities, indicating that this decision will probably likely extend to other municipalities using similar data processing structures.

854. In this second decision, the DPA found that the provided risk assessment generally addressed the most important scenarios and threats (Datatilsynet - Danish Data Protection Authority, 2022c). However, it failed to outline the risk scenarios stemming from the data processor design and the decisions made regarding the system. More specifically, this applies to the actual handling of personal data by the devices and applications, as well as to how Helsingør Municipality controls Google's access to personal data. This includes Google Chromebook's operating system and the interaction of Google Workspace with Google's backend concerning the necessary separation of personal data as mandated by the data processing agreement. This means that the Municipality has not demonstrated that personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.

855. In relation to the use of information for other purposes, the DPA emphasized that the Danish Primary and Lower Secondary Education Act establishes a list of lawful data processing activities, meaning that data must not be further processed. The Helsingør Municipality was only using Google Workspace for Education's core services and these do not process data for marketing purposes. However, the Municipality stated that a possible breach of the contractual obligations could not be ruled out, which would go against art. 28(1), GDPR, according to the DPA. The DPA was of the view that the data controller could only contract data processors who could guarantee their compliance with the data protection rules. Therefore, the mere expectation that it could breach the data processing agreement means that this data processor could not be selected by the controller (Datatilsynet - Danish Data Protection Authority, 2022c).

856. Although the Municipality framed this risk only as hypothetical, the DPA found that if it materialized, there would be a significant infringement upon the rights of the data subjects. No effective technical or organizational measures were documented to reduce this risk, and any risk involving high consequences for the rights and freedoms of data subjects, even when they are unlikely to be realized, should trigger the obligation to carry out a DPIA. The Municipality, therefore, also acted in breach of art. 35(1), GDPR (Datatilsynet - Danish Data Protection Authority, 2022c).

857. Regarding data transfer to third countries, the Municipality argued that, in general, data processed within Chromebooks and Google Workspace for Education would remain within EU data centers. However, there was still a risk that the support access was provided in third countries, which would demand a data transfer. The contract between the Municipality and Google included standard clauses pursuant to art. 46(2)(c), GDPR, as a basis for the transfer. However, the Danish DPA found that the transfer in question is covered by conditions in the USA that prevent the standard clauses from being a sufficient means of ensuring a level of protection that essentially corresponds to the level within the EU/EEA. Helsingør Municipality would be, thus, obliged to ensure that additional measures are put in place to bring the level of protection up to the required level.

858. According to the Helsingør Municipality, personal data was encrypted both in transit and at rest when the data were transmitted to and processed by Google, but Google would still be able to access the information in plain text, which does not guarantee sufficient protection. The DPA found, therefore, that the transfer does not occur in accordance with art. 44, GDPR, and that should be suspended until the Municipality demonstrates that provisions of Chapter V, GDPR, have been observed (Datatilsynet - Danish Data Protection Authority, 2022c).

859. After reviewing the material sent by the Municipality in early August 2022, the Danish DPA issued a new decision upholding the ban (Datatilsynet - Danish Data Protection Authority, 2022b). This time, the DPA prohibited Helsingør Municipality from processing personal data using Google Chromebooks and Workspace for Education.

860. A day after this decision, a meeting was held between the DPA, Helsingør Municipality, Local Government Denmark—the association and interest organization of the 98 Danish municipalities—and the Danish Agency for IT and Learning (Datatilsynet - Danish Data Protection Authority, 2022e). The meeting aimed to establish a shared understanding among the involved parties on how schools could legally use Chromebooks and Google Workspace for Education. In the meeting, Helsingør Municipality recognized the considerable risk associated with the data processing, and, as a result, all parties committed to quickly collaborate to bring the municipality’s adoption of the technologies into compliance.

861. In September 2022, the Danish DPA lifted the ban but issued an order for compliance (Datatilsynet - Danish Data Protection Authority, 2022a). A similar injunction has been issued to Aarhus Municipality. This meant that students could resume using Google Workspace, but their permanent use would be subject to the handling of several issues related to contracts,

technology, and documentation by the Municipality. The DPA received additional material from the municipalities in November 2022 (Datatilsynet - Danish Data Protection Authority, 2022d), and, in December 2022, the association of the local governments—on behalf of the approx. 50 municipalities that use Google Workspace for Education—informed the DPA that they would submit further material in the case. Against this background, the DPA extended the documentation deadline to January 23, 2023, without issuing a new decision yet (Datatilsynet - Danish Data Protection Authority, 2022f).

10.3 Finland

862. In April 2018, the *Tietosuojavaltuutettu* (Finish Data Protection Ombudsman) initiated an investigation related to the use of Google Suite for Education (now Google Workspace for Education) in a school within a municipality of Finland. More specifically, the DPA assessed (i) whether art. 6(1)(c) of the GDPR could be applied as a legal basis for processing personal data and (ii) whether the controller has appropriately ensured that international data transfers took place in accordance with data protection framework (Tietosuojavaltuutettu, 2021).

863. In its statement, the controller specified that it processes students' data to comply with a statutory obligation, more specifically to provide basic education in accordance with the Finish Basic Education Act. The DPA was of the opinion that the law does not provide the specificities of the processing activities, and fulfilling this obligation as such would not require the use of digital technologies. The means of data processing are not defined by the law, and it leaves significant discretion to the controller in the processing of personal data (Tietosuojavaltuutettu, 2021).

864. According to the authority, when the legal basis for processing personal data is compliance with a legal obligation, the law imposing it must fulfil all relevant conditions for the obligation to be valid and binding. It must also meet the requirements of data protection legislation, including necessity, proportionality, and purpose limitation and the controller must not have a choice as to whether or not it can comply with it. Therefore, voluntary unilateral commitments and public-private partnerships that process data beyond what is required by law would not fall within the scope of this legal basis (Tietosuojavaltuutettu, 2021).

865. In this specific case, the DPA draws attention to the fact that digital technologies would process more data than traditional teaching activities. The DPA considers that, due to the various options available for providing education online, it would not be justified to

automatically consider the processing activities within this specific platform as necessary and proportionate. Instead, the controller should justify the processing of students' data on a case-by-case basis, according to its statutory obligation to provide basic education (Tietosuojavaltuutettu, 2021).

866. When assessing other possible legal bases for processing students' data by the municipality, the DPA considered that consent cannot be freely given if the data subject does not have a genuine free choice and cannot refuse or withdraw consent without detriment. This does not imply that it should be outrightly disregarded in instances where there is a power imbalance between the controller and the data subject. However, the controller would need to demonstrate the voluntary nature of consent and ensure that data subjects who refuse to provide their consent are offered a genuine, equal alternative (Tietosuojavaltuutettu, 2021).

867. Apart from the analysis regarding the legal basis, the authority highlighted that by accepting the standard ToS offered by Google, the controller has affected its ability to properly control and supervise the processing of personal data. The DPIA carried out by the controller itself recognizes the risks arising from the general terms and conditions. According to the municipality, since the terms and conditions are general and partly difficult to interpret, there is a risk that the processing activities are not defined in a sufficiently transparent and clear manner. The ombudsman also notes that the technology is not only used within the school but also in students' homes and own devices, which would require the data processing activity to be voluntary in these cases (Tietosuojavaltuutettu, 2021).

868. According to the DPA, due to its obligations related to data protection by design and by default, the controller must assess all functionalities of a service, especially when it is provided for free. It should pay attention to the type of service entity, how the controller is determined when using different parts of the service package, and which contract terms will be applied at any given time. Finally, the controller also failed to implement encryption, as the method used is considered outdated in terms of data security (Tietosuojavaltuutettu, 2021).

869. When it comes to data transfers to third countries, considering the existence of personal data transfers from the EU to the USA and the Schrems II ruling. The DPA requested information from the controller on whether it has introduced additional safeguards after the annulment of the Privacy Shield, which was not confirmed.

870. Based on the above, the DPA considered that art. 6(1)(c) of the GDPR does not apply to the processing of personal data, which means that the processing activities violated the

GDPR. The controller was reprimanded and ordered to bring processing operations into compliance. Regarding the international data transfers, the Municipality was ordered to notify the DPA of the measures it has taken as a result of the EDPS guidance on the matter (Tietosuojavaltuutettu, 2021).

10.4 France

871. In August 2022, a member of the French National Assembly, Mr. Philippe Latombe, raised concerns with the French Minister of National Education and Youth regarding the use of Microsoft Office 365 in schools. He emphasized that while free services might appear attractive, they pose risks to competition and data sovereignty (Assemblée Nationale, 2022b, p. 3866).

872. In his written response, the French Minister explained that, according to the French Public Procurement Code, public procurement contracts are typically intended for pecuniary interest to meet specific needs of public entities in terms of works, supplies, or services. Therefore, free offers of services would be, in principle, excluded from the scope of public procurement (Assemblée Nationale, 2022b, p. 3866). The Minister acknowledged that providing schools with a free office suite is probably meant to familiarize the public with the tools, increasing the likelihood of them later subscribing to the paid version. However, he considered that this indirect benefit does not make the service onerous in itself (Assemblée Nationale, 2022a).

873. The Minister also referred to several documents and recommendations: a) the Prime Minister's Circular No. 6282-SG on the Cloud at the Center Doctrine; b) a note from the Interministerial Director of Digital Affairs (*Directeur Interministériel du Numérique* - DINUM) dated September 15, 2021, indicating that Microsoft Office 365 did not comply with the Doctrine; and c) a letter from the Commission Nationale de l'Informatique et des Libertés (CNIL) dated May 27, 2021 (Commission Nationale de l'Informatique et des Libertés (CNIL), 2021), recommending that higher education institutions use collaborative suites offered by providers subject to European law, which host the data within the EU and do not transfer them to the USA. The Minister added that this also applied to Google Workspace for Education.

874. The Cloud at the Center Doctrine, adopted by the French Government, highlights that the cloud has become the default mode of hosting and producing the state's digital services. It aims at meeting French people's legitimate expectations of an exemplary state in terms of

protecting their data and guaranteeing the continuity of the public service, two prerequisites for their confidence in the digital public service. The digital services offered by the administrations must then be hosted on one of the two internal interministerial clouds of the state or on Cloud offers of manufacturers that meet strict security criteria (Borne, 2023; DINUM, [*s. d.*]).

10.5 Germany

875. In August 2018, Microsoft announced the end of its collaboration with Deutsche Telekom in providing Microsoft cloud services, including Office365, under strict German jurisdiction (the so-called German Cloud) (Dedezade, 2018). Under this agreement, data was handled by a trustee under German rules and Microsoft employees had no access to them (Poortvliet, 2018). After this decision and having received several complaints from teachers and school administrators, in July 2019 the German Land of Hesse's DPA prohibited the use of Microsoft Office 365 in schools since children's data were being stored in a European Cloud. The same decision was also extended to Google and Apple services using a similar cloud.

876. The rationale was based on several arguments. First, with the by then newly enacted USA Cloud Act, USA government agencies could request access to customer data from all USA-based companies even when the servers were outside the USA's territory. Second, it stressed the responsibility of German public institutions regarding data processing legality and traceability (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019a). The decision also mentioned the need for guaranteeing the state's digital sovereignty; and the unclear nature of telemetry data transmitted to Microsoft (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019a). Concerns that Windows 10 and 11 operating systems collect telemetry data had already been expressed by the Germany's Federal Office for Information (BSI, in German) (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018). Finally, the DPA stressed that gathering parent's consent would not be a solution to the issue, as the security and traceability of the data processing were not guaranteed.

877. A month later, however, the ban was lifted by the Supervisory Authority, which decided to "temporarily tolerate" the use of Office 365 in Hessian schools under certain conditions and subject to further examination (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019b). This happened after negotiations with Microsoft and a change in the DPA's assessment, which refuted some of the concerns. One of the applied safeguards was

preventing the transmission of any kind of diagnostic data. Google and Apple services were not mentioned in this second decision.

878. Specifically regarding Microsoft Office 365, it also faced bans in 2020 by the State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Wüttember, 2022), as well as in 2022 by North Rhine-Westphalia Data Protection Authority (Brinkmeyer, 2023; Gayk, 2023). This decision was confirmed in 2021 (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Wüttember, 2021). In November 2022, the German Data Protection Conference (DSK, in German)—the committee of Independent German Federal and State Data Protection Supervisory Authorities—published a the report of the DSK working group on Microsoft 365, concluding that the software still did not comply with the GDPR (Datenschutzkonferenz, 2022). The extension or applicability of this decision to other similar technologies, such as Google Workspace for Education, is still not confirmed.

879. The use of Google Services was also prohibited at one of Dortmund's seven secondary schools, after a student's privacy concerns led to his refusal to use the platform in 2021. Despite the school offering an alternative solution, it was rejected as it was believed that participating in school activities without discrimination was not possible. Unable to use the same tools as their peers, the student could not engage in visual exchanges with teachers, submit his/her homework, and upload solutions, as the communication was only done via email. The student eventually filed a complaint with the Petitions Committee of the State Parliament, and, after some appeals, the case reached the Higher Administrative Court of North Rhine-Westphalia (mrtee, 2023a).

880. Google Workspace for Education has been procured by the school itself but the latter was unable to prove the data protection conformity of the platform. Following the discussions, the judge presented a proposal to the representatives of the Arnsberg district government, which would ensure that Google Workspace for Education would no longer be adopted and students would use a platform whose compatibility with national and European data protection law has been checked (mrtee, 2023a). The Arnsberg district accepted the proposal and the school announced on its website that it has been instructed to discontinue the use of Google Workspace for Education after Easter Holidays 2023 (mrtee, 2023b).

10.6 Netherlands

881. In February 2021, SURF—the collaborative organization for IT in Dutch education and research (SURF, [*s. d.*])—and SIVON—a cooperative of school boards in primary and secondary education (SIVON, [*s. d.*])—disclosed that a DPIA of Google Workspace for Education had been commissioned by the University of Groningen and Amsterdam University of Applied Sciences (SURF, 2021c).

882. Completed on 15 July 2020, the DPIA identified ten high[29] and three low[30] data protection risks affecting data subjects when they used Google Workspace for Education (Nas, Sjoera; Terra, 2021). More specifically, it found that Google could not qualify as a data processor for the collected personal data, and, as joint controllers, Google and the universities lacked legal grounds for their processing activities. According to surveys conducted by SURF and SIVON, Google Workspace was employed by 52% of primary schools and 36% of secondary schools in the Netherlands. It was also used by certain faculties within 4 out of the 14 universities and 4 out of the 36 government-funded universities of applied sciences across the country (Nas, 2021).

883. After providing the first version of the DPIA to Google, discussions took place until January 2021, during which Google implemented various technical and organizational measures to mitigate risks, particularly regarding consumer data (Bonamigo, 2021). For example, measures were taken to prevent spill-over of personal data, such as when end-users access additional services with their Google Account, as well as to address privacy-unfriendly default settings (Nas, Sjoera; Terra, 2021). However, only these two of the ten high risks had been completely mitigated.

884. Due to the remaining risks identified by the DPIA, SURF and SIVON asked for advice from the Dutch Personal Data Authority (Autoriteit Persoonsgegevens, AP). Based on the documentation provided by the two institutions, the AP advised them (and therefore the educational institutions they represented) not to start or continue using Google Workspace for

[29] The ten high data protection risks identified by Privacy Company were: Lack of purpose limitation (in relation to customer data); lack of purpose limitation (in relation to diagnostic data); lack of transparency (in relation to customer data); lack of transparency (in relation to diagnostic data); lack of lawful grounds for processing personal data; missing privacy controls; privacy-unfriendly default settings; the use of multiple Google accounts; lack of control of subprocessors; lack of access by data subjects to their personal data.

[30] The three low data protection risks identified by Privacy Company were: Unlawful access to customer data and diagnostic data in the USA by the cloud provider; the chilling effect generated by the employee monitoring system; and the impossibility of deleting individual diagnostic data.

Education before the problems raised were solved (AP, 2021a). More specifically, the authority advised them to determine a) which processing of personal data takes place and for which purposes; b) which parties determine the purpose and (essential) means of the processing activities and the roles they assume as a result; c) the lawful bases for the intended processing activities; and d) the specific risks related to the processing of children's data, insofar as applicable for the relevant educational institution(s). In the same document, the AP warned that if SURF and SIVON could not reach an agreement to sufficiently mitigate the risks related to Google Workspace for Education, it should be phased out before the start of the 2021/2022 school year.

885. The AP also addressed two letters to the Dutch Minister for Primary and Secondary Education, and Media, and to the Dutch Minister of Education, Culture, and Science (AP, 2021c, 2021b). They were advised to coordinate efforts, including within the EU with other MS; inform educational institutions about their responsibilities; explore which digital resources are commonly used by educational institutions; and having them carry out DPIAs. Furthermore, specific actions related to Google Workspace for Education should be taken, such as communicating the outcomes of the advice to educational institutions, mapping which of them used the software, and investigating the possibilities for educational institutions to take measures independently to reduce risks. In a letter sent to the House of Representatives in June 2021, the Ministry of Education, Culture and Science said it expected Google to resolve the identified issues before the start of the 2021/2022 school year (Ministry of Education, 2021).

886. In July 2021, Google and the educational institutions reached an agreement to sufficiently mitigate all high risks identified in the DPIA (SURF, 2021a). These measures mostly applied to Google Workspace for Education's core services, but Google has committed itself to continue discussions with SURF and SIVON to solve issues related to the Google Cloud Platform and Chrome OS (the operating system for the Chromebooks) (SURF, 2021a). This meant that the education institutions could resume Google Workspace for Education use, provided that specific measures were applied (SURF, 2021b).

887. A new DPIA report was then requested by SURF and SIVON to Privacy Company, which was published in August 2021. The report shows that Google had finally agreed to lower the eight remaining high data protection risks (Nas, Sjoera; Terra, 2021). For instance, Google has agreed to act as a data processor for the Diagnostic Data about the individual use of the services; to implement measures to increase transparency; and to develop a processor-version of the Chromebooks and the Chrome browser (Nas, 2021). Google remained as a data controller

for additional services and would not provide additional safeguards in relation to them. In this case, students would need to use them with a personal account.

888. The new DPIA also directly addressed children's data processing and consent for additional services, which was previously omitted. Privacy Company explained that Google was found to be a data controller for the additional services. If they were used in schools, consent from end-users would need to be obtained. However, there was clearly an imbalance of power between schools and parents/children, as they are frequently not in a position to refuse the service, and their consent would most probably not be valid (Nas, Sjoera; Terra, 2021).

889. Before September 2021, Google would automatically log students out of their school accounts when they accessed additional services, and their data would be anonymized. However, Google has discontinued this option. When using YouTube, for instance, students were limited to viewing content without the option for anonymous interaction. Additionally, even though they were not subjected to personalized advertisements, students were still exposed to contextual ones. Consequently, the DPIA anticipated that the only viable course of action would be for schools to disable these additional services. When teachers desire to use any YouTube video, for example, they should embed them within Google Classroom (Nas, Sjoera; Terra, 2021). It should be noted, however, that the risk of creating personal accounts should also be considered by schools. Although they can technically prevent access to additional services at the school environment, as well as simultaneous log-in, they would not be able to prevent students from creating a personal account (Nas, Sjoera; Terra, 2021).

890. The agreement was said to prompt global changes in Google Workspace for Education data processing (Crandall, 2022b), which as we saw in the Belgian case (and will see in the Brazilian case), was not actually the case. Considering that some schools might need to carry out DPIAs for their specific cases, Google also created a Cloud DPIA Resource Center (Crandall, 2022a; Google, 2023d).

891. In December 2022, SIVON and SURF reported Google's progress in addressing the risks identified in the 2021 DPIA, with ongoing efforts to solve remaining issues by mid-June 2023 (SURF, 2023b). Despite negotiations, the DPA was still concerned about the Minister's additional findings, especially if any substantial privacy risks for students remained. On 8 March 2023, the AP issued a letter to the Dutch Government asking for urgent clarifications regarding the possibility of using Google Workspace for Education in schools in a lawful manner before the beginning of the 2023-2024 academic year (AP, 2023).

892. On 20 April 2023, the Ministry of Education, Culture, and Science informed the House of Representatives how the advice from the DPA was followed (Ministerie van Onderwijs, 2023). It explained the agreements made between SIVON, SURF, and Google and the fact that schools would receive instructions about Workspace for Education by mid-June 2023 (SIVON, 2023). A verification report was issued by Privacy Company confirming the measures implemented by Google (Nas; Terra, 2023). However, the new assessment revealed new potential risks, which were meant to be discussed separately between SURF, SIVON, and Google.

893. Regarding the separate negotiations on the ToS governing the utilization of Chrome OS and the Chrome browser on Chromebooks, SURF and SIVON reached another agreement with Google in May 2023. Under these revised ToS, Google would be a data processor in relation to "essential services" (SURF, [*s. d.*]), while additional services would need to be turned off by the administrator (SURF, 2023c). The new processor version would become available in August 2023. Additional agreements were made to eliminate other privacy risks (SURF; SIVON, 2023), and an inspection report was published (Terra *et al.*, 2023). This allowed SURF and SIVON to conclude that Dutch educational institutions could continue to use Google Workspace for Education and Google Chromebooks (SURF, 2023a).

894. Finally, it is important to mention that a separate process started in the beginning of 2023 to address concerns pertaining to data transfers, particularly to the USA. A Data Transfer Impact Assessment (DTIA) was underway and was anticipated to conclude in autumn 2023 (SURF, 2023a).

10.7 Norway

895. Although not part of the EU, Norway is part of the EEA and adopts the GDPR. As per the Decision n. 154, of the EEA Joint Committee, the EEA countries not part of the EU are also members of the EDPB, although without voting rights and the right to be elected as chair and vice-chair. Therefore, the decisions taken by the Norwegian DPA, Datatilsynet, are also relevant for this part of the thesis, where the violations of the GDPR are analyzed.

896. In Norway, several municipalities have adopted Google Workspace for Education in primary and lower secondary schools. Based on some parents' complaints coming from parents, the DPA has taken a closer look at three of them (Datatilsynet - Norwegian Data Protection Authority, 2020b).

897. Although based on different complaints and different grounds, the decision taken in relation to these three municipalities were focused on the same four issues identified by the authority: (i) the municipalities have not kept a log of processing activities taking place on students' Chromebooks and in G Suite for Education; (ii) they have not implemented appropriate technical and organizational measures to achieve a level of security appropriate to the risk; (iii) they have not conducted a privacy impact assessment of the use of Chromebooks and G Suite for Education in schools; and (iv) they have not provided adequate information to enable students and parents to safeguard their interests and privacy when using Chromebook and G Suite for Education (Datatilsynet - Norwegian Data Protection Authority, 2020e, 2020c, 2020d).

898. With respect to maintaining a record of processing activities, Sandnes municipality has stated that no protocol has been created for processing activities related to the use of Google Chromebook and G Suite for Education. In Strand municipality, a protocol has been created, but upon revision of the DPA, several shortcomings have been identified, such as the legal basis used for processing students' data. Although the municipality would rely on the performance of a contract and consent, the DPA was of the opinion that the processing was necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The same issue was detected in the Bergen municipality case. While the municipality considered that a legal obligation would be the appropriate legal basis, the DPA recommended using art. 6(1)(e) instead. In the Bergen municipality case, the DPA also found that the purposes for data processing were not specific enough.

899. The DPA also stated that when acquiring hardware and software to be used in schools, municipalities must carry out a risk assessment based on art. 32, GDPR, to analyze the security of the processing. This was not conducted by Sandnes municipality. Strand and Bergen municipalities have provided a risk assessment to the DPA, but the latter considered that they have not implemented sufficient measures to keep themselves informed of future changes to Google's ToS, which would result in more risks to students.

900. With regard to the assessment of data protection risks, the DPA was of the opinion that a DPIA was mandatory in the case of implementation of the platform by the municipalities. These processing activities would meet at least two criteria present in the DPA's guidance on DPIAs: the involvement of vulnerable subjects and the innovative use or application of a new technological or organizational solution (in this case, the use of cloud services in primary schools).

901. Finally, concerning the provision of sufficient information to data subjects in accordance with arts. 12 through 14 of the GDPR, the DPA held the view that municipalities have fallen short. Sandnes municipality asserts that this obligation was met by conducting a meeting with the children's parents, who then signed a form at its conclusion. However, this information was not supplemented by any information in writing, and parents were given only a few minutes after the presentation to sign the form. A similar situation occurred in Strand municipality. In the case of Bergen municipality, although the controller mentioned a meeting had taken place, the complainants argue that the information was rather provided in a fragmented way, which they considered insufficient.

902. The DPA found that the information given to parents was not enough to meet the GDPR requirements, especially because the service was targeted to children. Simply referring to Google's ToS was not considered enough. The DPA also mentioned the need for schools to provide clear information about where their responsibility stops and the parents' responsibility begins. If it is the case that the children can use the Chromebook for private purposes, and log in with private accounts through the browser, the municipality should clearly inform about the privacy risks that may arise from private use.

903. After dealing with these three cases, the DPA issued guidelines applicable to all municipalities within Norway mainly focused on Google Chromebooks and Google Workspace for Education, but also very much transferable to other cloud services (Datatilsynet - Norwegian Data Protection Authority, 2020a).

10.8 Spain

904. In the case of Spain, two decisions are important for the scope of this thesis. The first decision originated from a complaint of a parent, dated July 2021, who argued that they were not consulted for the implementation of G Suite for Education (now Google Workspace for Education) in a school under the organization of the Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias. According to the Spanish DPA, Agencia Española de Protección de Datos (AEPD), the now Google Workspace for Education gained prominence with the onset of the COVID-19 pandemic as a digital tool in Spanish schools due to the absence or insufficient resources available to them (AEPD, 2023a).

905. The first data protection issue identified by the DPA in this case was the lack of proper information provided to the data subjects as per art. 13, GDPR. The authority listed several

elements that were missing from the documents provided by the school to parents and students. It considered this particularly concerning because consent served as a legal basis for processing students' data and, in certain situations, students themselves would provide consent if they were aged 14 or older. The DPA considered that the language of the documents was not clear and simple so a minor could understand. This issue has, therefore, led to the lack of a proper legal basis for processing personal data, which would also infringe art. 6(1), GDPR (AEPD, 2023a).

906. The second element identified by the DPA was the incompleteness of the DPIA carried out by the controller. The controller used a template provided by the authority to identify the risks associated with the platform. However, it failed to identify specific risks related to Google Workspace for Education, which would prevent it to take adequate measures to address them, especially due to the involvement of minors. The DPA also considered that the controller's conclusions reached within the DPIA were not well-founded and logical in relation to the facts (AEPD, 2023a).

907. The second relevant decision of the AEPD is related to the use of Google Workspace for Education at Colegio Menor Nuestra Señora de Loreto. It also originated from a parent's complaint dated August 2021, who argued that consent had not been provided for the use of the tool within the school. The authority clarified that, in this specific case, the school would not need to request parents' consent, as it cannot be considered an adequate legal basis due to the power imbalance between the controller and the data subject. The appropriate legal basis in this case would thus be art. 6(1)(e) (AEPD, 2023b). This is an interesting conclusion, as in the previous case the authority has not questioned consent as an appropriate legal basis, just the appropriateness of the information received by the parents and data subjects.

908. Despite the legal basis not being deemed inappropriate, other issues were identified by the authority. The use of Google Workspace for Education in this specific school was implemented based on Google's ToS. The DPA considered that this agreement was not enough to clarify the roles and responsibilities between the controller (the school) and the processor (Google), as well as to implement the requirements of art. 28, GDPR (AEPD, 2023b).

909. A second issue identified by the authority was the lack of proper information related to the processing activities provided to the data subjects, which would be in breach of art. 13, GDPR. The DPA considered that the information given to parents and students was not presented in simple, intelligible, concise, and didactic language for easy understanding (AEPD, 2023b).

910. It is important to mention that there was an appeal to this decision from August 2023. The decision regarding the appeal was published in November 2023. The DPA considered that the appellant did not present new facts or legal arguments that would allow reconsideration of the validity of the challenged decision (AEPD, 2023c).

10.9 Sweden

911. The Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten - IMY) initiated a procedure to investigate whether the barn- och utbildningsnämnden (Children and Education Board), in Östersund Municipality, has failed in its obligation to conduct an impact assessment before the introduction of Google Workspace for Education in 24 schools in the fall of 2020 (IMY, 2023a).

912. In a response to IMY, the board stated that the Jämtland County Regional Council conducted a risk analysis of Google Apps for Education (now Google Workspace for Education) in 2014. The analysis showed that there were no significant risks in relation to the use of the service. In May 2020, the council decided to move the service to its own domain, and by June 2020, the service was active in the council's IT environment. However, after the migration, the Board identified shortcomings in managing the new domain (IMY, 2023a).

913. Although the migration assessment resulted in the same risks as the 2014 analysis, documentation was not prepared in accordance with applicable legislation, considering the relocation of the service to a separate domain. The board has initiated training for IT administrators to ensure that they can manage the service according to the instructions provided by the board. The next step involved conducting an audit, which was included in the consultation of the impact assessment. Since the audit has not been finalized, neither has the impact assessment. The latter would also include an analysis of whether the use of the service involves transferring personal data to a third country (IMY, 2023a).

914. In the decision, the DPA considered that the Board is the data controller for the processing of personal data when the service is used in the municipality's schools. It also provides examples of how the service is used and the types of data that are collected. The service is employed by schools, for instance, for teaching and communication, distributing planning and assignments to students, providing feedback to students, and facilitating communication between students when needed for specific assignments, etc. Examples of the data collected include first name, last name, email address, class, and group membership. Based on the data

collected in other cases described in this thesis, it seems likely that these are only the data directly provided by the school, and not data collected by Google itself to provide the services.

915. In September 2023, a communication from the Board to the DPA outlined the outcomes of an audit, which unveiled several risks that demanded further work to identify solutions. However, the safety deficiencies had been effectively addressed, with numerous safeguards already implemented. For instance, the Board signed an agreement with Google for an extended license, ensuring data encryption and facilitating the implementation of security protocols mandated by the audit within the municipality's IT infrastructure. Furthermore, the municipality has implemented policy documents, training programs, information management plans and restrictions on the storage/processing of personal data (IMY, 2023a).

916. The IMY observed that the processing activities involved 5,945 children within the context of education, wherein the data subjects are highly dependable on the controller. The large-scale processing and handling of data from vulnerable individuals already satisfied two criteria from the list developed by the authority based on art. 35(4) of the GDPR. Moreover, the impact assessment has not been completed even after three years of the beginning of the processing activities, indicating a high degree of negligence. Consequently, on November 30, 2023, the IMY imposed an administrative fine of SEK 300,000 (approximately 26 thousand euros) against the board of Östersund Municipality (IMY, 2023b). It is important to mention that this was the only situation of the cases analyzed in the thesis where there a fine was issued.

10.10 Brazil

917. The Brazilian Internet Steering Committee, through its Network Information Center, conducts an annual survey on the use of the internet and digital resources in Brazil. One of its surveys focuses on the use of ICT in education, which serves as a crucial and reliable source for understanding the Brazilian context where Google Workspace for Education is deployed.

918. The data for the 13th edition of the survey was gathered between May 2022 and October 2023, marking the first in-person data collection following the reopening of schools after the COVID-19 pandemic. Through the historical series of the survey, it is possible to identify an increase in the connectivity of Brazilian schools. According to the latest findings, 93% of public primary and secondary schools, and 99% of private schools now have access to the internet (Brazilian Network Information Center, 2023).

919. However, apart from universal connectivity (connectivity for all), it is also important to provide meaningful connectivity ("a level of connectivity that allows users to have a safe, satisfying, enriching and productive online experience at an affordable cost" (International Telecommunication Union (ITU), 2022, p. 2). The survey found, for example, that in municipal schools it is common for the internet connection not to support multiple simultaneous access (45%). Other issues such as a poor signal range within the school premises (38%), poor internet quality (35%), and frequent internet crashes (34%) were also identified (Brazilian Network Information Center, 2023).

920. In relation to the use of digital devices, mobile phones were the most popular among teachers (67%), while computers (53%) and tablets (14%) were mentioned less frequently. Among all teachers, 31% used their personal devices and 24% used school devices. 8% mentioned that mobile phones were the exclusive means for accessing the internet with their students. Within their households, 42% of students had portable computers, followed by desktop computers (31%) and tablets (26%). 83% of the students had a mobile phone of their own that could be used for educational activities (Brazilian Network Information Center, 2023).

921. When it comes to digital applications and platforms used within schools, 77% of them employed online class record books or student enrollment, grade, and attendance control systems. In the 2022 edition of the survey, 33% of the schools said they officially adopted a LMS, compared to 51% in the 2020 edition, most probably attributed to the return to in-person classrooms. Nevertheless, 47% of the teachers reported using a LMS and 48% reported using Google Classroom, indicating a misunderstanding of what is meant by a LMS (Brazilian Network Information Center, 2023).

922. Among the criteria used to choose an edtech, being free appeared as the primary factor for 69% of educators, surpassing even its suitability to the curriculum and learning objectives. The survey highlights, however, that data protection has also been a concern among educators. For instance, 27% of primary and secondary education schools have refrained from adopting an edtech due to these concerns (Brazilian Network Information Center, 2023).

923. Another significant endeavor mapping the Brazilian reality is conducted by the *Observatório Educação Vigiada* (Surveilled Education Observatory). Led by academic researchers and NGOs, this initiative is dedicated to collecting and disseminating information concerning the integration of platforms in public education across Brazil and South America (Observatório Educação Vigiada, [*s. d.*]). To map the presence of large technology companies

in Brazilian education, the project has developed software capable of identifying the storage location of official email servers used by public educational institutions. The results underwent a qualitative validation process through freedom of information requests.

924. According to the latest data, 51.22% of Brazilian state schools incorporate Google services in their educational systems, while 24.39% rely on Microsoft. Of the 52 municipal schools across Brazilian cities with populations exceeding 100,000**,** 14 use Google services, 10 use Microsoft, and 32 employ other services. Notably, 4 of these schools use both Google and Microsoft services simultaneously (Amiel *et al.*, 2021). Another research based on freedom of information requests made to the Education Secretariats of the Brazilian Central Government, the Federal District, and the states of Amazonas, Maranhão, Rio de Janeiro, and São Paulo, confirmed that all of them used Google Workspace for Education (Núcleo de Informação e Coordenação do Ponto BR, 2022)**.**

925. The increasing use of private platforms within education is directly linked to the lack of public investment in education, especially in ICT (Cruz; Venturini, 2020). Apart from economic crises and neoliberal policies, the COVID-19 pandemic created the need for a sudden adoption of technologies without a proper public debate on how this should be done. It caught governments off guard, as they were mostly not technically and organizationally prepared for the implementation of technologies supporting distance education overnight. The urgency in the decision-making and the lack of a holistic view of children's fundamental rights often led to the implementation and, to this day, the maintenance of problematic edtech. Before the pandemic, only 21% of Brazilian schools provided remote learning activities and the use of LMS grew dramatically between 2019 (28%) and 2020 (66%) (Brazilian Network Information Center, 2021)

10.10.1 The formalization of the relationship between Google and the schools

926. Having mapped all the partnerships carried out by Google and State Education Secretariats in Brazil until 2023, Lopes (2023) identified that the state of Minas Gerais was the first to establish an agreement for the provision of Google Apps for Education in 2009. Since then, out of the 27 Brazilian federative units, direct partnerships were not identified in only 4 of them.

927. In 2018, in collaboration with the Lemann Foundation, Google was already directly influencing the content taught in Brazilian schools. Within the NOVA ESCOLA policy, for

example, the organizations launched the first templates of digital lesson plans aligned with the National Common Curricular Base (BNCC)[31].

928. In 2019, the National Council of State Secretaries of Education (*Conselho Nacional de Secretários da Educação* - Consed)[32] was approached by Google to establish a partnership for the provision of Google Workspace for Education to the networks of state schools whose secretaries were signatories to the agreement. Despite this partnership, many states signed new agreements after 2020 due to COVID-19 in order to extend the duration of the partnership or include addendum terms (Lopes, 2023).

929. In 2022, the Brazilian Ministry of Education itself signed a partnership with Google for the implementation of Google Workspace for Education in federal educational institutions and making it available for other federative entities throughout the country (Nascimento, 2022).

930. Legal arrangements between schools and Google vary across the Brazilian educational landscape. In a study conducted by Amiel *et al.* (2021), which involved information requests to public educational institutions including State Education Secretariats, Federal Institutes of Education, and Federal Universities, diverse modes of adherence to Google and Microsoft technologies were observed. These include terms of cooperation, agreements, work plans, etc. In some situations, the object of the agreements is shaped to specify a mere technical consultancy service using expressions such as “encouraging the adoption of technology,” “providing solutions,” “promoting the improvement of educational actions,” and “creating an environment” (Núcleo de Informação e Coordenação do Ponto BR, 2022).

931. This legal relationship is frequently established directly through Google’s website, where schools accept its ToS and other policies. This contradicts the response to some information requests received by the researchers, which state that the school had no contract with Google, despite confirming its use. The ease of access to the services can lead to the erroneous conclusion that there is no legal relationship involved, particularly because it is perceived as a “free” service (Amiel *et al.*, 2021). Even in cases where the school does not use the technology, this does not imply a lack of ties with Google. On the contrary, one of the strategies used by the company is to directly contact teachers, laboratories, etc., which

[31] The BNCC is a public policy endorsed in 2017 that defines what each student is entitled to learn in school and directly impacts classrooms across the country (Consed, 2018).
[32] The National Council of State Secretaries of Education is an association founded in 1986, which brings together the Secretaries of Education from the States and the Federal District. Among its purposes are the integration of state education networks and the participation of states in the development of national policies, as well as collaboration among the federative units (Consed, [*s. d.*]).

facilitates the use of technology and circumvents the basic bureaucratic hurdles for its use by the school.

932. Partnerships between the schools and Google could also be formalized through intermediaries such as local start-ups that would embed Google Classroom in their apps (Derechos Digitales; Privacy International, 2022). Other type of intermediaries include foundations and other companies that fund a specific project where the app is used (Núcleo de Informação e Coordenação do Ponto BR, 2022).

933. In 2018 and 2019, Google conducted several presentations nationwide to showcase the company's applications, which included Google Workspace for Education, and to train professionals in their use (Leme, 2019). This is facilitated by the great amount of autonomy that states and municipalities have within the Brazilian legal framework.

934. Although the focus of this research does not revolve around public procurement rules, it is important to note that, according to Brazilian Law, cooperation terms should be used only when both parties share a common interest (aligned with the public interest) and no transfer of resources is permitted. These are instruments outlined in Law n. 13,019 (Brasil, 2014) and meant for establishing partnerships between the administration and civil society organizations. Although the law itself does not explicitly mention for-profit entities, the majority of Brazilian legal scholars argue that, considering the company's social function and the principle of solidarity, it would still be possible to establish partnerships not involving the transfer of funds between the state and for-profit entities, thus bypassing bidding laws.

935. The absence of monetary transfer, as previously explained, does not imply that the product can be considered free or that there is no economic interest on the part of the company in the contract. The existence of common interests, particularly aligned with the public interest, is also questionable. This is particularly serious when contracts are mostly standardized and easily signed over the internet.

936. Consequently, important steps that guarantee transparency and due process within bidding procedures are not followed. Art. 118, of Law n. 14.133, 2021, states that the provisions within this law could govern this type of agreement, where applicable, in the absence of a specific regulation. Thus, although cooperation agreements are *a priori* exempt from the specific rules of the bidding process, they are not entirely outside the scope of application of Law no. 14,133. In the absence of specific legislation for similar instruments, there is subsidiary

application of the legislation and, in particular, the dimension of constitutional principles of administrative law (Núcleo de Informação e Coordenação do Ponto BR, 2022).

937. This does not reflect the current Brazilian context, though. Other factors that should influence the procurement beyond the price of the product or service, such as the degree of protection of children's fundamental rights, are also not taken into account, as demonstrated by research conducted by Derechos Digitales and Privacy International (2022), as well as the data from Brazilian Network Information Center, mentioned above (2023). Cruz and Venturini (2020) also emphasize that some educational departments adopted Google's technologies because they were already used by teachers and students, making the transition to a remote/hybrid learning environment smoother. Another study shows that certain states adopted the technology based on its approval by other states in the country, indicating it had undergone some kind of vetting and testing (Núcleo de Informação e Coordenação do Ponto BR, 2022). Therefore, there is a real lack of acceptable grounds that justify the procurement of this technology in particular, beyond mere convenience and its free-of-charge nature.

10.10.2 Privacy and data protection issues

938. In order to use Google Workspace for Education, Brazilian schools must comply with various documents provided by Google. The Google Workspace for Education ToS (Google, 2023f) serves as the main contract between the parties, in the absence of a specific offline version. In addition, the use of the products is also governed by the general Google ToS (Google, 2022), the Google Cloud ToS (Google, 2023e), the Google Workspace for Education Privacy Notice (Google, 2023b), the Google's general Privacy Policy (Google, 2023d), the Google Cloud Privacy Notice (Google, 2023a), and the Cloud Data Processing Addendum (Customers) (Google, 2023c).

939. The Google Workspace for Education Privacy Notice is the primary governing document for the application suite and should take precedence in the event of any conflicting clauses with other notices. Within this document, Google delineates the distinction between core services and additional services already mentioned above to elucidate the implications each one has on the personal data of users. In the sections below I will focus on the main issues which are possible to assess based on the available data provided by Google and previous data identified in the literature review. They are going to be compared with the findings of EU MS competent authorities in Section 11.1, below.

10.10.2.1 Roles and responsibilities

940. When it comes to core services, Google makes a further rather artificial distinction between “information you provide or create with the core services (customer data)” and “information we collect when you use these services (service data)”. The distinction between customer data (data provided directly by schools, educators, students, or their parents) and service data (any other data collected by Google, such as observed data or inferred data) reinforces a narrative previously identified by Lindh and Nolin (2016). The data directly associated with the service’s benefits (front end) are presented and handled differently compared to the data more closely related to the back-end activities (and, therefore, to Google’s business model). The use of the term “service data” gives the impression that the collected data is not personal data and would not directly affect data subjects’ fundamental rights. This division adds an extra layer of complexity for schools, in addition to the existing one between core and additional services.

941. Google states that customer data provided or created within core services are processed according to the school’s instructions and does not mention the possibility of using them for its own purposes. In a separate section, Google mentions that service data are subject to the Google Cloud Privacy Notice. Unlike the case of customer data, there is no mention of Google acting under the school’s instructions (thus implying that schools are data controllers under LGPD). Given that the Google Cloud Privacy Notice is generic and applicable to all Google Cloud users (not necessarily just schools), there is also no mention of the respective roles and responsibilities regarding the protection of personal data between schools and Google.

942. Some of the aforementioned research sought to obtain, through information requests, the contracts made between states and municipalities and Google (Derechos Digitales; Privacy International, 2022; Núcleo de Informação e Coordenação do Ponto BR, 2022). Among the documents obtained, there were no agreements between the school and Google regarding the responsibilities of each party and how the data would be processed based on schools’ instructions. On the contrary, contracts were often signed directly online without any discussion about its clauses and necessary adaptations for the context of each school. This situation was also observed by the AEPD in one of the Spanish cases described above.

943. It is certainly possible that such documents exist but are not shared publicly, especially if they contain sensitive information. However, this scenario is highly unlikely, as this kind of document was not even mentioned in any of the responses, not even to state its unavailability.

Some public officials even claimed that the use of the platform did not entail personal data processing, which shows that data protection was not a concern. Thus, it is highly unlikely that Brazilian schools have real control over the purposes and means used to process personal data. At the very least, this would call into question the role of Google as a processor in the case of customer data and as a sole controller when it comes to service data.

944. Regarding additional services, the same division between data provided/created and data collected by Google is also applicable. However, in relation to these services, Google does not make any distinction regarding the responsibilities between the school and Google, which implies that it considers itself a controller for the processing activities within both types of services.

10.10.2.2 Purposes for processing personal data

945. The processing purposes described in the Google Workspace for Education Notice are provided in a non-exhaustive way. Data are processed to "provide, maintain, and improve services offered to students and schools; make recommendations to optimize the use of services; provide and improve other requested services; provide support; protect users, the public, and Google; and comply with legal obligations".

946. They should be complemented by the purposes described in Google's general Privacy Policy and Google Cloud Privacy notice when it comes to service data within the core services and all data within additional services. These purposes are also non-exhaustive and include processing data for providing, maintaining, and improving services; providing personalized services; measuring performance; communicating with the customer; and protecting Google, its users, and the public.

947. In the Google Workspace for Education Privacy Notice, Google underscores that core services are free from advertisement, and data is not processed for this purpose in other services. On the other hand, additional services may display advertisements, but are not personalized when these services are through accounts created by primary and secondary schools. Contextual factors like searches, time of day, or the content of the page content the student is viewing may still be used to tailor advertisements.

948. It is important to mention that, based on the principle of the best interests of the child and the guarantees provided in the CRFB, the CDC, and the ECA, advertising to children (whether based on their personal data or not) is prohibited in the Brazilian legal framework, and

such practice may also be considered abusive concerning adolescents (Henriques *et al.*, 2021; Henriques, Meira, *et al.*, 2020).

949. As will be emphasized in the section on transparency obligations, the purposes for which data are processed are extremely vague and non-exhaustive, which hampers the exercise of data subjects' rights and the analysis of compliance with various other parts of the LGPD.

10.10.2.3 Lawful Bases

950. In its ToS for Google Workspace for Education, Google states that schools can enable or disable any additional services at any time through the Administrator Console. Additionally, it states that they must "obtain parental consent for the collection and use of personal data in any Additional Products that the Customer intends to enable before allowing End Users under the age of 18 to access or use such Additional Products".

951. This statement brings with it many complexities that must be carefully analyzed. First, if Google considers itself a sole controller for the data processed within additional services, it should be the one responsible for selecting the appropriate legal basis for processing the data. If consent were at all applicable, Google should be the one to collect it based on its direct relationship with the user.[33]

952. Another issue that arises is related to the choice of consent for processing personal data within additional services. Considering the asymmetrical relationship between schools and students/their parents, and that education is mandatory in Brazil, it could not be considered freely given. Even if that were the case, it is difficult to identify how this would be operationalized in practice without violating other fundamental rights of children. Would the school have to provide different activities for students who do not consent to the use of additional services with their school account? How could this be implemented when the activity takes place in a group? What are the risks of the child facing discrimination at school?

953. Another issue is that, as discussed earlier, consent as a legal basis for the processing of personal data can be provided by individuals over 12 years old according to LGPD, not 18 years old. Thus, if this were an applicable and lawful basis in the specific case, Google could be

[33] As previously discussed in the EU cases, Google's access to data within additional services is facilitated by its legal relationship with schools. Consequently, schools would need to be considered joint controllers in this scenario.

violating the informational autonomy of adolescents by requiring parental consent, considering that it is their right to provide it independently.

954. Considering only the documents provided by Google, it was not possible to identify the legal basis used by schools to process student data through Google Workspace for Education in the core services as a controller or in the additional services if considered a joint controller. Most likely, according to the legal bases available in LGPD, schools would need to process them based on art. 7º, III (data processed by public administration, which are necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements, or similar instruments).

955. The Google Cloud Privacy Notice does not provide a clear list of the legal bases used for processing personal data, which unfortunately is not legally required by LGPD. In some sections of the documents, it is possible to infer that data are collected, for example, to fulfill legal obligations (in a section focused on the purposes of data processing), or consent (in a section focused on occasions when personal data will be shared with third parties).

10.10.2.4 Transparency obligations

956. According to art. 9º, LGPD, data subjects must have easy access to information about the processing of their data, which must be made available in a clear, appropriate, and conspicuous manner. It also lists the minimal information that should be provided to the data subject, including (a) the specific purpose of the processing; (b) the form and duration of the processing, while respecting commercial and industrial secrets; (c) the identification of the data controller; (d) contact information of the data controller; (e) information about the use of shared data by the data controller and its purpose; (f) the responsibilities of the agents who will carry out the processing; and (g) the rights of the data subject, with explicit mention of the rights contained in art. 18, LGPD. Apart from art. 9º, the controller should also consider art. 14, §6º, as explained above, when children's data are being processed.

957. In this section, I provide a brief analysis of the privacy policies applicable to Google Workspace for Education in Brazil, focusing both on their content and format in relation to transparency obligations. It is worth noting that art. 9º, LGPD, stipulates the issuance of guidance by the ANPD for compliance with the principle of free access. This guidance would discuss how this provision should be implemented, but it has not yet been issued. Therefore, it is not possible to define in advance the level of detail that will be required by the authority

regarding each of the items listed in the provision. It is already possible, though, to observe some inconsistencies between Google's policies and the LGPD, which will be discussed below.

958. When it comes to the format, the documents schools must agree to in order to use Google Workspace for Education are structured through engaging titles, and the language used can be considered appropriate for an average adult, with minimal legal jargon. Throughout the documents, certain icons and images related to the subject matter are used, which facilitates understanding, although this is not consistently applied across all sections.

959. Certain words and expressions also contain hyperlinks that redirect the reader to specific articles, providing more detailed information on certain topics. This is an interesting technique to provide both conciseness and the necessary detail, depending on the level of information sought by the user.

960. However, as previously explained, understanding how students' data are processed requires consulting at least seven different documents, which is a significant number by today's standards. Moreover, one of them is not translated to Portuguese (the Cloud Data Processing Addendum (Customers)), which can severely hinder the understanding of information by Brazilian schools and data subjects, as most of the country's population does not speak English.

961. Finally, it should be highlighted that the documents are the same for adults and children. Although the language may be considered suitable for adults, the same cannot be said for children, who will have limited comprehension of the provided information. Considering the wide range of different children who have access to the platform in the country, with different ages and backgrounds, it cannot be said that the policy complies with art. 14, §6º, LGPD, by presenting information in a simple, clear, and accessible manner, considering the user's physical, motor, perceptual, sensorial, intellectual, and mental characteristics. Audio-visual resources are also not used in a way that provides the necessary information to parents or legal guardians and is suitable for the child's understanding, as the same article mandates.

962. Regarding the minimal content that should be provided in the privacy policies, it is generally scattered around the different documents. As stated above, the specific purposes for processing data are listed in the Google Workspace for Education Privacy Notice, Google's general Privacy Policy, and the Google Cloud Privacy Notice. The applicability of each of the policies depends on the type of service (if it is a core or additional service) and the type of information that is collected ("customers data" or "service data"), which can already be confusing for the schools and the data subjects. Even when compliance with a requirement was

verified in one of the policies, this was not always the case for the others. This continues to be a violation of the LGPD, considering that the documents apply to different services and data processing activities.

963. As specified above, the lists of data that are collected and the purposes of the processing are not exhaustive and worded in vague terms such as “provide, maintain and improve the service”, “develop products” etc. While the extent of information required by the ANPD remains unknown, it is evident that the current level of abstraction is maximal. Given the limited details available, data subjects face challenges in effectively exercising their rights and maintaining control over their data. Beyond sparse examples scattered throughout the policies, Google fails to specify the form and duration of data processing, a deficiency that already violates Article 9, b, of the LGPD

964. The same observation applies to roles and responsibilities within the context of data processing. Not only do the policies fail to clearly delineate the roles, but they also do not specify the responsibilities of each party, particularly in cases of joint-controllership, nor do they provide guidance on whom the data subject should contact to exercise their rights. In instances where the school assumes the role of controller, this must be explicitly stipulated in a privacy policy drafted by them. However, this does not seem to be the case with the educational secretariats consulted in the aforementioned research.

965. In instances where Google is considered the controller, its identification and contact information (items c and d) are not directly available. While the Google Cloud Privacy Notice does specify the name of the data controller in Brazil, accessing this information is not straightforward. To address any uncertainties regarding the policy or to exercise their rights, data subjects must navigate through the Privacy Center. Here, they encounter numerous questions and answers about Google’s privacy policies. After several clicks, they can eventually access a data access form, which seemingly does not cater to other rights under LGPD and is only available in English.

966. In the analyzed documents, Google does not include information about the data shared with it, which constitutes a violation of art. 9°, LGPD. Despite detailing the circumstances under which data is shared with third parties, it fails to include a list of these partners. While this information is not explicitly mandated by art. 9º, LGPD, it would be crucial for effective data control. Even when the data subject is aware of the content of Google’s privacy policies, it holds little value if the individual is unaware of whom their data are shared with, hindering their

understanding of how these partners process personal data. Thus, it can be argued that this lack of disclosure violates the principles of transparency, accountability, and good faith outlined in art. 6º of the LGPD.

967. Finally, the rights of the data subject as outlined in art. 18, LGPD, are also not detailed in the policies. Reference to the Brazilian framework is found only once in the Google Cloud Privacy Notice and is absent from both the Google Workspace for Education Policy Notice and Google's general Privacy Policy. The latter contains information on how to exercise the data subjects' rights if the GDPR applies to the processing of data, but it does not mention the requirements of the LGPD.

Interim Conclusion

968. Google Workspace for Education is used worldwide by millions of students, and its application has been particularly expanded during the COVID-19 pandemic. Google's educational approach, more strictly focused on the development of skills and competencies, especially for the job market, establishes a digital environment that does not necessarily accommodate divergent pedagogical methodologies. This vision smoothly aligns with the datafication and quantification of education, which brings several challenges to the protection of children's personal data.

969. This chapter aimed to describe the role of Google Workspace for Education in both the EU and Brazil and the impacts it brings to children's data protection in both jurisdictions. Considering the existence of decisions by EU competent authorities, there exists a natural filter that allows a more detailed analysis of these issues. In the Brazilian case, the lack of a specific decision on the matter demanded an analysis of publicly available documents provided by Google and previous research published on the subject.

970. Although both jurisdictions feature very similar data protection laws, they significantly differ in their levels of maturity regarding data protection culture. While the EU has had special laws since the 1970s, Brazil issued its first law in 2018, with enforcement beginning only in 2020. This implies that the ANPD and other competent regulatory bodies (such as consumer protection agencies) are still consolidating and adjusting to the new reality, significantly affecting the application of the law and its integration into people's daily lives. Nevertheless, the divergence in Google's approaches across these closely related jurisdictions speaks volumes about its intentions to expand its collection of personal data.

971. The next chapter will analyze the information outlined in this chapter, not only through a lens of compliance with the GDPR and LGPD, presenting convergences and divergences in the measures adopted in each country but also from a perspective of data colonialism, delving deeper to grasp the prevailing gaps in the current model that still allow data to be processed contrary to children's best interests.

Chapter 11. Analysis

972. After introducing Google Workspace for Education and its main features in Chapter 9, Chapter 10 was dedicated to delineating the challenges it poses to children's rights to privacy and data protection in the EU and Brazil. This was achieved by outlining the primary issues identified in Europe by competent authorities and, in the case of Brazil, by analyzing Google's ToS and privacy policies alongside previous research on the topic.

973. This chapter goes deeper by analyzing these cases data to find convergences, divergences, and gaps. I will first focus on the insights that can be gathered from the decisions of EU MS competent authorities, as well as from the description of how data is processed within the Brazilian reality. This analysis will be structured around the main aspects of data protection laws that are in tension with the identified challenges. The second part of the chapter aims to understand these cases through the lens of data colonialism. Challenges mapped in Chapter 8 will also be useful to situate the discussion and derive conclusions that hold relevance for other edtech.

11.1 Tensions between the GDPR, LGPD and Google Workspace for Education

974. The decisions of EU MS competent authorities outlined in the previous chapter, along with the operation of Google Workspace for Education in Brazil, shed light on systematic concerns regarding children's data protection in the adoption of this technology by public schools. This section is dedicated to pinpointing the primary areas within the GDPR and LGPD that may conflict with the implementation of Google Workspace for Education, while also delineating possible convergences, divergences, and gaps.

11.1.1 Roles and responsibilities

975. A very important topic that stands out in almost all EU decisions and the Brazilian case is the difficulty in delimiting the roles and responsibilities of schools and Google regarding the processing of personal data. This discussion was very clear within the Dutch case and the contracts analyzed by Privacy Company. Google qualified itself

> as [a] data processor for the personal data in Customer Data it processes through the Core Services in G Suite (Enterprise) for Education (described as the Customer Data in this DPIA) [and] as data controller for the Google Account, most of the Additional

> Services including Chrome OS and the Chrome Browser, the Diagnostic Data and other services related services such as Feedback (Nas, Sjoera; Terra, 2021, p. 6).

976. For other services, the roles were considered not to be clearly defined or were unlawfully designated. Google could not be considered neither a sole controller nor a processor for some activities. It had access to some personal data only because of its relationship with educational institutions, meaning that there should be a joint controllership relationship according to the EDPB guidelines. The joint controllership was, however, not a possibility in cases when the purposes of the data processing were not aligned with the legal duties of the school to provide education, something also identified by the Danish DPA. The only situations where this would not apply would be when Google processes data for its own legitimate business purposes, like invoicing, or when they are required to disclose data to authorities (in cases where Google is not able to forward this request to schools) (Nas, Sjoera; Terra, 2021, p. 107).

977. A situation mirroring that identified by Privacy Company could be seen in Brazil. Upon reviewing the ToS and privacy policies applicable to the country, the only certainty we have is that Google considers schools as controllers when it comes to customers data (information directly provided by schools or data subjects when using their services) within core services. Their roles and responsibilities concerning service data in core services and all data in additional services remain unclear, although it can be inferred that Google considers itself as a controller- in these contexts.

978. Apart from identifying ambiguities regarding who determined the means and purposes of data processing, the VTC within the Belgian case found it unrealistic to consider schools as controllers in some instances. The power imbalance between schools and Google made it difficult for the former to discern which data are being collected for each purpose, thereby posing a challenge for them to monitor Google's activities as a data processor.

979. In some instances, the lack of properly defined roles and responsibilities was also attributed to the acceptance of the standard ToS. The AEPD found that the ToS lacked precision regarding the roles and responsibilities for each processing activity under art. 28, GDPR. According to the authority, the agreement should have been supplemented by another document specifying the roles and responsibilities of each party involved.

980. In the Finnish case, the DPA found that by accepting Google's ToS as it was, the controller undermined its ability to adequately control and supervise the processing of personal data, a concern also recognized in a previous DPIA. Similarly, in the Danish case, the Helsingør

municipality was unaware of many changes made by Google to its ToS, which contributed to a breach of students' data. Lastly, the VTC in the Belgian case also highlighted that the purposes and means of processing personal data could change at any time when Google modifies its ToS, posing a concern for schools.

981. The common thread connecting all the issues above is the factual influence exerted by Google on the purposes and means of the processing activities. As controllers, schools bear the responsibility to ensure that the processor adheres to data protection laws and implements necessary safeguards. Regarding AI systems, schools must understand how they work and make decisions, as they must explain this information to data subjects (ICO, 2022).

982. In this sense, a specific analysis of each data processing activity or set of processing activities must take place. While it may be evident that schools act as controllers and Google as the processor in tasks such as registering students and staff on the platform, it is not so clear when the platform processes data to offer personalized learning activities within Google Classroom, for instance.

983. Even if schools agree with the purpose of the processing, it must be verified whether Google is actually deciding essential means such as which data is processed; for how long they are processed; if decisions are automated, etc. Given the often limited expertise of schools in understanding the operations of AI systems, especially when trade secrets are involved, and the lack of explicit prior instructions provided to Google (depending on how the ToS have been signed and the influence exerted by the schools on its terms), a scenario where Google is considered a joint controller in these cases becomes a possibility. The discussion in such cases would also demand consideration of appropriate legal bases.

11.1.2 Purposes for processing personal data

984. Defining the purposes for which personal data are processed is a crucial step towards compliance with the GDPR. Transparency regarding these purposes is essential to ascertain adherence to principles such as purpose limitation, data minimization, lawful processing, among others. The cases narrated above show that the purposes for which student data were processed were not clear, especially when Google was the controller for the processing activity.

985. The Brazilian case stands out as particularly relevant in this context, given that the ANPD has not yet provided guidance on the level of detail required in the information to be provided to data subjects. Nevertheless, it is evident that the information currently available

regarding the purposes of processing personal data is excessively vague and incomplete. This lack of clarity makes it difficult, if not impossible, for data subjects to effectively exercise their rights, which shows that the available information is not fulfilling its intended functions.

986. In two other cases, Germany and the Netherlands, the irregular processing of telemetry and diagnostic data was specifically highlighted. Telemetry data refers to information obtained through telemetry, a process involving the automatic collection, transmission, and measurement of data from remote sources using sensors and other devices. Even though some level of pseudonymization is applied, telemetry data can still contain elements that could be used to identify individuals, which can be considered personal data. Diagnostic data are often collected through telemetry, providing insights into the devices employed and the performance of the applications used (Hessel, 2022).

987. At the time of the first DPIA carried out by Privacy Company, Google had not made available any public documentation regarding the specific purposes for which it processes diagnostic data, whether to be used in core or additional services. Just as in the case of the collected data, information about all the purposes for which Google processed data was also not clearly and thoroughly available, especially when Google was acting as a data processor (Nas, Sjoera; Terra, 2021, p. 6). Although the narrative behind the use of diagnostic data is often linked to the implementation of security measures on the platform, the lack of clear purposes means that one cannot be sure of their beneficial use.

988. The separation of core services and additional services, as well as customer data and service data, may initially be perceived as positive, as it allows Google to distinctly delineate controllership, thereby specifying the entities responsible for determining the intended purposes. However, the Dutch case, where multiple DPIAs have been carried out, has shown that this separation is not straightforward and can be difficult to operationalize in practice. Even when schools were required to disable additional services (as they are not in control of the processing of data and Google would not have a legal basis to process them in that context), students would often create personal accounts to use them, ensuring a smoother integration between services.

989. The DPIAs also highlighted that the data flow between accounts and among core and additional services lacked clarity. Consequently, even when the school initially defines the purposes for processing student data, the structure of the services facilitates the collection of data for commercial purposes.

990. In a study conducted on the terms of use and privacy policies adopted in 2021 by Google Workspace for Education, the ones analyzed by Privacy Company, Hopper *et al.* (2022) also demonstrated the difficulty of identifying the data collected by Google Workspace for Education and the purposes for which they are processed, as it employs various terms to describe data types, leading to confusion and complexity.

991. Finally, there was little or no discussion in relation to the use of AI systems within Google Workspace for Education and how the purposes of processing personal data were impacted. If data were collected to provide the service to schools and is being further used to train AI or improve Google's service, a careful analysis of art. 6(4), GDPR, would be imperative.

11.1.3 Lawful Bases

992. The appropriate legal basis for processing data related to Google Workspace for Education by schools was widely discussed by the EU MS authorities. Some cases were brought to their attention due to complaints regarding the absence of parental consent for schools to process data within the platform. The Danish DPA clarified that the Municipality's use of art. 6(1)(e) of the GDPR was correct, and consent was not applicable] for the provision of Google Workspace for Education Core Services and the creation of individual user accounts within the platform.

993. In the Norwegian case, some municipalities relied on consent, the performance of a contract, and the legal obligation to process students' data. However, the DPA determined that in all cases, the appropriate legal basis should be the task carried out in the public interest, as outlined in art. 6(1)(e) of the GDPR. Similarly, in the Finnish case, the authority concluded that relying on a legal obligation was not lawful, as the Finnish Education Act lacked specificity and did not mandate the use of digital technologies. Consent was also deemed inappropriate since data subjects would not be able to provide it freely.

994. Although not much detail has been provided within the publicly available decision, the case discussed under the Hessian DPA's jurisdiction briefly mentioned the fact that consent should not be used as a legal basis to justify the use of cloud services such as Microsoft Office 365 and Google Workspace for Education.

995. In Spain, the authority provided two different opinions on the matter. In one instance, the AEPD determined that consent was not suitable as a legal basis for processing students'

data under Google Workspace for Education by schools, as requested by the complainant, due to the power imbalance between the school and the data subjects. In this case, the appropriate basis would also be art. 6(1)(e), GDPR. Nonetheless, in a very similar case, the authority did not consider consent as an inappropriate legal basis but still deemed it invalid due to the lack of adequate information provided to the data subject.

996. The appropriateness of consent was also discussed within the Netherlands case, though focused on the processing of data within additional services by Google as a controller. According to the DPA, consent was also not considered to be the right lawful basis, as there was a clear imbalance of power between schools and parents/children, and it would not be freely given.

997. Within the EU, most of the cases indicate that art. 6(1)(e) is the most appropriate legal basis to be used when schools are processing data as controllers within the deployment of Google Workspace for Education. In cases where Google would like to process personal data for their own purposes, such as within additional services, a new legal relationship between them and the data subjects must be established, and a new legal basis defined. An important issue remains, however, regarding the data that Google has access to only because of its relationship with schools. If data is used for training AI, for example, the question remains whether schools could be recognized as joint controllers as this would probably not fall within their responsibilities as public entities and, therefore, the legal basis of art. 6(1)(e).

998. A similar issue was also observed in Brazil. Since the reviewed documents only comprised those publicly disclosed by Google, it remained unclear which legal bases schools relied upon to process children's data within the platform when acting as controllers. Google's privacy notices did not provide a clear enumeration of legal bases for their processing activities. However, within its ToS for Google Workspace for Education, Google stipulates that schools must "obtain parental consent for the collection and use of personal data in any Additional Products that the Customer intends to enable before allowing End Users under the age of 18 to access or use such Additional Products." As previously discussed, this statement raises significant concerns. Not only does Google assume the role of controller in this scenario, but relying on consent may fail to meet crucial criteria outlined in the LGPD, such as being freely given and ensuring compliance with age of consent requirements.

11.1.4 Transparency obligations

999. The provision of information to data subjects under arts. 12-14, GDPR, was also subject to analysis in some EU cases. In Norway, the Municipality in question held a meeting with parents, where information regarding the processing of data was said to be presented. The DPA was of the opinion that having this type of meeting or only referring to Google's ToS was not sufficient and should be supplemented by information in writing, especially considering the services being targeted at children. This is particularly important when Chromebooks can be used for private purposes with private accounts.

1000. In Spain, the AEPD considered that the documents provided to parents were insufficient to comply with the information requirements in the GDPR. Key information was missing from the documents, and they were not written in a language that children, as data subjects, could understand. In the case of Finland, the DPA found Google's ToS general and difficult to interpret, meaning that there was a risk that the processing activities were not properly defined.

1001. It is important to emphasize that Google's ToS establish a relationship and are binding between the school and Google. In cases where the school is a controller, it must provide appropriate information to the data subjects and include how it also processes student data beyond what was agreed upon with the processor. This information must be aligned with the understanding of children when they are the data subjects.

1002. In the Brazilian case, it was not possible to ascertain the information that schools were providing to data subjects. However, the review of ToS and privacy policies applicable to Google Workspace for Education in the country revealed a lack of essential information as mandated by the LGPD.

1003. First, pertinent information regarding data processing is scattered across different documents, some of which are solely available in English. The documents are the same for children and adults alike, which directly infringes art. 14, §6º, LGPD. Concerning their content, details about the data collected and the purposes for their collection are vague and incomplete. Data subjects are not afforded the option to access additional information if desired, and crucial details such as the duration of data processing, the respective roles and responsibilities of Google and schools, data sharing practices, and procedures for exercising data subject rights are notably absent.

1004. In a similar exercise of reviewing Google's ToS and privacy policies, Hooper *et al.* (2022) emphasized the large number of documents and legal terms (over 60) that schools must

navigate in order to understand Google Workspace for Education's activities. Determining which one is applicable mainly depends on the context and services used by the school. The same conclusion was reached by Marrafon and Fernandes (2020) while analyzing the 2019's policies applicable to the Brazilian reality. The policies were scattered, many of them only available in English, and the actual implementation of each one was challenging to define. This gets even more difficult when third-party apps are used within Google Classroom through its API, as mentioned above.

11.1.5 DPIA and risk assessment

1005. The EU cases described above show how important and yet challenging it can be for educational institutions to assess the risks to the rights of the data subjects involved in the data processing. Most cases discuss the need to carry out a risk assessment on the security of data processing (art. 32, GDPR), and/or a DPIA (art. 35, GDPR).

1006. In relation to the obligations under art. 32, GDPR, the Danish DPA found that the Helsingør Municipality should have conducted a risk analysis to identify the risks that access to Google Workspace for Education's additional services would entail. In that case, it meant that students' personal data were being displayed when they used YouTube. In the Norwegian case, the DPA found that when acquiring hardware and software to be used in education, municipalities have an obligation to carry out a risk assessment based on art. 32, GDPR. Although some of the municipalities have done so, it was not considered sufficient as they have not implemented safeguards to keep themselves up to date about the changes in Google's ToS.

1007. Although the actual list of processing activities that are considered high risk differs from authority to authority, there is a high degree of convergence in the cases presented above. The Danish DPA found that the Municipality in question should have carried out a DPIA because it involved new and complex technology and data from children were being processed. The authority considered that the risk was especially higher because the technology was implemented within the scope of education and because other products offered by Google were financed by targeted advertisement and selling of information. The first two reasons were also mentioned by the Norwegian DPA due to the application of a new technological or organizational solution (in that case, the use of cloud services in primary schools) and the processing of personal data of vulnerable data subjects.

1008. The lack of a DPIA constituted the main reason to initiate investigations within the scope of the Swedish DPA. Although the controller had conducted a DPIA when the service was first implemented in 2014, it failed to review it in 2020, when the service was migrated to the controller's own IT environment. The IMY considered that the case would fulfil two criteria for carrying out a DPIA, namely the large-scale processing of data and the processing of data pertaining to vulnerable individuals.

1009. The first case brought before the Spanish DPA highlighted the incompletion and inadequacy of the conducted DPIA. Although the assessment had been carried out using a template furnished by the authority, it failed to account for the unique aspects of the case, notably the processing of children's data.

1010. Finally, the Dutch case stands out when it comes to performing a DPIA. Of all the cases, this was the most comprehensive one and delved the deepest into the specifics of the technology. This was only possible due to the DPIAs and audits conducted by the Privacy Company on behalf of educational institutions. Several risks were only identified through these analyses, which most likely would have also emerged if they had been conducted in the cases discussed by other DPAs. This illustrates that conducting well-executed DPIAs is extremely time-consuming and financially demanding, which may not necessarily be feasible for schools in other situations. Furthermore, it demonstrates that despite modifications made by Google, these changes led to the need for new assessments, uncovering additional issues.

1011. Thus, more than just a step in the adoption of technologies, the DPIA should be something carried out constantly, especially when there are changes in the technological or organizational situation. In a situation where the company offers standard ToS for schools and has the prerogative to change them at any time, the latter find themselves in an extremely complicated situation. This prompted the Belgian authority VTC to assert that for schools, conducting DPIAs is not merely difficult but frequently unfeasible. Apart from the shortage of human and financial resources necessary for such undertakings, schools also lack real visibility of the risks posed by the technology. The collaborative decision-making model identified in the Netherlands and Denmark, for example, where human and financial resources are pooled, may be an effective way to address this problem. Furthermore, focusing on technologies over which the state and schools have more control can also help solve it.

11.1.6 Data Transfers

1012. Data transfers between the EU and third countries can be carried out under certain circumstances defined by Chapter V, GDPR. In the case of the US, this has been historically legitimized by adequacy decisions based on art. 45, GDPR. However, the situation has become increasingly complex over the years, due to invalidations of these arrangements by the CJEU. Two main challenges in this regard were identified by the Court, namely

> (1) a lack of legal safeguards to ensure that any governmental access by the US authorities is necessary and proportionate from the perspective of the EU Charter, considering the substantial interference with EU fundamental rights such governmental access poses; (2) a lack of effective legal remedies for affected data subjects in the EU in order to enable them to access their personal data or to rectify or erase them (Drechsler *et al.*, 2023, p. 5).

1013. In the analyzed decisions within the EU, the transfer of data to the USA emerged as a recurrent theme. In the Dutch case, the Privacy Company's 2021 DPIA found that the only two relevant differences between the free and premium versions of Google Workspace for Education were additional security measures and the option to select EU data center storage for specific Core Services. Nevertheless, certain data processing activities, like providing technical support to users, might still involve transfers to the USA.

1014. As a result of the jurisprudence in Schrems-II and of the EDPB measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB, 2021), schools would need to perform a risk analysis of the transfers outside the EEA. In the Netherlands case, it was unclear if schools would be able to use Standard Contractual Clauses (SCC) due to the change of the definition of international transfer in the SCC published by the Commission in 2021. If that were the case, schools would be required to implement supplementary measures to guarantee compliance with the EU's standards for safeguarding personal data. The same was identified in the Danish and Finish cases.

1015. The EDPB recommends the employment of strong encryption as the best measure to mitigate the risks associated to unlawful processing when transferring data outside of the EEA. Although the municipality in the Danish case argued to use encryption when data was transmitted and processed by Google, it was not considered strong enough by the DPA, as Google could still access the information in plain text.

11.2 Appropriation of resources through the lack of compliance with the data protection framework

1016. An important element of data colonialism, as described in Chapter 3, is the appropriation of resources. Data are seen as readily available and abundant, much like a natural resource such as oil or minerals. This perspective leads to the perception that data can be harvested, exploited, and used without considering the implications or consequences for the individuals and groups from whom the data is collected. Just as historical colonial powers exploited land, natural resources, and labor from colonized territories, the social quantification sector may similarly exploit data without sufficient regard for people's rights to privacy, data protection, and autonomy.

1017. Viewed through the lens of data commodification, data are perceived as traces left behind by individuals or groups when utilizing technology, as something that naturally exists, representing missed opportunities if not adequately harnessed. However, as we have previously discussed, data always result from an abstraction process, one facilitated by specific design choices.

1018. As discussed in section 11.1, non-compliance with data protection regulations is an important means to guarantee that more data are available for the company's commercial purposes. Both Google and the public entities using its services have failed to adhere to fundamental rules outlined in the GDPR and LGPD. This was particularly evident in the Netherlands and Denmark cases, where more comprehensive investigations into the technology's functionality were conducted, either through third-party DPIAs or by the DPAs themselves.

1019. The lack of compliance is generally disguised by very specific narratives that help justify data colonialism, which is also one of its main aspects as highlighted by Couldry and Mejias (2019). Apart from this broader narrative of data commodification, the strategy adopted by Google is related to what Lindh and Nolin (2016) define as a front end/back end strategy. While the service's advantages are evident to users (front end) such as free services and interoperability, the back-end activities are relatively hidden by a specific narrative. The authors have analyzed Google Apps for Education's (now Google Workspace for Education) policy documents and concluded that they had the aim of "disguis[ing] the business model and persuad[ing] the reader to understand Google as a free public service, divorced from marketplace contexts and concerns" (Lindh; Nolin, 2016, p. 650). This is done through many

different tactics such as focusing on the benefits for user experience (benefiting rhetoric) and framing practices related to their business model as minor aspects of their activities (side-lining rhetoric) (Lindh; Nolin, 2016). As observed, it also involved using specific language that fosters the perception among users that the information Google collects is not personal data, but "service" data.

11.3 Unequal data relations and global distribution of the benefits of resource appropriation

1020. Apart from the appropriation of resources, justified by specific narratives, data colonialism is also embedded in unequal social-economic relations and unequal global distribution of the benefits of resource appropriation. Although these are two separate components, they can certainly be identified together in the cases described above. Chapter 9 has described Google Workspace for Education and the business model it relies upon. It showed that the data relations established by Google and schools are unequal for several reasons.

1021. First, it is important to emphasize that providing digital technology solutions for education is not Googles' main activity. Google's business model is primarily based on data harvesting and targeted advertising. Some view Google's offer of this edtech for free as a genuine act of charity, something the company does to fulfill its social role in the world and improve it. While this may indeed be part of a broader justification for its provision (see discussion in Chapter 9), the facts above demonstrate that children's data have been processed for purposes contrary to their best interests. The true intention behind the technology, or the narrative presented by the company, loses significance when such evidence is brought to light.

1022. As stated in the mapping exercise conducted in Chapter 8, the very way AI systems operate brings several challenges to the exchange of necessary information between data controllers and processors. It is not easy to identify which data have been used by these systems to draw inferences or make decisions, as well as the weight each piece of data has. Schools generally lack the expertise and resources required to obtain relevant information about their operation, not only to procure the service but also to ensure its compliance with data protection rules and the best interest of children. The opacity of the operations conducted with personal data, therefore, not only interferes in several rights put forth in the data protection frameworks, but also increases the power imbalance between schools and edtech providers.

1023. This is even more serious in the Brazilian context, where the lack of investment in education and sovereign digital infrastructure makes partnering with companies that provide

their products “for free” much more attractive. During the pandemic, when states and municipalities had to switch from in-person to online classes overnight, employing these technologies was the only way to maintain educational activities. Therefore, data colonialism feeds into a vicious cycle. By adopting free education technologies, the investment in sovereign technologies is further neglected and the possible available budget passed on to other sectors.

1024. It further emphasizes the influence wielded by the social quantification sector over individuals as a whole. This is evident as the accumulation of data enables deeper insights to be extracted, thereby amplifying the potential for manipulation by these entities. This is even more problematic when it comes to educational data, which are so valuable within a human profile and so indicative of a country’s human capacity and resources.

1025. The power imbalance among the involved actors also results in the benefits of data appropriation being concentrated in the hands of the social quantification sector. Considering the provision of technology by private actors, any crucial insight that can be derived from data collected within education remains restricted to the information that the company is willing to share with the government. Public entities lose the capacity for adequate analysis of the implemented public policy and the use of data for other purposes aligned with children’s development and education.

11.4 Digital sovereignty

1026. We have discussed above the key elements of data colonialism, how it manifests, and how it could be identified through the mapping of challenges undertaken in the preceding chapters. It is now essential to delve deeper into something that underlines these aspects, which has been directly addressed in certain EU cases and is closely linked to some of the potential solutions that will be highlighted in the conclusion of this thesis.

1027. The cases mentioned above all involve elements of digital sovereignty, a critical concept associated with the imperative to bolster the autonomy of individuals and society in the face of data colonialism. The German case in Hesse, for instance, gained attention due to Microsoft’s announcement that its services would no longer be delivered through a German cloud. This implied that the state’s control over the data processed by these services would be affected, prompting a reconsideration of other services, such as Google Workspace for Education. In a similar fashion, France decided that Microsoft and other cloud services like Google do not comply with its Cloud at the Center doctrine, and their provision of free services would also

impact competition and be contrary to public procurement rules. The Danish, Dutch, and Finish cases relied on digital sovereignty arguments while focusing on Google Workspace for Education's compliance with data transfer requirements outlined in the GDPR, particularly in light of the latest developments on this matter within the CJEU.

1028. Discussing digital sovereignty solely through the lens of competition, data localization and data transfers can be narrow, and other aspects should be highlighted. After providing a brief definition and main aspects of the concept, I will analyze additional elements that could have been identified by the authorities, which can be highly significant for the development of digital sovereignty also in the Brazilian context.

11.4.1 The concept of digital sovereignty

1029. The modern concept of national sovereignty is based on an analog world, and encompasses the power exercised by the state on all affairs within its territory, such as its resources and people. The digital environment, however, puts tension on this concept, as it lacks physical boundaries and is mostly subjected to private forces, especially multinational corporations, which makes it increasingly globalized (Floridi, 2020, p. 372). Therefore, rather than being just a subcategory of sovereignty, digital sovereignty affects the core of political institutions and their very ability to exercise sovereignty in a broader sense (Smuha, 2023a, p. 3).

1030. Digital sovereignty can be understood as the "control of the digital", i.e., the ability not only "to influence [it] (e.g. its occurrence, creation, or destruction), [but also] its dynamics (e.g. its behavior, development, operations, interactions), including the ability to check and correct for any deviation from such influence" (Floridi, 2020, p. 371). This could be understood in relation to individuals and their ability to shape the digital sphere in a self-determined way or in relation to states (Herlo; Ullrich; Vladova, 2023; Núcleo de Tecnologia do MTST, 2023).

1031. In the case of states, this can occur in two ways. First, by controlling the digital infrastructure, which includes capital resources (such as software, hardware, standards, and cables); intellectual resources (such as human resources and institutions); and financial resources to experiment and design new models and possibilities (Pinto, 2018, p. 17). Second, by controlling a country's destiny through public policies (Lefèvre, 2023) and norm-setting capacity (Smuha, 2023a, p. 8).

1032. The control of digital infrastructure is challenging, and will depend on the policies, political power, international pressure and influences, as well as resources available to each country. It requires understanding that allocation of resources to this area is essential for the existence of democracy and people power. This is enough to demonstrate how dangerous and detrimental short-term policies like accepting free services from foreign technology companies with data-driven business models can be. However, considering the broader context also involves recognizing that some countries have limited choices.

1033. Policies focused on the adoption of open-source software, for example, can be an interesting path in the case of countries with few resources (European Commission, Directorate-General for Education, Youth, Sport and Culture, 2021, p. 142), as, in addition to being free, it is open to public scrutiny. However, this alone is insufficient to build a robust digital policy in a given country. This inadequacy arises not only from the need to prioritize sustainability and achieve widespread adoption, but also from the pervasive influence of private entities and foreign states in shaping public policies through lobbying and manipulation. This demonstrates how the two types of control in digital sovereignty—economic and normative—are interconnected (Pinto, 2018, p. 21; Smuha, 2023a).

1034. The relationship between companies and states is also asymmetric in the digital age, with the latter frequently depending on the infrastructure provided by the former. Companies are currently the ones determining the nature and speed of technological change, while states' role is often perceived as being able to control its direction (Floridi, 2020, p. 371). However, this has not been the case for most countries, which already struggle to set this direction, let alone innovate and proactively consider what kind of technology serves best the public good and aligns with the state's strategies, such as through procurement mechanisms (Mazzucato, 2019, 2020).

1035. Controlling a country's or even a supranational entity like the EU's digital destiny through legislation and public policies can also be extremely challenging in a globalized world. This includes dealing, for example, with the intense lobbying of tech companies and foreign states in the definition and drafting of policies, investment plans, as well as in proposing specific legislation related to the digital domain. Defining digital strategies through policy can, for instance, be influenced by consultancy firms, which are increasingly moving from the sidelines to the center of important decisions within the public sphere. Their business models, underlying conflicts of interest, and lack of transparency are ever more a problem to our democracies and economies (Corporate Europe Observatory, 2023; Mazzucato; Collington, 2023).

1036. The AI Act serves as an important example of the influence on the legislative activities themselves. A report published by Corporate Europe Observatory, for example, showed how the EU's pioneering attempt to regulate AI has faced intense lobbying from USA tech companies. This happened not only through pressure from the corporations themselves but also through covert groups, tech-funded experts, and the USA Government (Schyns, 2023). These activities have been ongoing since the initial drafting of the act, and previous research indicates that this is not an isolated case (Bank *et al.*, 2021).

1037. Even when legislators are able to pass regulations, the latter still have their limits because of possible poor choices while legislating or the difficulties related to their enforcement (Massé, 2022; Smuha, 2023a). Therefore, more than regulating technologies themselves, it is important to actually regulate the incentives to undermine regulation, such as the widespread DDBM depicted above.

1038. Strengthening digital sovereignty is certainly not linked to anachronic notions of digital sovereignism or digital statism. It does not involve replacing a nation's sovereignty, it rather, seeks to complement it with a contemporary digital counterpart. This kind of digital sovereignty serves as a crucial enabling factor to sovereignty in general, offering a broader array of advantages, such as harmonization (including standards and requirements), ensuring a fair competitive environment, and fostering greater opportunities for coordination among all stakeholders (Floridi, 2020, p. 375).

11.4.2 Data colonialism actors and digital sovereignty

1039. Before considering how we can broaden the notion of digital sovereignty as identified in the cases above, it is first important to remember that the network of actors and powers involved in historical colonialism are not the same as in data colonialism.

1040. Despite being the protagonist of historical colonialism, Europe is also grappling with the adverse effects of data colonialism. The GDPR and, more recently, the European Data Strategy stand as clear illustrations of the EU's attempt to guarantee digital sovereignty and pursue a "third way", different from the laissez-faire USA approach and China's state-controlled model.

1041. Indeed, historical, social, economic, and cultural disparities—often remnants of historical colonialism—have resulted in more extensive identification and discussion of data colonialism issues in Europe. This includes not only data protection issues but also how big

tech companies' operations impact competition and the democratic discourse through disinformation and manipulation. The EU is trying to reverse its position in the world regarding digital technologies, investing in new legislation that seeks to give individuals and companies more control over their data, and directly in infrastructure based on European values, in order to reduce its dependence on foreign technologies.

1042. Heidebrecht (2022) is of the view that stakeholders and public authorities (rather than business actors), have gained greater significance in the EU's digital governance processes, leading to the introduction of more market-correcting instruments. In Section 6.3, I briefly discussed how, despite the importance of the EU data strategy for bolstering digital sovereignty, it may still be imbued with a narrative of data flow that is detrimental to individuals and society. It fails to adequately address the root causes of data colonialism, such as data commodification. Delving deeper into this topic unfortunately falls outside the scope of this thesis.

1043. On the other hand, most countries in the world are still trying to keep up with drafting and implementing basic legislation, such as personal data protection laws. Countries within the Global South have fewer material resources and political power available to independently shape their digital destiny and tame the social quantification sector, which is one of the reminiscences of historical colonialism. This includes the enactment and enforcement of new, stricter legislation, as well as the creation of a sovereign infrastructure that enables the implementation of new perspectives regarding the role of data in society.

1044. This is especially challenging within the current political scenario, where many of the pieces of legislation are "imported" from Europe, the GDPR being a great example of the Brussels effect. Although driven by good intent, this kind of universalism can ignore the particularities of each country, especially when it comes to their institutional design, social-economic situation and cultural specificities. Merely transposing legislation can be meaningless if strong enforcement mechanisms are not in place (Arora, 2019).

1045. On the contrary, the existence of stricter legislation without adequate enforcement can even legitimize harmful practices and hinder the demands for the realization of the most basic human rights. Within the context of Brazil, the

> "[p]olitical, economic and social challenges have prevented, and still prevent, the construction of a complete citizenship […]. Although influenced by the philosophical discourse of modernity, the adoption of legal models in Brazil has occurred, in various situations, in a particular and partial way, as in a real game of imitation, an incomplete and untimely simulacrum of never-realised expectations" (Negri, 2021, p. 8).

1046. This is especially interesting considering that, as I have shown in Chapters 7 and 8, the legal framework that governs personal data processing in the EU and in Brazil are extremely similar. The LGPD is based on the same structure, spirit, and principles of the GDPR, with only some specific differences. However, considering the existence of vulnerability layers and the material differences between the two jurisdictions, the laws are not necessarily applied equally.

1047. It must also be considered that these differences, although to a lesser extent, also exist within the EU. As will be discussed below, the decisions made in the region regarding Google Workspace for Education have mainly come from wealthier and more politically powerful countries that allocate more resources to education and personal data protection, therefore affording to be stricter with the social quantification sector.

11.4.3 A broader notion of digital sovereignty

1048. To expand the scope of digital sovereignty beyond the parameters delineated by EU competent authorities, we can identify interesting elements emerging from the decisions that go beyond competition and data localization/data transfer concerns.

1049. The first one is the very existence of resources that allowed for enforcement and negotiations with Google that led to amended contracts. In the case of the Netherlands, for example, the Government has been able to engage Google in months of highly technical discussions based on several DPIAs and deep analysis of the technology. This indicates that they have both capital and intellectual resources at hand to comprehend the implications related to the processing of children's data. The symbolic power of the Dutch DPA also played a significant role, as some even consider that certain USA tech firms now view the Dutch endorsement as a prestigious status symbol, as a seal of approval that they have navigated one of Europe's most rigorous data protection compliance procedure (Singer, 2023).

1050. Secondly, a centralized approach was key to enhance their bargaining power and making the solution scalable. They have demonstrated that this is possible not only by centralizing procurement activities within a specific government entity but through cooperatives of schools and universities. Most schools would not have the means, power, and expertise to independently audit technologies, so cooperatives represent their collective interest and preserve, at the same time, some of their autonomy. The same centrality through cooperatives was identified in the Danish case. One of the cases that took place in Germany, on the other hand, demonstrates the imbalance of power and the need for collective approaches. A

student in Dortmund refused to use Google Workspace for Education due to privacy concerns but faced technical and discriminatory issues within the school.

1051. However, it is essential to consider that focusing solely on the strategies outlined above, while crucial and indicative of the potential for effective enforcement of the GDPR, may not be sufficient to ensure the delivery of education in the best interests of children and in a manner that guarantees digital sovereignty.

1052. These negotiations do not address the core issue of data commodification/data flow paradigm and the market incentives related to the business model of big tech platforms. Children get used to these platforms and are continuously subjected to surveillance and detrimental practices as soon as they leave the controlled school digital environment. The persistence of the business model and incentives for massive data collection also mean that new risks can continuously arise, as highlighted in the most recent DPIA conducted in the Netherlands.

1053. The case of France, in this sense, is particularly noteworthy not only because it bans certain technologies based on a digital sovereignty perspective, but also because the decision was taken by the French Minister of Education and Youth. The possibility of making decisions including broader political considerations beyond the data protection framework (which becomes more difficult when this is done by DPAs), suggests that other elements beyond compliance should be considered.

1054. Lastly, entrusting crucial digital infrastructures to private entities often involves surrendering education-related data that could be used by governments and civil society in the best interest of children, such as to develop privacy-preserving technologies, as well as innovative and collaborate solutions to improve learning (Hooper; Livingstone; Pothong, 2022, p. 56).

1055. This is where digital sovereignty intersects with the imperative to challenge data universalism. We have observed how issues stemming from datafication, particularly certain business models, are systemic and global in nature. However, endeavors to identify solutions must consistently account for local specificities, encompassing both the material and cultural dimensions of knowledge production. It is essential to harness the full potential of each society to foster new imaginaries and conceive alternatives for the data future we aspire to build.

Interim Conclusion

1056. Chapter 11 aimed at analyzing the information described in Chapter 10 to uncover convergences, divergences, and gaps. I have focused on examining the primary areas of conflict with data protection laws, as well as how they can be understood through a data colonialism lens. This analysis exposes a consistent failure of schools and Google Workspace for Education to adhere to data protection frameworks in the EU and in Brazil, revealing challenges that transcend regulatory compliance.

1057. It also underscores the inherent challenges posed by the adopted business model, despite efforts made during negotiations to ensure compliance. Even if children's data are not processed for target advertising, they may still be leveraged for other commercial purposes not necessarily aligned with their best interests. Additionally, children are familiarized and nudged to continue using these technologies outside the school environment and throughout their lives.

1058. I have also discussed how a comprehensive understanding of digital sovereignty extends beyond issues of competition and data localization/transfer. The decisions taken within EU illustrate how the economic and political capital of the analyzed countries significantly influence their level of digital sovereignty, and, consequently, the decisions they can actually make. The social and economic disparities within the EU itself become evident as the countries in question belong to the wealthiest and most politically influential group in the region.

1059. While adequate enforcement remains crucial, both within the EU and Brazil, it alone may not suffice to deliver education in the best interests of children or to ensure digital sovereignty, at both individual and collective levels. A discussion on the appropriate purposes for which children's data are processed is needed. Entrusting essential digital infrastructures to private entities raises significant concerns regarding their business models and governance along with their potential short- and long-term impacts on society. There is a pressing need to challenge data universalism and collaboratively devise solutions that account for local specificities, while leveraging the unique potential of each community to explore alternative approaches in shaping the society we aspire to be part of.

CONCLUDING REMARKS

1060. This thesis aimed to investigate the challenges that edtech presents to children's rights to privacy and to the protection of personal data, and the extent to which the existing legal framework in both Brazil and Europe address them. In this conclusion, I will summarize the path taken to answer this question, along with the main findings and contributions of the research, which will be emphasized in italics for clarity and ease of reference.

1061. From a descriptive approach, **Part I** aimed to set the scene and discuss the context of edtech deployment. **Chapter 1** introduced and explained the concept of edtech, providing a historical perspective on the evolution of technology in education. The purpose of this historical overview extends beyond simply illustrating the steps taken for the current technologies to be available, viewing computers or AI technologies as the pinnacle of edtech technological development. Its primary aim was to discuss the methodologies and epistemologies behind previously adopted technologies that continue to shape contemporary technological paradigms. An important example in this regard was the development of so-called teaching machines, heavily influenced by behaviorist and mechanical views of education, which still impact how education is currently understood and delivered, especially concerning personalized learning technologies.

1062. I have also discussed the concept of education, which directly informed the analysis made in the previous chapters. More specifically, I have embraced a comprehensive understanding of education, essential for framing history and future as a possibility. By conceiving education as not only capable of shaping children's knowledge and skills but also influencing their worldview and ethical-political expressions, we recognize its profound impact on human intervention in reality and the development of their agency for effective change. *Recognizing education's transformative and multiplier role sheds light on the enormous power that edtech has on shaping society. This stresses the need to understand education and a highly political and strategic sector, which demands transparent, democratic, and fair decisions*.

1063. Given the vast quantity of technologies available, their diverse purposes, and the different risks they pose, the chapter presented a typology of edtech to systematize the complex landscape. The typology differentiated between technologies used to *provide education* and to *learn about education*. The first category was further branched to include technologies that support either educational institutions or teaching and learning activities. Although the latter

could also be seen as a single category, research has shown that popular technologies usually focus on replacing teachers and include minor modifications to support them at the end of the design process, such as dashboards. The different objectives also influence the analysis of necessity and proportionality concerning their impact on children's rights to privacy and data protection.

1064. Finally, the second broader category is related to technologies that seek to learn about how students learn. Although the technologies and data used to power them are often the same as those for supporting students, there is a difference in their purpose. Learning about how students learn is generally a phase of the data analytics process within edtech, and the insights developed therein are fed back into the AI model, influencing the student's own experience while learning. Learning analytics technologies are usually employed to analyze data from longer periods and focus on structure interventions on the algorithm of AI system in general, or even on the curriculum and other elements that may prevent students' progress.

1065. **Chapter 2** explored foundational aspects within edtech and how they interplay with long-standing discussions in education. The first important aspect of interplay involves the participation of private actors in the sector. The rise of neoliberal policies in recent decades has facilitated the marketization of education, either through privatization or commercialization.

1066. *The dynamic between states and private actors has long been established, but the increasing prominence of private sector involvement, particularly in providing digital ICT to schools, has fundamentally altered the very nature of education, i.e., what we understand by it and how it should be realized*. Education is increasingly seen as a private good; students and their families as consumers; and the dynamics of the private sector as the main way to "deliver" it.

1067. *This trend serves as a catalyst for the learnification phenomenon, wherein education is narrowly regarded as synonymous with learning. The emphasis shifts to the transmission of knowledge and skills that individuals should acquire, along with the exploration of efficient methods to achieve it*. This approach sidelines other crucial aspects of a holistic view of education, such as the subjectification and socialization of individuals, as well as education's collective impact and its key role as a foundation for democracy. This broader understanding of education was captured by Paulo Freire's definition of education, as described above, and complemented in Chapter 5 by the aims of education outlined in art. 29, CRC.

1068. *This limited perspective on education further encourages classroom quantification, aligning itself with the educational measurement movement and processes of datafication. Education is seen as something that could and should be modeled and standardized. Beyond concerns about the validity of measurements and what may be overlooked, this mindset shapes curricula and pedagogical methodologies, with targets and indicators being mistaken for the quality of education itself.*

1069. This notion is reinforced by the logic that governs platforms, which increasingly define the landscape of edtech implementation. As an interface that intermediates the user experience and the role of its provider, it helps concretize and interpret abstract processes. They are also progressively integrating aspects of other commercial services, including customization and on-demand features. *While this can potentially enhance engagement, it reflects a belief in learning as a prescriptive process, impacting students' and teachers' autonomy, and naturalizing the processing of extensive amounts of data*.

1070. **Chapter 3** presented the theory of data colonialism as a theoretical and normative lens that guided the discussions in this thesis. The theory refers to an emerging order of appropriation of human life and social relations through data, arguing that our current relationship with personal data could be seen as an extension of historical colonial practices. *The datafication of life leads to the progressive reconfiguration of larger parts of the social domain, as it is increasingly built to generate data. This positions technology companies as privileged providers not only of social solutions but also of social knowledge*.

1071. To better explain their rationale, Couldry and Mejias articulate four main interlinked components that historical colonialism and data colonialism share: appropriation of resources, unequal social and economic relations, uneven global distribution of the benefits of resource appropriation, and ideologies that help us make sense of the new order.

1072. Data are appropriated by the social quantification sector, making use of already existing unequal data relations or creating new ones. These relations are extremely asymmetrical due to (i) the opacity of the operations conducted with personal data, (ii) the powerful overview of the social world that these companies possess as a consequence, and (iii) the fact that they are built on top of historical asymmetries, often as a product of historical colonialism. This intensifies the disparity in value distribution and is justified through specific narratives. Importantly, this theory recognizes that data colonialism affects some people more than others. It means that children, for example, due to their specificities explained in Chapter 4, will have extra layers of

vulnerability compared to adults. Similarly, underprivileged communities will also present additional layers of vulnerability that can profoundly affect their experience with edtech.

1073. Based on this conceptual overview, **Part II** focused on describing and evaluating the current legal framework applicable to children's rights to privacy and to the protection of personal data in the EU and in Brazil. I first discussed why children deserve differential treatment in **Chapter 4**. *The chapter explored their special status as humans in development, which brings them an extra layer of vulnerability*. Specifically within the digital realm, understanding the implications of data processing is already difficult enough for adults. More than a way to enhance fundamental rights, digital technologies are increasingly the gateway for their realization and children have often no choice whether they would like to use them or not for the most different purposes. They are less experienced, can be easily manipulated, and decisions concerning them are generally taken by others on their behalf, and *by having been raised surrounded by technologies, children's lives are increasingly datafied, meaning that they have proportionally larger digital footprints compared to adults*.

1074. The chapter also introduced a risk classification of children's online presence. The matrix included risks to their privacy, broadly understood as encompassing the interpersonal, institutional, and commercial dimensions. It discussed how privacy risks are cross-cutting and extremely connected to other risks children face in the digital realm, reinforcing the need for a holistic children's rights approach. Finally, the chapter underlined the specific implications that surveillance technologies have on children's trust and development, which can hinder their creativity and critical thinking, directly impacting how they learn.

1075. *More importantly, this chapter underscored the need for a comprehensive and nuanced approach to children's presence in the digital environment, which recognizes their distinct characteristics and developmental needs. It acknowledges the transformative potential of edtech in offering opportunities for learning, information access, and developing physical, social, and digital skills. This can help realize several rights enshrined in the CRC, such as the right to education, access to information, play, and freedom of speech. Innovation within the edtech sector should then be fostered to continuously play that role while being integrated into a broader pedagogical strategy based on scientific evidence. At the same time, along with opportunities, edtech also presents risks, as delineated in Part III. Consequently, policymakers, schools, educators, parents, and children must strike a delicate balance, ensuring protective measures while empowering children to grow autonomously*.

1076. **Chapter 5** was dedicated to presenting the CRC and some of its provisions related to the scope of this thesis. It emphasized that discussing the rights to privacy and to the protection of personal data in isolation is not feasible, as they mutually reinforce and impact other rights. For example, the realization of the right to education makes individuals more aware and critical of the issues surrounding them, enabling them to better exercise their rights to privacy and data protection. On the other hand, ensuring the latter is essential for the implementation of quality education, allowing children to feel secure in learning and interacting with educators and fellow students.

1077. First, I presented some provisions considered to be cross-cutting standards that should be used to interpret and implement other articles of the CRC. *The principle of the best interests of the child particularly stands out, as it should be viewed as a fundamental right, interpretative principle, and procedural rule. It also plays an essential role in raising the threshold regarding interferences with children's fundamental rights, serving as a precautionary principle*. These standards also include the right to non-discrimination, the right to be given appropriate direction based on the evolving capacities of the child, and the right to be heard.

1078. Additionally, I have addressed three more substantial provisions: the right to privacy, the right to education, and the right to protection against economic exploitation. The objectives of education delineated in art. 29 of the CRC should consistently guide the advancement of edtech, ensuring it upholds children's privacy from its conception.

1079. *Safeguarding children's right to protection against economic exploitation is paramount within the digital environment and should go beyond the protection against child labor, encompassing any form of exploitation driven by economic and commercial interests. This stance resonates with the concept of data colonialism, which recognizes exploitation within the realm of data commodification*. *A critical implication of this perspective is that children's data should not be exploited for commercial purposes not aligned with their best interests*. This does not imply a blanket prohibition on procuring edtech or processing data for ancillary activities related to the provided service (such as invoicing). Rather, it means that children's data should not be processed solely for the sake of commercial interests and financial gain, as this would also go against the need to prioritize their rights.

1080. **Chapters 6 and 7** discussed how the GDPR and the LGPD regulate the processing of children's data and how these rules relate to the implementation of edtech by schools. The focus of these chapters was not necessarily on comparing laws, although something inevitable due to

their similarity, but on describing and evaluating their potential, limitations, and gaps to deal with the challenges presented in Part III of the thesis. The current legal frameworks of both jurisdictions already incorporate fundamental rules for safeguarding children's data within edtech. However, there has been limited exploration into the specific purposes for which children's data may be processed, as well as how the mindset of data commodification could serve as the root cause of various risks described in Chapter 8. *While this could certainly be argued to fall within the scope of the right not to be subjected to economic exploitation, it has yet to be translated into enforceable obligations for data controllers beyond the existing prohibition of profiling for targeted advertising purposes in the DSA*.

1081. Despite not being the main focus of this thesis, considering the lack of a final text, the AI Act is also important in the discussion of AI-powered edtech more suitable for the best interests of children. It not only considers certain AI systems deployed in education as high-risk, but also prohibits the use of emotion recognition in this environment.

1082. High-risk systems must comply with various specific obligations, such as those related to data management, cybersecurity, accuracy, and the prevention of bias, which would address many challenges described in Chapter 8. *However, it appears that the AI Act cannot be relied upon as a panacea. Several fundamental questions remain unanswered, including how to align the risk-based approach within an originally product safety legislation with the need to consider values such as human rights, democracy, and the rule of law, as well as the fact that risk assessment is self-assessed, what is problematic due to conflicts of interest*. Despite still being behind in the legislative process and focusing more on the rights of those affected by AI, it is possible to say that similar challenges are going to be faced in the implementation of Bill 2,838 in Brazil.

1083. **Part III** was formulated based on a descriptive, evaluative, and normative approach, aiming to map the challenges posed by data-driven edtech to children's rights to privacy and to the protection of personal data. Given that the majority of data processing activities within edtech involve AI systems, **Chapter 8** initially focused on the overarching risks they present. It began by examining the process of datafication itself and the issues arising from the reduction and abstraction of reality into quantifiable variables. Additionally, it briefly addressed the training of AI systems and highlighted how the substantial amount of data required for their training and operation, along with the issue of repurposing data, already creates tension with the principles of purpose limitation and data minimization in the GDPR and LGPD.

1084. I have also emphasized the concerns surrounding data generation within AI systems and how] inferences drawn therein can be tainted with bias and significantly affect individuals' control over their data. *I have argued that this issue does not seem to be fully addressed by either the GDPR/LGPD or the current text of the AI Act/Bill 2,338. Consequently, there should be a greater focus on the outputs of AI systems and the development of more tools for controlling personal data, such as the right to reasonable inferences*.

1085. Finally, I have also presented the challenges related to decision-making involving algorithms, such as profiling, predictions, and human interpretation of data. Decisions made within edtech have a direct bearing on children's academic performance and their future prospects. *Algorithmic predictions can not only solidify past circumstances, hindering social mobility, but also shape future outcomes as patterns are not merely identified but actively constituted*.

1086. After presenting horizontal challenges related to AI in education, I have also discussed specific ones identified within personalized learning, student monitoring technologies, and learning analytics. Technologies for personalized learning were analyzed as an example of edtech that aims to support students. Despite showing great potential, the evidence of their effectiveness in improving learning is currently weak. On the other hand, the risks already identified are significant. In their current form, this kind of edtech still excessively focus on individual efforts, sidelining social aspects of education, and the aspects that can truly be personalized are limited to the paths that will guide students to the same outcome. Students have a limited ability to define their overall educational goals and, more specifically, the design of the technology and the degree of data processing to which they may be exposed.

1087. Another controversial issue about personalized learning is its internal dynamics and its tendency to amplify what the student is interested in and reduce their contact with the different. Besides being problematic for their learning and development as individuals, it can also affect how the student deals with diversity in society. The reductionist nature of data-driven technologies' architecture can also lead to consider behaviors merely correlated with better academic outcomes being mistakenly identified as their cause and replicated for other students.

1088. Chapter 8 also discussed monitoring and proctoring technologies as examples that directly automate and aim to support teachers' activities. Although the purposes for the use of this kind of technology are usually noble, such as dealing with students' mental health and preventing cheating, they are not necessarily effective and foster a surveilled environment. This

can hinder students from seeking help or expressing their emotions openly, as well as create a chilling effect that affects children's learning and development. The focus on control and mistrust, under the guise of care, can undermine the development of ethical, responsible citizens and perpetuate biases and inequalities, disproportionately impacting more vulnerable groups.

1089. Finally, this chapter described and analyzed technologies used for learning about learning, as explained above. The concept of learning analytics was discussed, as well as their role in leveraging data from students interactions with the AI model to generate insightful information about their learning process. They are usually employed to analyze data from longer periods and focus on structure interventions on the algorithm used by the AI system, or even on the curriculum and other elements that may prevent students' progress. While learning analytics hold promise and provide valuable insights to enhance learning efficacy and efficiency, the collected data are generally used for purposes that may not necessarily prioritize the best interests of the child.

1090. The rest of Part III was dedicated to understanding the Google Workspace for Education case in the EU and in Brazil in order to gain insights into its functioning, the business model behind it and how it affects children's rights to privacy and to the protection of personal data. *Due to Google's primary role in pushing forward the current prevailing business model of data-driven technologies and its widespread use in European and Brazilian classrooms, I argue that these insights could be extrapolated to other technologies. It helps us not only better understand how to enhance the enforcement activities of the current applicable legal framework, but also assess if further legislation or policies are needed.*

1091. **Chapter 9** focused on describing what Google Workspace for Education is, its main features, and its role in Google's broader business model. I have discussed how, although being considered free and part of the company's initiatives focused on social responsibility, Google Workspace for Education is still tied to Google's commercial interests. The blurred boundaries between core and additional services, with varying levels of data protection; their indirect access to children's data via other edtech; and the use of data for other commercial purposes beyond targeted advertising demonstrate how Google Workspace for Education can be used as a strategic tool within its business model.

1092. **Chapter 10** examined the impacts Google Workspace for Education has had on children's privacy and data protection in two different jurisdictions: the European Union and Brazil. To map the challenges faced within the EU, I have used decisions made by competent

authorities as a filter, taking advantage of their auditing capabilities and comprehensive DPIAs carried out within the scope of some cases. Such information is not available for the Brazilian reality, which prompted the examination of Google Workspace for Education's ToS and Privacy Policies to check their compliance with LGPD whenever possible. This has been complemented by a literature review of studies that have also performed a similar exercise and gathered further data through information requests. We have seen that although both jurisdictions feature very similar data protection laws, they significantly differ in their levels of maturity regarding data protection culture, which directly impacts enforcement activities.

1093. Finally, **Chapter 11** analyzed the data described in Chapter 10 to find convergences, divergences, and gaps not only based on main areas of tension with data protection laws, but also through the lens of data colonialism. *This analysis shows a systematized lack of compliance of schools and Google Workspace for Education with data protection frameworks and sheds light on broader challenges*.

1094. Two main conclusions could be drawn from the Google Workspace for Education case. First, *adequate enforcement of the current legal framework is still needed to safeguard children's rights to privacy and to the protection of personal data*. Within the EU, there is evidently a greater concern regarding the use of edtech, particularly in relation Google Workspace for Education. However, there are also regional disparities that result in national decisions being primarily made by the wealthiest and most powerful countries within the bloc. *In the case of Brazil, the enforcement of the LGPD is still in its early stages, and much still needs to be done to ensure that its rules are followed*.

1095. Second, even in cases where authorities negotiated with Google to align the employment of the edtech with the GDPR, *the business model based on data commodification adopted by Google can be considered, in itself, harmful to children's best interests*. Although their data are not directly used for targeted advertisement within the core services, it is still processed for other commercial purposes. Children are familiarized and nudged to continue using the technology outside the school environment and throughout their lives. *This results in the need to discuss the actual purposes we would like children's data to be processed for and to rethink the epistemologies we currently use to understand the role of data within society*.

1096. We have seen that economic and political capital are essential to achieving even basic compliance with the GDPR. *The social and economic disparities within the EU and between*

the EU and Brazil highlight how profound the influence of the social quantification sector is on countries' digital sovereignty and, consequently, on individual autonomy and democracy.

1097. It highlights that despite the EU's ongoing efforts to implement its data strategy, adding constant pages to its digital rulebook, *it is still necessary to discuss the core essence of digital sovereignty. It prompts us to question whether the policies being implemented genuinely enhance both individual and collective autonomy, or are possibly reinforcing problematic DDBM*. We should also question whether all the EU values are actually being considered, or if innovation and economic development of a few are being prioritized. In light of the Brussels effect, the ramifications of these policies need also to be carefully weighted, justifying global dialogues on digital sovereignty that effectively support individuals and communities beyond the limits of countries, blocs, and companies.

Recommendations and indications for future research

1098. Based on the findings described above, it is possible to outline a few recommendations and suggestions for future research. These are mainly focused on states, the primary duty bearers when it comes to implementing edtech in schools, but some are also directed to technology companies.

1099. States have many roles to play in addressing the concerning scenario depicted throughout the thesis. Considering that the private sector is the main one developing edtech and that innovation requires investment, one of the best ways for states to steer it in the right direction is through public procurement. Public procurement should ideally be seen through the lens of a mission-oriented approach. This includes selecting pathways for the economy and placing the issues that require solution at the core of economic system's design; crafting policies that stimulate investment, innovation, and collaboration among different stakeholders, making sure to involve both businesses and citizens; discussing the type of markets we as a society want; and using instruments to foster the most innovative solutions for addressing specific challenges according to our collective needs and purposes (Mazzucato, 2021).

1100. When it comes to safeguarding children's data, public procurement could serve as a mechanism to choose only the technologies that align with the societal goals we have collectively established. The thesis has demonstrated that this process is most effective when centralized to some extent, enhancing bargaining power with technology companies. It does not necessarily imply that it should only be carried by a single governmental actor but it could be a

collective decision-making process involving various schools or administrative entities. Collaborating interdepartmentally can also boost the full scale of public procurement, enabling the use of a substantially larger budget (Mazzucato, 2021).

1101. If doing it at scale is not possible, states should provide schools with standards to understand and choose among vetted edtech products, as schools are probably not in the best position to evaluate and understand all of their nuances due to a lack of expertise and resources. (Hillman, 2022). A roadmap that can help schools and other administrative entities navigate not only the technological specificities of existing edtech but also existing evidence and the applicable legal framework is an interesting tool to be developed in future research.

1102. As we have seen throughout the thesis, this can be a challenge in cases where the educational budget is insufficient or not prioritized for purchasing technologies and contracting services that are privacy-friendly, such as in Spain or in Brazil. Being free is often the main reason for choosing some technologies. In these cases—always considering the best interest of the child and the legal frameworks described in this thesis—it is possible to envision a path that can assist in decision-making.

1103. The first step that should be applied to any decision by states or schools (whether the product/service is free or not) is to analyze whether the technology is indeed necessary for the specific context. If the desired outcome can be achieved without technology or through applications with simpler algorithms or that require less personal data, these should be prioritized. The availability of technologies should not inevitably lead to their implementation, and a potential "modernization" of education should not be pursued for its own sake. This also includes analyzing their effectiveness, efficiency, and added value more generally (Smuha, 2023b, p. 133), taking into account a holistic analysis of their effects on education and on children's rights. This could be carried out, for instance, by leveraging CRIAs methodologies. The choice of technology must always be evidence-based and use the best interest of the child as a precautionary principle. Considering all their specificities, children should not be used for experiments of which we do not know the real consequences.

1104. Following this assessment, and considering the actual necessity of the technology for the specific context, a shift in mindset must begin to take place within the public sector. It must begin to see itself as a purchaser oriented towards the public good. This entails understanding the true underpinnings of the technology, including its business model, and recognizing the value it derives when offering its services free of charge. If a company benefits from future

customers despite not receiving direct payment, it means it has an underlining interest in offering the service. The public sector should leverage this dynamic in negotiating more favorable contracts that prioritize the best interests of the child, including opting for technology with privacy-friendly business models. Selling products or providing services to public educational institutions should be regarded as a privilege accompanied by significant responsibility, meaning that edtech companies should adhere to minimum legal and ethical standards (Hillman, 2022).

1105. Apart from procurement, States can also use their resources to directly foster, develop, or improve (core) digital infrastructure in order to make sure they are digitally sovereign and less dependent on external providers. This is aligned with need to transcend data universalism. The discourse around big data and datafication tends to homogenize social-economic and political contexts, overlooking cultural nuances. Viewing technologies as social-technical artifacts prompts an understanding that although opposing homogenization must be global in framing, solutions must be local.

1106. An interesting type of investment is related to using open standards and open-source software, as well as technology that promote privacy, democratic participation and human centrality by design (Herlo; Ullrich; Vladova, 2023). Apart from being less expensive to implement, they provide extra means of auditing not available in proprietary technologies. This also means fostering the development of technology by and for the community which will directly use it based on their needs. An interesting example in this regard is the Brazilian Homeless Worker Movement (Movimento dos Trabalhadores sem Teto – MTST). The movement has an internal group focused on digital technology, which aims not only to empower participants to become self-sovereign in relation to technologies but also to choose and apply technologies that can address the movement's most immediate issues with autonomy and minimal side effects (Grohmann, 2023; Núcleo de Tecnologia do MTST, 2023).

1107. States have also the power and the duty to properly legislate on the issue of edtech and, especially, AIED. This includes not only demanding privacy-friendly design, but also understanding how AI systems affect data control and questioning the sufficiency of the current legal and policy framework to deal with the economic and political structures enabling data commodification. It also encompasses restricting business models that can harm human dignity and human rights, especially concerning the most vulnerable groups. This should particularly consider the social-economic specificities of each state, which can affect the possibilities of enforcement and success of the legislation (Arora, 2019).

1108. Finally, critical thinking and digital literacy of teachers and students should be fostered through training and implementation of specific measures in school curricula. Understanding and properly using digital technologies have become a prerequisite for participation in society and the exercise of fundamental rights. It serves a dual purpose of protecting children's rights, and enabling their participation, equipping them with the necessary tools to navigate the online environment.

1109. Therefore, learning about how technologies function, as well as who the actors and interests behind them are, is essential for nurturing citizens who are critical and engaged in society. This should certainly be seen as a crucial step, but its value is limited if the preceding measures are not taken. As individuals, there is little one can do in the face of the power of certain edtech companies, so the most significant decisions regarding technology and data governance must be made collectively.

1110. When it comes to edtech companies, they should be seen as the ones to bear the primary responsibility for children's data protection. We have seen throughout the thesis, for example, that the design of learning platforms often resembles those of social media, based on maximizing data processing, and the recommendation of content based on what the student has previously engaged with (5Rights Foundation, 2023). We have also seen that edtech industry often markets its products to schools based on unsubstantiated success metrics and insinuating misleading effectiveness rates (American Civil Liberties Union (ACLU), 2023).

1111. These are only a few examples of situations that are deliberate, mostly due to commercial imperatives, and that can cause harm to children's rights. The best interest of the child imposes a duty to adhere to ethical and legal standards to deliver the best learning experience possible to children. Practices that are not aligned with it should be abandoned, recalibrated, or redesigned to meet children's real needs (5Rights Foundation, 2023).

1112. This is the tone given by the USA Federal Trade Commission (FTC) in its most recent Notice of Proposed Rulemaking (NPRM) that proposes changes to the Children's Online Privacy Protection Rule (COPPA Rule). According to the FTC Chair Lina M. Khan, children should be able to play and learn in the digital environment without being tracked by companies that seek to monetize their personal data (Federal Trade Commission (FTC), 2023).

1113. The proposal places affirmative obligations on service providers, shifting the burden historically placed on parents. Some of the changes to the rule proposed by the FTC are directly related to edtech and include a prohibition on commercial use of children's data, including for

the development of different services (Federal Trade Commission (FTC), 2023; Vance; Sexton; Kalpos, 2023). Others are more general such as a prohibition against conditioning a child's participation on collection of personal information, limits on nudging kids to stay online and the requirement of a separate opt-in for targeted advertising.

1114. As a society, including state agents, businesses, families we must approach the topic discussed in this thesis with the gravity it warrants. The success of future generations hinges on the actions taken by today's adults on their behalf, and we have yet to fully grasp the breadth of the long-term effects that data-driven digital ICT will have on children's rights. More significantly, today's children will inhabit an increasingly interconnected world dominated by digital technologies, particularly AI. In this landscape, the boundaries between human-created and machine-created becomes increasingly blurred, as well as what is true or false. The most important decisions about children's lives will very often be made based on what data say about them.

1115. What we allow to be applied and developed today will shape how younger generations navigate the complex problems of the world we are entrusting to them. We must take charge of technological development to ensure it is evidence-based and human-centric. Instead of us becoming dependent on and serving technology (and technology companies), technology should serve the purposes we have collectively defined.

COMPLETE TABLE OF CONTENTS

ACKNOWLEDGEMENTS **3**
ABSTRACT **5**
RESUMO **6**
SAMENVATTING **7**
LIST OF ACRONYMS AND ABBREVIATIONS **8**
LIST OF FIGURES **13**
LIST OF TABLES **13**
INTRODUCTION **17**
Research question and methodology **21**
a) Relevance 21
b) Research question(s) 23
c) Hypothesis 23
d) Scope of the research 24
e) Methodological approach and thesis structure 25
PART I. SETTING THE SCENE **29**
Chapter 1. The use of technology in education **29**
1.1 A brief history of edtech 31
1.2 Edtech typology 44
Interim conclusion 48
Chapter 2. Exploring the interplay between edtech and longstanding discussions in education **50**
2.1 Public and private values in education 50
2.1.1 The role of philanthropy in education 53
2.2 The “learnification” of education 55
2.3 Learning, calculation and efficiency 57
2.4 Platform learning 59
Interim conclusion 61
Chapter 3. Data Colonialism as a theoretical and normative framework **62**
3.1 The concept of data colonialism 62
3.2 Main components of data colonialism 64
3.3 Colonizing agents 66
3.4 Data Commodification 67

3.5 Data colonialism and its incursion into autonomy 68
Interim conclusion 70
PART II. LEGAL FRAMEWORK ON CHILDREN'S PRIVACY AND DATA PROTECTION 72
Chapter 4. Why children need special privacy and data protection rights 72
4.1 Why do children's data require special treatment? 73
4.1.1 Childhood as an extra layer of vulnerability 73
4.1.2 A proportionally larger digital footprint 76
4.2 Privacy and data protection as a cross-cutting dimension of risks to children's online presence 78
4.3 The importance of privacy and data protection for children's development and learning 81
Interim conclusion 84
Chapter 5. The CRC in the digital environment 86
5.1 The right to non-discrimination 88
5.2 The right to have the child's best interests taken as a primary consideration 89
5.3 The right to be given appropriate direction and guidance in a manner consistent with the evolving capacities of the child 92
5.4 The right to have their views given due weight in accordance with their age and maturity 93
5.5 The right to privacy 95
5.6 The right to education 97
5.7 The right to protection against economic exploitation 101
Interim conclusion 103
Chapter 6. EU's relevant legal and policy frameworks 104
6.1 The General Data Protection Regulation (GDPR) 106
6.1.1 General Principles 106
6.1.2 Roles and responsibilities 109
6.1.3 Article 8, GDPR 111
6.1.3.1 ISS 111
6.1.3.2 Offering directly to a child 113
6.1.3.3 Age for consent 113
6.1.3.4 Consent as an appropriate legal basis for processing children's data 115
6.1.4 Other legal bases for processing children's data 118
6.1.4.1 Contractual necessity 119

6.1.4.2 Compliance with a legal obligation 120
6.1.4.3 Vital interest 121
6.1.4.4 Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller 121
6.1.4.5 Legitimate interests 122
6.1.5 Analysis of selected data subjects' rights 124
6.1.5.1 Transparency obligations and the right of access 124
6.1.5.2 Rectification and erasure 125
6.1.5.3 Right to data portability 126
6.1.5.4 Right to object 127
6.1.5.5 Automated individual decision-making 129
6.1.6 Data Protection Impact Assessment (DPIA) 131
6.2 AI Act 132
6.3 EU policy on digital education 138
Chapter 7. Brazil's relevant legal frameworks 142
7.1 The Brazilian General Data Protection Law (LGPD) 143
7.1.1 General Principles for Data Processing 143
7.1.2 Art. 14, LGPD 144
7.1.2.1 Children's consent and applicable legal bases for processing children's data 145
7.1.2.2 Transparency obligations 150
7.1.2.3 Purpose limitation and data minimization requirements 151
7.1.3 Other legal bases for processing children's data 152
7.1.4 Data subjects' rights 154
7.1.5 DPIA 155
7.2 The right to education 156
7.3 The Brazilian Artificial Intelligence Bill 157
7.4 Brazilian policy on digital education 159
PART III. CHALLENGES INTRODUCED BY EDTECH TO CHILDREN'S RIGHTS TO PRIVACY AND TO THE PROTECTION OF PERSONAL DATA 163
Chapter 8. Mapping the challenges introduced by edtech 164
8.1 Datafication 165
8.1.1 Reduction and abstraction 166
8.1.2 Data collection for AI systems operation 167

8.2 Data Generation 169
8.2.1 Bias 172
8.2.2 The challenge of controlling inferences based on personal data 175
8.3 Decision-making 176
8.3.1 Profiling 177
8.3.2 Predictions 180
8.3.2.1 Crystallization of the past 180
8.3.2.2 Unfalsifiability and preemptive intervention 182
8.3.2.3 Performativity 183
8.3.3 Human mis-interpretation and mis-use of data 186
8.3.4 Personalized learning 190
8.3.4.1 Technologies for Personalized Learning 192
8.3.4.2 Lack of robust evidence of their effectiveness 194
8.3.4.3 Limits to personalization 195
8.3.4.4 Content filtering 196
8.3.5 Student monitoring technologies 197
8.3.5.1 Behavior Monitoring 198
8.3.5.2 e-Proctoring 201
8.3.6 Learning Analytics and further use of data 202
Interim conclusion 206
Chapter 9. Google Workspace for Education 208
9.1 What is Google Workspace for Education 208
9.2 The main features of Google Workspace for Education 211
9.3 The role of Google Workspace for Education within Google's business model 213
Interim conclusion 219
Chapter 10. The use of Google Workspace for Education in the European Union and in Brazil 221
10.1 Belgium 222
10.2 Denmark 225
10.3 Finland 229
10.4 France 231
10.5 Germany 232
10.6 Netherlands 234
10.7 Norway 237

10.8 Spain 239
10.9 Sweden 241
10.10 Brazil 242
10.10.1 The formalization of the relationship between Google and the schools 244
10.10.2 Privacy and data protection issues 247
10.10.2.1 Roles and responsibilities 248
10.10.2.2 Purposes for processing personal data 249
10.10.2.3 Lawful Bases 250
10.10.2.4 Transparency obligations 251
Interim Conclusion 254
Chapter 11. Analysis 256
11.1 Tensions between the GDPR, LGPD and Google Workspace for Education 256
11.1.1 Roles and responsibilities 256
11.1.2 Purposes for processing personal data 258
11.1.3 Lawful Bases 260
11.1.4 Transparency obligations 262
11.1.5 DPIA and risk assessment 263
11.1.6 Data Transfers 265
11.2 Appropriation of resources through the lack of compliance with the data protection framework 266
11.3 Unequal data relations and global distribution of the benefits of resource appropriation 267
11.4 Digital sovereignty 268
11.4.1 The concept of digital sovereignty 269
11.4.2 Data colonialism actors and digital sovereignty 271
11.4.3 A broader notion of digital sovereignty 273
Interim Conclusion 275
CONCLUDING REMARKS 276
Recommendations and indications for future research 285
COMPLETE TABLE OF CONTENTS 290
REFERENCES 295

REFERENCES

5RIGHTS FOUNDATION. **Disrupted Childhood: The cost of persuasive design**. [*S. l.: s. n.*], 2023. Available at: https://5rightsfoundation.com/uploads/Disrupted-Childhood-2023-v2.pdf. Accessed on: 26 dec. 2023.

5RIGHTS FOUNDATION. **Pathways: How digital design puts children at risk**. [*S. l.: s. n.*], 2021. Available at: https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf. Accessed on: 8 jun. 2023.

AEPD. **Resolución de Procedimiento Sancionador. Expediente N.º EXP202102527**. [*S. l.: s. n.*], 2023a. Available at: https://www.aepd.es/documento/ps-00176-2022.pdf. Accessed on: 6 dec. 2023.

AEPD. **Resolución de Procedimiento Sancionador. Expediente N.º EXP202104450**. [*S. l.: s. n.*], 2023b.

AEPD. **Resolución de Recurso de Reposición. Expediente N.º EXP202104450**. [*S. l.: s. n.*], 2023c. Available at: https://www.aepd.es/documento/reposicion-ps-00334-2022.pdf. Accessed on: 6 dec. 2023.

AGÊNCIA SENADO. Política Nacional de Educação Digital é sancionada com vetos. **Senado Notícias**, [*s. l.*], 12 jan. 2023. Available at: https://www12.senado.leg.br/noticias/materias/2023/01/12/politica-nacional-de-educacao-digital-e-sancionada-com-vetos#:~:text=O%20presidente%20Luiz%20In%C3%A1cio%20Lula,programa%C3%A7%C3%A3o%20e%20rob%C3%B3tica%20nas%20escolas. Accessed on: 25 oct. 2023.

AGUIAR JÚNIOR, Ruy Rosado de. **Jornadas de Direito Civill I, III, IV e V: Enunciados Aprovados**. Brasília: [*s. n.*], 2012. Available at: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/EnunciadosAprovados-Jornadas-1345.pdf. Accessed on: 9 oct. 2023.

ALLEN, Simon. How A Culture Of Listening Can Drive Digital Transformation. **Forbes**, [*s. l.*], 9 sep. 2022. Available at: https://www.forbes.com/sites/forbesbusinesscouncil/2022/09/09/how-a-culture-of-listening-can-drive-digital-transformation/. Accessed on: 30 jul. 2023.

ALSTON, Philip. **Extreme poverty and human rights. Note by the Secretary-General. A/74/493**. [*S. l.: s. n.*], 2019. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement. Accessed on: 1 jul. 2023.

AMERICAN CIVIL LIBERTIES UNION (ACLU). **Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling**. [*S. l.: s. n.*], 2023. Available at: https://www.aclu.org/publications/digital-dystopia-the-danger-in-buying-what-the-edtech-surveillance-industry-is-selling. Accessed on: 25 dec. 2023.

AMIEL, Tel *et al.* Os modos de adesão e a abrangência do capitalismo de vigilância na educação brasileira. **Perspectiva**, [*s. l.*], v. 39, n. 3, p. 1–22, 2021.

AMIEL, Tel; GONSALES, Priscila; SEBRIAM, Debora. Recursos Educacionais Abertos no Brasil: 10 anos de ativismo. **Em Rede: Revista de Educação à Distância**, [*s. l.*], v. 5, n. 2, 2018. Available at: https://www.aunirede.org.br/revista/index.php/emrede/article/view/346/326. Accessed on: 25 oct. 2023.

ANPD. **Estudo Preliminar: Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. 2022a. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Accessed on: 5 oct. 2023.

ANPD. **Glossário de Proteção de Dados Pessoais e Privacidade**. 2024a Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf. Accessed on: 5 Feb. 2024.

ANPD. **Guia Orientativo. Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse**. 2024b. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Accessed on: 5 feb. 2024.

ANPD. **Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**. [*S. l.*], 2023. Available at: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Accessed on: 8 oct. 2023.

ANPD. Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União, Edição 20, Seção 1**: Brazil, n. Resolução CD/ANPD Nº 2, p. 6, 27 jan. 2022b. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Accessed on: 8 oct. 2023.

AP. **Advies Autoriteit Persoonsgegevens (AP) aan SURF en SIVON inzake Google G Suite for Education**. [*S. l.: s. n.*], 2021a. Available at: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10202&did=2021D22378. Accessed on: 27 sep. 2023.

AP. **Borging privacy in het onderwijs bij Google producte**. [*S. l.: s. n.*], 2023. Available at: https://www.autoriteitpersoonsgegevens.nl/uploads/imported/brief_ap_privacy_in_het_onderwijs_bij_google-producten.pdf. Accessed on: 27 sep. 2023.

AP. **Brief van de Autoriteit Persoonsgegevens aan de minister van Onderwijs Cultuur en Wetenschap over borging privacy in het onderwijs en de inzet van Google G Suite for Education**. [*S. l.: s. n.*], 2021b.

AP. **Brief van de Autoriteit Persoonsgegevens aan de minister voor Basis- en Voortgezet Onderwijs en Media over borging privacy in het onderwijs en de inzet van Google G Suite**

for Education. [*S. l.: s. n.*], 2021c. Available at: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10202&did=2021D22378. Accessed on: 27 sep. 2023.

ARORA, Payal. General Data Protection Regulation-A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South. **Surveillance & Society**, [*s. l.*], v. 17, n. 5, p. 717–725, 2019.

ARORA, Payal. The Bottom of the Data Pyramid: Big Data and the Global South. **International Journal of Communication**, [*s. l.*], v. 10, p. 1681–1699, 2016. Available at: https://ijoc.org/index.php/ijoc/article/view/4297/1616. Accessed on: 20 jun. 2023.

ASSEMBLÉE NATIONALE. **16ème législature. Question N° 971 de M. Philippe Latombe (Démocrate (MoDem et Indépendants) - Vendée) Question écrite**. [*S. l.: s. n.*], 2022a. Available at: https://questions.assemblee-nationale.fr/q16/16-971QE.htm. Accessed on: 30 sep. 2023.

ASSEMBLÉE NATIONALE. **Numérique. Gratuité d'Office 365**. [*S. l.: s. n.*], 2022b. Available at: https://questions.assemblee-nationale.fr/static/16/questions/jo/jo_anq_202234.pdf. Accessed on: 30 sep. 2023.

ATABEY, Ayca. Balancing interests in EdTech: When is the lawful basis of "legitimate interests" justified? **The Digital Futures Commission, 5Rights Foundation**, [*s. l.*], 20 sep. 2021.

AUSLOOS, Jef. Balancing in the GDPR: legitimate interests v. right to object. **Centre for IT and IP Law Blog**, Leuven, 28 fev. 2017. Available at: https://www.law.kuleuven.be/citip/blog/balancing-in-the-gdpr-legitimate-interests-v-right-to-object/. Accessed on: 20 fev. 2024.

BÄCKE, Maria. Resisting Commodification: Subverting the Power of the Global Tech Companies. **Bandung**, [*s. l.*], v. 9, n. 1–2, p. 49–79, 2022.

BAKER, Ryan S. Artificial Intelligence in education: Bringing it all together. *In*: OECD (org.). **OECD Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots,**. Paris: OECD Publishing, 2021. p. 43–54. Available at: https://doi.org/10.1787/589b283f-en. Accessed on: 12 nov. 2023.

BANK, Max *et al.* **The Lobby Network: Big Tech's Web of Influence in the EU**. [*S. l.: s. n.*], 2021. Available at: https://corporateeurope.org/sites/default/files/2021-08/The%20lobby%20network%20-%20Big%20Tech%27s%20web%20of%20influence%20in%20the%20EU.pdf. Accessed on: 27 sep. 2023.

BARASSI, Veronica. **CHILD | DATA | CITIZEN**. [*S. l.*]: MIT Press, 2020.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, [*s. l.*], v. 104, n. 3, p. 671–732, 2016. Available at: http://dx.doi.org/10.15779/Z38BG31.

BARRET, Lindsey *et al.* **The Case for Better Governance of Children's Data: A Manifesto**. [*S. l.: s. n.*], 2021. Available at: https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance. Accessed on: 9 oct. 2023.

BATES, A. W. **Teaching in a Digital Age - Second Edition**. [*S. l.*]: Tony Bates Associates, 2019. Available at: https://pressbooks.bccampus.ca/teachinginadigitalagev2/.

BEDINGFIELD, Will. Everything that went wrong with the botched A-Levels algorithm. **Wired**, [*s. l.*], 19 aug. 2020. Available at: https://www.wired.co.uk/article/alevel-exam-algorithm. Accessed on: 4 mai 2023.

BEIJING CONSENSUS ON ARTIFICIAL INTELLIGENCE AND EDUCATION. . [*S. l.: s. n.*], 2019. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000368303. Accessed on: 17 dec. 2023.

BERTRAND, Melanie; MARCH, Julie. How data-driven reform can drive deficit thinking. **Phi Delta Kappan**, [*s. l.*], v. 102, n. 8, p. 35–39, 2021.

BERTRAND, Melanie; MARSH, Julie A. Teachers' Sensemaking of Data and Implications for Equity. **American Educational Research Journal**, [*s. l.*], v. 52, n. 5, p. 861–893, 2015.

BESSON, Samantha; KLEBER, Eleonor. Article 2: The Right to Non-Discrimination. *In*: TOBIN, John; ALSTON, Philip (org.). **The UN Convention on the Rights of the Child: A Commentary**. [*S. l.*]: Oxford University Press, 2019. p. 41–72. Available at: http://www.

BIESTA, Gert. Against learning: Reclaiming a language for education in an age of learning. **Nordik Pedagogik**, [*s. l.*], v. 25, p. 54–66, 2005. Available at: http://www.learndirect.co.uk/personal;

BIESTA, Gert. **Beyond Learning: Democratic Education for Human Future**. [*S. l.*]: Routledge, 2016a.

BIESTA, Gert. **Good Education in an Age of Measurement: Ethics, Politics, Democracy**. New York: Routledge, 2010.

BIESTA, Gert. **The Beautiful Risk of education**. [*S. l.*]: Routledge, 2016b.

BINDER, Krisztina. **Progress on the European Commission's 2021-2027 digital education action plan**. [*S. l.: s. n.*], 2023. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/745689/EPRS_BRI(2023)745689_EN.pdf. Accessed on: 22 oct. 2023.

BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. **Temas Centrais na Regulação de IA: o local, regional e o global na busca da interoperabilidade regulatória**. São Paulo: [*s. n.*], 2023. Available at: https://www.dataprivacybr.org/wp-content/uploads/2023/12/dataprivacy_nota-tecnica-temas-regulatorios.pdf. Accessed on: 19 dec. 2023.

BONAMIGO, Samuel. Our commitment to the privacy and security of Google Workspace customer data. **Google Cloud Blog**, [*s. l.*], 2 mar. 2021. Available at: https://cloud.google.com/blog/topics/inside-google-cloud/our-commitment-to-the-privacy-and-security-of-google-workspace-customer-data. Accessed on: 27 sep. 2023.

BORNE, Élisabeth. **Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre»)**. [*S. l.*], 2023. Available at: https://www.legifrance.gouv.fr/circulaire/id/45446?fonds=CIRC&page=1&pageSize=10&query=cloud&searchField=ALL&searchType=ALL&tab_selection=all&typePagination=DEFAULT. Accessed on: 27 sep. 2023.

BOUT, Bram. Protecting Students with Google Apps for Education. **Google Cloud Official Blog**, [*s. l.*], 30 apr. 2014. Available at: https://cloud.googleblog.com/2014/04/protecting-students-with-google-apps.html. Accessed on: 10 aug. 2023.

BRADFORD, Anu. **The Brussels effect : how the European Union rules the world**. Oxford: Oxford University Press, 2020.

BRASIL. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. Brazil: 9 jul. 2019. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Accessed on: 17 nov. 2023.

BRASIL. **Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança**. Brazil: 1 jan. 2023a. Available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm. Accessed on: 17 nov. 2023.

BRASIL. **Código Civil (CC)**. Brazil: 10 jan. 2022a. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Accessed on: 17 nov. 2023.

BRASIL. **Código de Defesa do Consumidor (CDC)**. Brazil: 11 sep. 1990. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Accessed on: 17 nov. 2023.

BRASIL. **Constituição da República Federativa do Brasil (CRFB)**. Brazil: 5 oct. 1988. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on: 17 nov. 2023.

BRASIL. **Estabelece normas educacionais excepcionais a serem adotadas durante o estado de calamidade pública reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020; e altera a Lei nº 11.947, de 16 de junho de 2009**. Brazil: 18 aug. 2020. Available at: https://www.in.gov.br/en/web/dou/-/lei-n-14.040-de-18-de-agosto-de-2020-272981525. Accessed on: 17 nov. 2023.

BRASIL. **Estabelece o regime jurídico das parcerias entre a administração pública e as organizações da sociedade civil, em regime de mútua cooperação, para a consecução de**

finalidades de interesse público e recíproco, mediante a execução de atividades ou de projetos previamente estabelecidos em planos de trabalho inseridos em termos de colaboração, em termos de fomento ou em acordos de cooperação; define diretrizes para a política de fomento, de colaboração e de cooperação com organizações da sociedade civil; e altera as Leis nºs 8.429, de 2 de junho de 1992, e 9.790, de 23 de março de 1999. 31 jul. 2014. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13019.htm. Accessed on: 17 nov. 2023.

BRASIL. **Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital**. Brazil: 21 mar. 2018a. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Accessed on: 17 nov. 2023.

BRASIL. **Lei de Acesso à Informação (LAI)**. Brazil: 18 nov. 2011a. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Accessed on: 17 nov. 2023.

BRASIL. **Lei de Interceptação Telefônica**. Brazil: 24 jul. 1996. Available at: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Accessed on: 17 nov. 2023.

BRASIL. **Lei de Licitações e Contratos Administrativos**. Brazil. 1 apr. 2021. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Accessed on: 1 jan. 2024.

BRASIL. **Lei do Cadastro Positivo**. Brazil: 9 jun. 2011b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Accessed on: 17 nov. 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brazil: 14 aug. 2018b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: 17 nov. 2023.

BRASIL. **Marco Civil da Internet (MCI)**. Brazil: 23 apr. 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 17 nov. 2023.

BRASIL. **Política Nacional da Educação Digital (PNED)**. 11 jan. 2023b. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm#:~:text=LEI%20N%C2%BA%2014.533%2C%20DE%2011%20DE%20JANEIRO%20DE%202023&text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,30%20de%20outubro%20de%202003. Accessed on: 17 nov. 2023.

BRASIL. **Projeto de Lei N° 2338, de 2023, Dispõe sobre o uso da Inteligência Artificial**. Brazil: 2023c. Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1701182930272&disposition=inline. Accessed on: 19 dec. 2023.

BRASIL. **Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019**. 25 oct. 2022b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm. Accessed on: 17 nov. 2023.

BRAUN, Anette *et al.* **Rethinking education in the digital age**. [*S. l.: s. n.*], 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641528/EPRS_STU(2020)641528_EN.pdf. Accessed on: 30 jul. 2023.

BRAZILIAN NETWORK INFORMATION CENTER. **2022 ICT in Education. Survey on the Use of Information and Communication Technologies in Brazilian Schools**. São Paulo: [*s. n.*], 2023. Available at: https://cetic.br/media/docs/publicacoes/2/20231122132216/tic_educacao_2022_livro_completo.pdf. Accessed on: 11 dec. 2023.

BRAZILIAN NETWORK INFORMATION CENTER. **ICT in Education 2020: Survey on the Use of Information and Communication Technologies in Brazilian Schools**. [*S. l.: s. n.*], 2021. Available at: https://cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf. Accessed on: 1 nov. 2023.

BRIGGS, S. **The evolution of Learning Technologies**. [*S. l.*], 2014. Available at: https://www.opencolleges.edu.au/informed/features/the-evolution-of-learning-technology/. Accessed on: 11 mar. 2023.

BRIN, Sergey; PAGE, Lawrence. **The anatomy of a large-scale hypertextual Web search engineComputer Networks and ISDN Systems**. Stanford: [*s. n.*], 1998. Available at: http://infolab.stanford.edu/pub/papers/google.pdf. Accessed on: 21 jul. 2023.

BRINKMEYER, Holger. LfDI Nordrhein-Westfalen gibt Update zum Einsatz von Microsoft 365 in Schulen. **Datenschutz Notizen**, [*s. l.*], 11 jul. 2023. Available at: https://www.datenschutz-notizen.de/lfdi-nordrhein-westfalen-gibt-update-zum-einsatz-von-microsoft-365-in-schulen-1043574/. Accessed on: 27 sep. 2023.

BROWNLOW, Josh *et al.* **Data and Analytics-Data-Driven Business Models: A Blueprint for Innovation**. [*S. l.: s. n.*], 2015. Available at: https://cambridgeservicealliance.eng.cam.ac.uk/system/files/documents/2015MarchPaperTheDDBMInnovationBlueprint.pdf. Accessed on: 21 jul. 2023.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). **SiSyPHuS Win10: Telemetry in Windows 10**. [*S. l.*], 2018. Available at: https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html. Accessed on: 27 sep. 2023.

BYGRAVE, Lee A. Article 4(4). profiling. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation (GDPR): A Commentary**. [*S. l.*]: Oxford University Press, 2020a. p. 127–131.

BYGRAVE, Lee A. Article 22. Automated individual decision- making, including profiling. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary**. [*S. l.*]: Oxford University Press, 2020b. p. 522–542.

CALZATI, Stefano. Decolonising "Data Colonialism" Propositions for Investigating the Realpolitik of Today's Networked Ecology. **Television and New Media**, [*s. l.*], v. 22, n. 8, p. 914–929, 2021.

CANNATACI, Joseph A. **Artificial intelligence and privacy, and children's privacy. Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. A/HRC/46/37**. [*S. l.: s. n.*], 2021. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement. Accessed on: 16 jul. 2023.

CARDONA, Miguel A; RODRÍGUEZ, Roberto J; ISHMAEL, Kristina. **Artificial Intelligence and the Future of Teaching and Learning - Insights and Recommendations**. Washington: [*s. n.*], 2023. Available at: https://www2.ed.gov/documents/ai-report/ai-report.pdf. Accessed on: 29 mai 2023.

CARR, John. The children's privacy debacle – Part 3. **Desiderata: Technology explained**, [*s. l.*], 6 jan. 2016. Available at: https://johncarr.blog/2016/01/06/the-childrens-privacy-debacle-part-3/. Accessed on: 14 jul. 2023.

CASSIDY, Arlette. Age Appropriate. *In*: VOLKMAR, F. R. (org.). **Encyclopedia of Autism Spectrum Disorders**. New York: Springer, 2013.

CENTER FOR DEMOCRACY & TECHNOLOGY (CDT). **Generative AI Systems in Education — Uses and Misuses**. [*S. l.: s. n.*], 2023. Available at: https://cdt.org/wp-content/uploads/2023/03/2023-03-15-CDT-Civic-Tech-Generative-AI-issue-brief-final.pdf. Accessed on: 27 jul. 2023.

CENTER FOR DEMOCRACY & TECHNOLOGY (CDT). **The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks**. [*S. l.: s. n.*], 2022. Available at: https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/. Accessed on: 8 mai 2023.

CHAKROUN, Borhene *et al.* **Minding the data: Protecting learners' privacy and security**. Paris: [*s. n.*], 2022. Available at: http://www.unesco.org/open-access/terms-. .

CHAUDHARY, Monica. Involvement of Children in the Family Buying: A Review. **Pacific Business Review International**, [*s. l.*], v. 8, p. 54–62, 2016. Available at: http://www.pbr.co.in/2016/2016_month/May/8.pdf. Accessed on: 2 aug. 2023.

CHENG, Hoi Wai Jackie. **Economic properties of data and the monopolistic tendencies of data economy: policies to limit an Orwellian possibility**. [*S. l.: s. n.*], 2020. Available at:

https://www.un.org/en/desa/economic-properties-data-and-monopolistic-tendencies-data-economy-policies-limit. Accessed on: 18 jun. 2023.

CHIRCOP, Denise. **The European Education Area and the 2030 strategic framework for education and training**. [*S. l.: s. n.*], 2021. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690630/EPRS_BRI(2021)690630_EN.pdf. Accessed on: 22 oct. 2023.

COBBE, Jennifer; SINGH, Jatinder. Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges. **Computer Law & Security Review**, [*s. l.*], v. 42, p. 105573, 2021. https://doi.org/10.1016/j.clsr.2021.105573.

COE. **Children's data protection in an education setting. Guidelines. Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data. Convention 108.** [*S. l.: s. n.*], 2021. Available at: https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html. Accessed on: 9 jul. 2023.

COHEN, Julie E. **Between Truth and Power: The Legal Constructions of Informational Capitalism**. [*S. l.*]: Oxford University Press, 2019.

COLLINS, Sara *et al.* **The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools**. [*S. l.: s. n.*], 2021. Available at: https://studentprivacycompass.org/resource/self-harm-monitoring/. Accessed on: 23 mai 2023.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche**. [*S. l.*], 2021. Available at: https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche. Accessed on: 27 sep. 2023.

COMMITTEE ON ECONOMIC SOCIAL AND CULTURAL RIGHTS. **CESCR General Comment No. 13: The Right to Education (Art. 13)**. [*S. l.: s. n.*], 1999a.

COMMITTEE ON ECONOMIC SOCIAL AND CULTURAL RIGHTS. **General comment No. 11: Plans of Action for Primary Education (Art. 14)**. [*S. l.: s. n.*], 1999b. Available at: https://www.refworld.org/docid/4538838c0.html. Accessed on: 11 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General Comment No. 1 (2001). Article 29(1): The aims of education**. [*S. l.: s. n.*], 2001. Available at: https://www.refworld.org/docid/4538834d2.html. Accessed on: 11 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General Comment No. 5 (2003). General measures of implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, para. 6). CRC/GC/2003/5**. [*S. l.: s. n.*], 2003. Available at: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6Zd2%2FQRsDnCTcaruSeZhPr2vUevjbn6t6GSi1fheVp%2Bj5HTLU2Ub%2FPZZtQWn0jExFVnWuhiBbqgAj0dWBoFGbK0c. Accessed on: 8 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General Comment No. 12 (2009). The right of the child to be heard. CRC/C/GC/12**. [*S. l.: s. n.*], 2009.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 13 (2011).The right of the child to freedom from all forms of violence. CRC/C/GC/13**. [*S. l.: s. n.*], 2011. Available at: https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.13_en.pdf. Accessed on: 23 jun. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14**. [*S. l.: s. n.*], 2013a.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16**. [*S. l.: s. n.*], 2013b. Available at: https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.16.pdf. Accessed on: 8 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 20 (2016) on the implementation of the rights of the child during adolescence. CRC/C/GC/20**. [*S. l.: s. n.*], 2016. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/404/44/PDF/G1640444.pdf?OpenElement. Accessed on: 9 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25**. [*S. l.: s. n.*], 2021. Available at: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Accessed on: 26 jun. 2023.

COMPUTER-BASED LEARNING. [*S. l.*], 2009. Available at: https://edutechwiki.unige.ch/en/Computer-based_learning. Accessed on: 11 mar. 2023.

COMPUTER-BASED TRAINING. [*S. l.*], 2009. Available at: https://edutechwiki.unige.ch/en/Computer-based_training. Accessed on: 11 mar. 2023.

CONSED. NOVA ESCOLA, com apoio da Fundação Lemann e do Google.org, lança primeiros planos de aula alinhados à BNCC, 2018. Available at: https://www.consed.org.br/noticia/nova-escola-com-apoio-da-fundacao-lemann-e-do-google-org-lanca-primeiros-planos-de-aula-alinhados-a-bncc. Accessed on: 11 dec. 2023.

CONSED. Sobre o Consed, [s. d.]. Available at: https://www.consed.org.br/conteudos/sobre-o-consed. Accessed on: 11 dec. 2023.

CONSELHO DA JUSTIÇA FEDERAL. **Jornadas de Direito Civil Enunciados Aprovados**. [*S. l.*], [*s. d.*].

CORCORAN, Betsy. A Brief History of (Edtech) Time. **Texas Education Review**, [*s. l.*], v. 1, p. 104–118, 2013.

CORPORATE EUROPE OBSERVATORY. **How the Commission outsourced its merger policy to Google's best friend**. [*S. l.*], 2023. Available at: https://corporateeurope.org/en/2023/04/how-commission-outsourced-its-merger-policy-googles-best-friend. Accessed on: 14 sep. 2023.

CORTADA, James W. **Before the computer : IBM, NCR, Burroughs, and Remington Rand and the industry they created, 1865-1956**. [*S. l.*]: Princeton University Press, 1993.

CORTESI, Sandra *et al.* **Youth and Extended Reality: An Initial Exploration of Augmented, Virtual, and Mixed Realities**. [*S. l.: s. n.*], 2021. Available at: https://cyber.harvard.edu/publication/2021/youth-extended-reality. Accessed on: 30 jul. 2023.

COTHRAN, Ann; MASON, George E. The Typewriter: Time-Tested Tool for Teaching Reading and Writing. **The Elementary School Journal**, [*s. l.*], v. 78, n. 3, p. 170–173, 1978. Available at: https://www.jstor.org/stable/1001415. Accessed on: 15 mai 2023.

COULDRY, Nick; DIJCK, José van. Researching Social Media as if the Social Mattered. **Social Media and Society**, [*s. l.*], v. 1, n. 2, 2015.

COULDRY, Nick; MEJIAS, Ulises A. **The Costs of Connection: How Data is Colonising Human Life and Appropriating it for Capitalism**. Stanford: Standard University Press, 2019.

COULDRY, Nick; MEJIAS, Ulises Ali. The decolonial turn in data and technology research: what is at stake and where is it heading?. **Information Communication and Society**, [*s. l.*], v. 26, n. 4, p. 786–802, 2023.

COUNCIL OF THE EUROPEAN UNION. **Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world**. [*S. l.*], 2023a. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Accessed on: 18 dec. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Recommendation of 22 May 2018 on key competences for lifelong learning. ST/9009/2018/INIT**. [*S. l.: s. n.*], 2018a. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AC%3A2018%3A189%3ATOC&uri=uriserv%3AOJ.C_.2018.189.01.0001.01.ENG. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Recommendation of 22 May 2018 on promoting common values, inclusive education, and the European dimension of teaching. ST/9010/2018/INIT**. [*S. l.: s. n.*], 2018b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0607%2801%29. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Resolution on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) 2021/C 66/01**. [*S. l.: s. n.*], 2021a. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32021G0226%2801%29. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Resolution on the governance structure of the strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) 2021/C 497/01. ST/14487/2021/INIT**. [*S. l.: s. n.*], 2021b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021G1210%2801%29. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Press conference following the trilogue on artificial intelligence**. [*S. l.*], 2023b. Available at: https://video.consilium.europa.eu/event/en/27283. Accessed on: 18 dec. 2023.

COUNCIL OF THE EUROPEAN UNION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement**. Brussels, 2024. Available at: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf. Accessed on: 30 jan. 2024.

COURSERA. **2021 Impact Report. Serving the world through learning**. [*S. l.: s. n.*], 2021. Available at: https://aboct.coursera.org/press/wp-content/uploads/2021/11/2021-Coursera-Impact-Report.pdf. Accessed on: 12 nov. 2023.

COURTIS, Christian; TOBIN, John. Article 28. The Right to Education. *In*: TOBIN, John (org.). **The UN Convention on the Rights of the Child: A Commentary**. Oxford: Oxford University Press, 2019. p. 1056–115.

COWAN, Leah; ARBOINE, Niellah; ALEMORU, Kemi. **For black students, badly-predicted grades are the tip of the iceberg**. [*S. l.*], 2020. Available at: https://gal-dem.com/for-black-students-badly-predicted-grades-are-the-tip-of-the-iceberg/. Accessed on: 5 mai 2023.

CRANDALL, Marc. Helping European education providers navigate privacy assessments. **Google Cloud Blog**, [*s. l.*], 18 aug. 2022a. Available at: https://cloud.google.com/blog/products/identity-security/helping-european-education-providers-navigate-privacy-assessments. Accessed on: 27 sep. 2023.

CRANDALL, Marc. Introducing new commitments on the processing of service data for our cloud customers. **Google Cloud Blog**, [*s. l.*], 17 jun. 2022b. Available at: https://cloud.google.com/blog/products/identity-security/introducing-new-commitments-on-the-processing-of-service-data-for-our-cloud-customers. Accessed on: 27 sep. 2023.

CRUZ, Leonardo Ribeiro da; VENTURINI, Jamila Rodrigues. Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19. **Revista Brasileira de Informática na Educação**, [*s. l.*], v. 28, p. 1060–1085, 2020.

CYNDECKA, Malgorzata Agnieszka. A dystopian story about COVID-19, Artificial Intelligence setting grades and the GDPR. **EFTA-Studies.org**, [*s. l.*], 5 sep. 2020. Available at: https://www.efta-studies.org/post/a-dystopian-story-about-covid-19-artificial-intelligence-setting-grades-and-the-gdpr. Accessed on: 17 oct. 2023.

CZERNIEWICZ, L. Educational technology - mapping the terrain with Bernstein as cartographer. **Journal of Computer Assisted Learning**, [*s. l.*], v. 26, n. 6, p. 523–534, 2010.

DAMANI, Kalifa; MITCHELL, Joel. **Rapid Evidence Review: Radio**. [*S. l.: s. n.*], 2020. Available at: http://edtechhub.org/wp-content/uploads/2020/09/Rapid-Evidence-Review_-Radio-1.pdf. Accessed on: 24 jul. 2023.

DARK, Martha. UK: Legal action threatened over algorithm used to grade teenagers' exams. **Statewatch**, [*s. l.*], 12 aug. 2020. Available at: https://www.statewatch.org/news/2020/august/uk-legal-action-threatened-over-algorithm-used-to-grade-teenagers-exams/. Accessed on: 17 oct. 2023.

DATA MINING OF SCHOOL KIDS. direção: Jose Ferreira. [*S. l.*]: Knewton Education Datapalooza, 2012. Available at: https://www.youtube.com/watch?v=qIbMLVJi4qc&t=0s. Accessed on: 17 dec. 2023.

DATA SPACES SUPPORT CENTRE (DSSC). **Blueprint Version 0.5**. [*S. l.: s. n.*], 2023. Available at: https://dssc.eu/space/BPE/179175433/Data+Spaces+Blueprint+%7C+Version+0.5+%7C+September+2023?attachment=/rest/api/content/179175433/child/attachment/att187400211/download&type=application/pdf&filename=DSSC-Blueprint-Version-1.0.pdf. Accessed on: 4 nov. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Alvorlig kritik af Helsingør Kommune i Chromebook-sag**. [*S. l.*], 2021. Available at: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brud-paa-persondatasikkerheden. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Chromebooks: Datatilsynet suspenderer forbud og giver påbud om lovliggørelse**. [*S. l.*], 2022a. Available at: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/chromebooks-datatilsynet-suspenderer-forbud-og-giver-paabud-om-lovliggoerelse-. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Datatilsynet fastholder forbud i Chromebook-sag**. [*S. l.*], 2022b. Available at: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Datatilsynet nedlægger behandlingsforbud i Chromebook-sag**. [*S. l.*], 2022c. Available at: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Datatilsynet undersøger kommuners materiale om Google Workspace**. [*S. l.*], 2022d. Available at: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/datatilsynet-undersoeger-kommuners-materiale-om-google-workspace. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Konstruktivt møde om Chromebooks**. [*S. l.*], 2022e. Available at: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/aug/konstruktivt-moede-om-chromebooks. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Yderligere materiale udsætter afgørelse om Chromebooks**. [*S. l.*], 2022f. Available at: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/dec/yderligere-materiale-udsaetter-afgoerelse-om-chromebooks. Accessed on: 27 sep. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Advance notification of order to rectify unfairly processed and incorrect personal data - International Baccalaureate Organization**. [*S. l.: s. n.*], 2020a. Available at: https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf. Accessed on: 17 oct. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Bruk av Google Chromebook og G Suite for Education (og andre skytjenester) i grunnskolen**. [*S. l.*], 2020b. Available at: https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bruk-av-google-chromebook-og-g-suite-for-education-og-andre-skytjenester-i-grunnskolen/. Accessed on: 5 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Order to provide information – International Baccalaureate Organization – Awarding model and grading system**. [*S. l.: s. n.*], 2020c. Available at: https://www.datatilsynet.no/contentassets/ea9284bbfcb64f819b2171228bc912a4/ibo---order-to-provide-information-by-24-july-2020.pdf. Accessed on: 17 oct. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om irettesettelse for feil bruk av Googles løsninger i skolen**. [*S. l.*], 2020d. Available at: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-irettesettelse-for-feil-bruk-av-googles-losninger-i-skolen/. Accessed on: 4 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om vedtak om irettesettelse - Bruk av G Suite for Education - Sandnes Kommune**. [*S. l.: s. n.*], 2020e. Available at: https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse---bruk-av-g-suite-for-education---sandnes.pdf. Accessed on: 4 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om vedtak om irettesettelse - Bruk av Google Chromebook i skolen - Strand Kommune**. [*S. l.: s. n.*], 2020f. Available at: https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse---bruk-av-google-chromebook-i-skolen---strand.pdf. Accessed on: 4 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om vedtak om irettesettelse - Bruk av Google Chromebook og G Suite for Education i skolen - Bergen Kommune**. [*S. l.: s. n.*], 2020g. Available at: https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse---bruk-av-google-chromebook-og-g-suite-for-education---bergen2.pdf. Accessed on: 4 dec. 2023.

DATENSCHUTZKONFERENZ. **AG DSK „Microsoft-Onlinedienste" Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung**. [*S. l.*: *s. n.*], 2022. Available at: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf. Accessed on: 30 sep. 2023.

DAVENPORT, Thomas H. **Big data @ work: dispelling the myths, uncovering the opportunities**. Boston: Harvard Business Review Press, 2014.

DEDEZADE, E. Microsoft to deliver cloud services from new datacentres in Germany in 2019 to meet evolving customer needs. **Microsoft Stories Europe**, [*s. l.*], 31 aug. 2018. Available at: https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/. Accessed on: 27 sep. 2023.

DENSA, Roberta. Artigo 14. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Comentários à Lei Geral de Proteção de Dados Pessoais**. 2. ed. [*S. l.*]: Editora Foco, 2023. p. 206–224.

DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT. **Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen**. [*S. l.*], 2019a. Available at: http://web.archive.org/web/20191220095453/https:/datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und. Accessed on: 27 sep. 2023.

DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT. **Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen**. [*S. l.*], 2019b. Available at: http://web.archive.org/web/20221203045150/https:/datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen. Accessed on: 27 sep. 2023.

DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT BADEN-WÜTTEMBER. **Empfehlung des LfDI hinsichtlich der Nutzung der geprüften Version von Microsoft Office 365 an Schulen**. [*S. l.*], 2021. Available at: https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-gepruefteten-version-von-microsoft-office-365-an-schulen-ab/. Accessed on: 27 sep. 2023.

DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT BADEN-WÜTTEMBER. **Hinweise des LfDI zur Nutzung von Microsoft 365 durch Schulen**. [*S. l.*], 2022. Available at: https://www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen/. Accessed on: 27 sep. 2023.

DERECHOS DIGITALES; PRIVACY INTERNATIONAL. **Stakeholder Report -Universal Periodic Review 41st Session-Brazil**. [*S. l.: s. n.*], 2022. Available at: https://privacyinternational.org/sites/default/files/2022-11/Final%20Brazil%20UPR.pdf. Accessed on: 1 nov. 2023.

DIJCK, José van. Datafication, dataism and dataveillance: data between scientific paradigm and ideology. **Surveillance & Society**, [*s. l.*], v. 12, n. 2, p. 197–208, 2014.

DIJCK, José van. Seeing the forest for the trees: Visualizing platformization and its governance. **New Media and Society**, [*s. l.*], v. 23, n. 9, p. 2801–2819, 2021.

DIJCK, José van. **The Culture of Connectivity: A Critical History of Social Media**. New York: Oxford University Press, 2013.

DIJCK, José van; POELL, Thomas; WAAL, Martijn de. **The Platform Society**. New York: Oxford Univeristy Press, 2018.

DINUM. **Le Cloud pour les administrations**. [*S. l.*], [*s. d.*]. Available at: https://www.numerique.gouv.fr/services/cloud/doctrine/. Accessed on: 27 sep. 2023.

DISHON, Gideon. New data, old tensions: Big data, personalized learning, and the challenges of progressive education. **Theory and Research in Education**, [*s. l.*], v. 15, n. 3, p. 272–289, 2017.

D'MELLO, Sidney. Improving student engagement in and with digital learning technologies. *In*: OECD DIGITAL EDUCATION OUTLOOK 2021: PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS. Paris: OECD Publishing, 2021. p. 79–104.

DOEK, Jaap. The CRC General Principles. *In*: 18 CANDLES: THE CONVENTION ON THE RIGHTS OF THE CHILD REACHES MAJORITY. [*S. l.*]: Institut International des Droits de l'Enfant, 2007. p. 31–38. Available at: http://www.childsrights.org.

DPC. **Children front and centre: Fundamentals for a child-oriented approach to data processing**. Dublin: [*s. n.*], 2021. Available at: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf. Accessed on: 17 jul. 2023.

DRECHSLER, Laura; ELBI, Abdullah; KINDT, Els; KUN, Eyup; MESZAROS, Janos; VRANCKAERT, Koen. **CiTiP Working Paper Series. Third time is the charm? The draft Data Privacy Framework for international personal data transfers from the European Union to the United States**. KU Leuven Centre for IT & IP Law – imec. 23 may 2023.

Available at: https://www.law.kuleuven.be/citip/en/docs/books/citip-working-paper-2023-drechsler-elbi-kindt-kun.pdf. Accessed on: 14 feb. 2024.

DRECHSLER, Laura; VOGIATZOGLOU, Plixavra. Quo vadis purpose limitation? Norra Stockholm Bygg AB v Per Nycander AB. **European Law Review**, [*s. l.*], v. 48, n. 4, p. 469–479, 2023.

DUCUING, Charlotte. Beyond the data flow paradigm: governing data requires to look beyond data. **Technology and Regulation**, [*s. l.*], p. 57–64, 2020. https://doi.org/10.26116/techreg.2020.006.

DUCUING, Charlotte; SCHROERS, Jessica. The recent case law of the CJEU on (joint) controllership: have we lost the purpose of "purpose"? **Computerrecht Tijdschrift voor Informatica, Telecommunicatie en Recht**, [*s. l.*], n. 6, p. 424–429, 2020.

EDPB. **Endorsed WP29 Guidelines**. [*S. l.*], 2018. Available at: https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en. Accessed on: 27 oct. 2023.

EDPB. **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0**. [*S. l.: s. n.*], 2019. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf. Accessed on: 17 jul. 2023.

EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1**. [*S. l.: s. n.*], 2020. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Accessed on: 14 jul. 2023.

EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.1**. [*S. l.: s. n.*], 2021.

EDPB. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**. Version 2.0. 2021. Available at: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. Accessed on: 14 jul. 2023.

ENGLER, Alex. **Enrollment algorithms are contributing to the crises of higher education**. [*S. l.: s. n.*], 2021. Available at: https://www.brookings.edu/articles/enrollment-algorithms-are-contributing-to-the-crises-of-higher-education/. Accessed on: 13 feb. 2024.

ERIKSEN, Thomas Hylland. What's wrong with the Global South and the Global North? *In*: [*S. l.*]: Global South Studies Center, University of Cologne, 2015. p. 3–4. Available at: https://kups.ub.uni-koeln.de/6399/1/voices012015_concepts_of_the_global_south.pdf. Accessed on: 20 jun. 2023.

EUROPEAN COMMISSION. **A Europe fit for the digital age: Empowering people with a new generation of technologies**. [*S. l.*], [*s. d.*]. Available at:

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en. Accessed on: 22 oct. 2023 a.

EUROPEAN COMMISSION. **A European approach to artificial intelligence**. [*S. l.*], 2021a. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#:~:text=The%202021%20review%20of%20the,critical%20component%20of%20AI%20excellence. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Antitrust: Commission sends Statement of Objections to Google over abusive practices in online advertising technology**. [*S. l.*], 2023a. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207. Accessed on: 14 aug. 2023.

EUROPEAN COMMISSION. **Artificial Intelligence – Questions and Answers**. [*S. l.*], 2023b. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION, Directorate-General for Education, Youth, Sport and Culture. **Blended learning for high quality and inclusive primary and secondary education Handbook**. Luxembourg: [*s. n.*], 2021. Available at: https://data.europa.eu/doi/10.2766/237842. Accessed on: 5 nov. 2023.

EUROPEAN COMMISSION. **Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digital Education action Plan 2021-2027 Resetting education and training for the digital age. SWD/2020/0209**. [*S. l.: s. n.*], 2020a. Available at: https://education.ec.europa.eu/sites/default/files/document-library-docs/deap-swd-sept2020_en.pdf#page=3. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Commission Staff Working Document on Common European Data Spaces. SWD/2022/45**. Brussels: [*s. n.*], 2022a. Available at: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces. Accessed on: 4 nov. 2023.

EUROPEAN COMMISSION. **Commission Staff Working Paper. Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and (…)**. Brussels: [*s. n.*], 2012. Available at: https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf. Accessed on: 15 jul. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A New Skills Agenda for Europe Working together to strengthen human capital, employability and competitiveness. COM/2016/0381**. [*S. l.: s.*

n.], 2016a. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0381. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digital Education Action Plan 2021-2027 Resetting education and training for the digital age. COM/2020/0624**. [*S. l.: s. n.*], 2020b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence. COM/2021/205**. [*S. l.*], 2021b. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2021%3A205%3AFIN. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Improving and Modernising Education. COM/2016/941**. [*S. l.: s. n.*], 2016b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0941&rid=3. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Investing in Europe's Youth. COM/2016/940. [*s. l.*], 2016c. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52016DC0940. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a renewed EU agenda for higher education. COM/2017/0247. [*s. l.*], 2017a. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0247. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on achieving the European Education Area by 2025. COM/2020/625**. [*S. l.: s. n.*], 2020c. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0625. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions School development and excellent teaching for a great start in life. COM/2017/0248. [*s. l.*], 2017b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A248%3AFIN. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the**

Committee of the Regions Strengthening European Identity through Education and Culture The European Commission's contribution to the Leaders' meeting in Gothenburg. COM/2017/0673 final. [*S. l.: s. n.*], 2017c. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A673%3AFIN. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Building a stronger Europe: the role of youth, education and culture policies. COM/2018/268**. [*S. l.: s. n.*], 2018a. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A268%3AFIN. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Coordinated Plan on Artificial Intelligence**. [*S. l.*], 2021c. Available at: https://digital-strategy.ec.europa.eu/en/policies/plan-ai. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Digital Education Action Plan Factsheet**. [*S. l.: s. n.*], 2018b. Available at: https://education.ec.europa.eu/sites/default/files/document-library-docs/digital-education-action-plan-factsheet.pdf. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **European Education Area explained**. [*S. l.*], [*s. d.*]. Available at: https://education.ec.europa.eu/about-eea/the-eea-explained. Accessed on: 22 oct. 2023 b.

EUROPEAN COMMISSION. **European Skills Agenda**. [*S. l.*], [*s. d.*]. Available at: https://ec.europa.eu/social/main.jsp?catId=1223&langId=en. Accessed on: 22 oct. 2023 c.

EUROPEAN COMMISSION. **Europe's Digital Decade**. [*S. l.*], [*s. d.*]. Available at: https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade. Accessed on: 22 oct. 2023 d.

EUROPEAN COMMISSION. **New measures to boost key competences and digital skills, as well as the European dimension of education**. [*S. l.*], 2018c. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_102. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)**. [*S. l.: s. n.*], 2022b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Recovery plan for Europe**. [*S. l.*], [*s. d.*]. Available at: https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_en. Accessed on: 22 oct. 2023 e.

EUROPEAN COMMISSION. **White Paper On Artificial Intelligence - A European approach to excellence and trust**. Brussels: [*s. n.*], 2020d. Available at: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Accessed on: 18 dec. 2023.

EUROPEAN COURT OF HUMAN RIGHTS. **Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence**. [*S. l.: s. n.*], 2022. Available at: https://www.echr.coe.int/documents/d/echr/Guide_Art_8_ENG. Accessed on: 23 jul. 2023.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). **Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments**. [*S. l.: s. n.*], 2023. Available at: https://edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf. Accessed on: 18 dec. 2023.

EUROPEAN PARLIAMENT. **Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI**. [*S. l.*], 2023. Available at: https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai. Accessed on: 18 dec. 2023.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Decision (EU) 2023/936 of the European Parliament and of the Council of 10 May 2023 on a European Year of Skills (Text with EEA relevance). PE/12/2023/REV/1**. [*S. l.: s. n.*], 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023D0936. Accessed on: 22 oct. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems**. Case C-311/18, ECLI:EU:C:2020:559. 2020. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3366705. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV**. Case C-40/17, ECLI:EU:C:2019:629. 2019. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=EN. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Hans-Dieter Jundt, Hedwig Jundt v. Finanzamt Offenburg**. C-281/06, ECLI:EU:C:2007:816. 2007a. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=71923&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1226224. Accessed on: 13 jul. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Mediakabel BV v. Commissariaat voor de Media**. C-89/04, ECLI:EU:C:2005:348. 2005. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=60336&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1290702. Accessed on: 13 jul. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **OQ v Land Hessen**. C-634/21, ECLI:EU:C:2023:957. 2023. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2565079. Accessed on: 14 dec. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis**. C-291/13, ECLI:EU:C:2014:2209. 2014. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=157524&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1225989. Accessed on: 13 jul. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta**. Case C-25/17, ECLI:EU:C:2018:551. 2018a. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2929029. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH**. Case C-210/16, ECLI:EU:C:2018:388. 2018b. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2928770. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **Official Journal L 281**: 23 nov. 1995. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Accessed on: 30 dec. 2023.

EUROPEAN UNION. Explanations relating to the Charter of Fundamental Rights. **OJ C 303, 14.12.2007, p. 17–35**: 2007b. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32007X1214%2801%29. Accessed on: 23 jul. 2023.

EUROPEAN UNION. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. **COM/2021/206**: 2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Accessed on: 30 dec. 2023.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. European Union: OJ L 119, 4.5.2016, p. 1–88, 4 mai 2016. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed on: 19 jul. 2023.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). **Handbook on European data protection law**. [*S. l.: s. n.*], 2018. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Accessed on: 18 jul. 2023.

FABBRINI, Federico. The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court. *In*: VRIES, Sybe de; BERNITZ, Ulf;

WRATHERILL, Stephen (org.). **The EU Charter of Fundamental Rights as a Binding Instrument : Five Years Old and Growing**. Oxford: Hart Publishing, 2015. p. 261–286.

FACEBOOK. **Free Basics**. [*S. l.*], [*s. d.*]. Available at: https://www.facebook.com/connectivity/solutions/free-basics. Accessed on: 1 aug. 2023.

FADER, Peter; HOYNE, Neil. Important lessons for embracing customer lifetime value. **Think with Google**, [*s. l.*], aug. 2021. Available at: https://www.thinkwithgoogle.com/marketing-strategies/data-and-measurement/customer-lifetime-value/?utm_source=rss-reader&utm_medium=rss&utm_campaign=rss-feed. Accessed on: 13 aug. 2023.

FEDDERS, Barbara. The Constant and Expanding Classroom: Surveillance in K-12 Public Schools Recommended Citation. **North Carolina Law Review**, [*s. l.*], v. 97, n. 6, p. 1673–1726, 2019. Available at: https://scholarship.law.unc.edu/nclr/vol97/iss6/4. Accessed on: 29 mai 2023.

FEDERAL TRADE COMMISSION (FTC). **FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data**. [*S. l.*], 2023. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens. Accessed on: 25 dec. 2023.

FERNANDES, Elora. Crianças e adolescentes na LGPD: Bases legais aplicáveis. **Migalhas**, [*s. l.*], 27 oct. 2020. Available at: https://www.migalhas.com.br/depeso/335550/criancas-e-adolescentes-na-lgpd--bases-legais-aplicaveis. Accessed on: 4 oct. 2023.

FERNANDES, Elora; MEDON, Filipe. Proteção de crianças e adolescentes na LGPD: desafios interpretativos. **Revista Eletrônica da PGE-RJ**, [*s. l.*], v. 4, n. 2, p. 1–24, 2021.

FERNANDES, Elora; SAS, Martin. **Putting Children First: A Critical Analysis of the European Data Strategy for Educational Data.** Gent: [*s. n.*], 2023. Available at: https://lirias.kuleuven.be/handle/20.500.12942/731220. Accessed on: 14 dec. 2023.

FLORIDI, Luciano. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. **Philosophy and Technology**, [*s. l.*], v. 33, n. 3, p. 369–378, 2020.

FLORIDI, Luciano. **The Philosophy of Information**. [*S. l.*]: Oxford University Press, 2011.

FLYNN, Laurie J. Google to Offer Services for Businesses. **The New York Times**, [*s. l.*], 28 aug. 2006. Available at: https://www.nytimes.com/2006/08/28/technology/28google.html. Accessed on: 8 aug. 2023.

FREEMAN, Michael D. A. Article 3. The Best Interests of the Child. *In*: ALEN, André *et al.* (org.). **A Commentary on the United Nations Convention on the Rights of the Child**. Leiden: Martinus Nijhoff, 2007.

FREIRE, Paulo. **Política e educação**. 5. ed. São Paulo: Cortez Editora, 2001. v. 23

GALLAGHER, Sean R *et al*. **Digital Credentials and Talent Acquisition Tech: Closing the Data Gap Between Learning and Hiring**. [*S. l.: s. n.*], 2023. Available at:

https://cps.northeastern.edu/wp-content/uploads/2023/03/Digital_Credentials_Talent_Acquisition_Tech.pdf. Accessed on: 4 mai 2023.

GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. Inteligência Artificial no Brasil ainda precisa de uma estratégia. **FGV**, Rio de Janeiro, 11 mai 2021. Available at: https://portal.fgv.br/artigos/inteligencia-artificial-brasil-ainda-precisa-estrategia. Accessed on: 19 dec. 2023.

GAYK, Betina. **28. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zum Datenschutz für die Zeit vom 1. Januar 2022 bis zum 31. Dezember 2022 und zur Informationsfreiheit für die Zeit vom 1. Januar 2021 bis zum 31. Dezember 2022**. Düsseldorf : [*s. n.*], 2023. Available at: https://www.ldi.nrw.de/system/files/media/document/file/28_datenschutzbericht_2023_ldi-nrw_1.pdf. Accessed on: 30 sep. 2023.

GIANNINI, Stefania. **Generative AI and the future of education**. [*S. l.: s. n.*], 2023. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000385877. Accessed on: 27 jul. 2023.

GLEASON, How; HEATH, B K. Injustice embedded in Google Classroom and Google Meet: A techno-ethical audit of remote educational technologies. **Italian Journal of Educational Technology**, [*s. l.*], v. 29, n. 2, p. 26–41, 2021.

GLOBAL PRIVACY ASSEMBLY (GPA). **43rd Closed Session of the Global Privacy Assembly October 2021. Adopted Resolution on children's digital rights**. [*S. l.: s. n.*], 2021. Available at: https://globalprivacyassembly.org/ wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf. Accessed on: 17 dec. 2023.

GOMES, Maria Cecília Oliveira; ZAPPELINI, Thaís Duarte. A LGPD e a obtenção do consentimento dos pais ou responsáveis pela Administração pública em escolas municipais. **Medium CEPI FGV**, [*s. l.*], 12 sep. 2020. Available at: https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1/a-lgpd-e-a-obten%C3%A7%C3%A3o-do-consentimento-dos-pais-ou-respons%C3%A1veis-pela-administra%C3%A7%C3%A3o-p%C3%BAblica-em-escolas-b9432ad3ab47. Accessed on: 4 oct. 2023.

GONZÁLEZ FUSTER, Gloria. Article 18. Right to restriction of processing. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary**. [*S. l.*]: Oxford University Press, 2020. p. 485–491.

GONZÁLEZ FUSTER, Gloria. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. [*S. l.*]: Springer, 2014.

GONZÁLEZ FUSTER, Gloria; HIJMANS, Hielke. **The EU rights to privacy and personal data protection: 20 years in 10 questions. Discussion paper**. [*S. l.: s. n.*], 2019. Available at: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf. Accessed on: 23 jul. 2023.

GOOD, Judith. Serving students with special needs better: How digital technology can help. *In*: OECD DIGITAL EDUCATION OUTLOOK 2021: PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS. Paris: OECD Publishing, 2021. p. 123–142. Available at: https://doi.org/10.1787/589b283f-en. Accessed on: 13 nov. 2023.

GOOGLE. **Aviso de Privacidade do Google Cloud**. [*S. l.*], 2023a. Available at: https://cloud.google.com/terms/cloud-privacy-notice?hl=pt-BR. Accessed on: 1 oct. 2023.

GOOGLE. **Aviso de Privacidade do Google Workspace for Education**. [*S. l.*], 2023b. Available at: https://workspace.google.com/intl/pt-br/terms/education_privacy/?hl=pt-BR#privacy-police-revamp-contact. Accessed on: 1 jan. 2024.

GOOGLE. **Choose the right edition for your institution**. [*S. l.*], 2023a. Available at: https://edu.google.com/workspace-for-education/editions/compare-editions/. Accessed on: 10 aug. 2023.

GOOGLE. **Cloud Data Processing Addendum (Customers)**. [*S. l.*], 2023c. Available at: https://cloud.google.com/terms/data-processing-addendum. Accessed on: 1 oct. 2023.

GOOGLE. **Compare Google Workspace editions**. [*S. l.*], 2023b. Available at: https://support.google.com/a/answer/6043385?hl=en&co=DASHER._Family%3DEducation. Accessed on: 10 aug. 2023.

GOOGLE. **Discover programs dedicated to teacher professional development and student engagement**. [*S. l.*], 2023c. Available at: https://edu.google.com/intl/ALL_be/for-educators/certification-programs/professional-expertise/?modal_active=none. Accessed on: 10 aug. 2023.

GOOGLE. **DPIA Resource Center - Introduction**. [*S. l.*], 2023d. Available at: https://cloud.google.com/privacy/data-protection-impact-assessment. Accessed on: 27 sep. 2023.

GOOGLE. **Find the best Chromebook for your institution**. [*S. l.*], 2023e. Available at: https://edu.google.com/intl/ALL_us/chromebooks/find-a-chromebook/. Accessed on: 21 aug. 2023.

GOOGLE. **Get Level 1 Teacher Certification**. [*S. l.*], 2023f. Available at: https://edu.google.com/for-educators/certification-programs/product-expertise/educator-level1/?modal_active=none. Accessed on: 10 aug. 2023.

GOOGLE. Google Announces Education News at Educause. **News from Google**, [*s. l.*], 10 oct. 2006a. Available at: http://googlepress.blogspot.com/2006/10/google-announces-education-news-at_10.html. Accessed on: 8 aug. 2023.

GOOGLE. **Google Apps**. [*S. l.*], 2006b. Available at: http://web.archive.org/web/20061208110748/https://www.google.com/a/. Accessed on: 8 aug. 2023.

GOOGLE. Google Introduces New Business Version of Popular Hosted Applications. **News from Google**, [*s. l.*], 22 feb. 2007. Available at: http://googlepress.blogspot.com/2007/02/google-introduces-new-business-version_22.html. Accessed on: 8 aug. 2023.

GOOGLE. Google Sets Its Sites on Google Apps. **News from Google**, [*s. l.*], 28 feb. 2008. Available at: http://googlepress.blogspot.com/2008/02/google-sets-its-sites-on-google-apps_28.html. Accessed on: 8 aug. 2023.

GOOGLE. **Google Workspace for Education Core and Additional services**. [*S. l.*], 2023g. Available at: https://support.google.com/a/answer/6356441?hl=en. Accessed on: 13 aug. 2023.

GOOGLE. Introducing Google Workspace and a new set of offerings to better meet your needs. **Google Workspace Updates**, [*s. l.*], 6 oct. 2020. Available at: https://workspaceupdates.googleblog.com/2020/10/introducing-google-workspace.html. Accessed on: 8 aug. 2023.

GOOGLE. **Join a community of passionate teachers to share, find inspiration and learn with them**. [*S. l.*], 2023h. Available at: https://edu.google.com/for-educators/communities/?modal_active=none. Accessed on: 10 aug. 2023.

GOOGLE. **Make learning more alive with Jamboard**. [*S. l.*], 2023i. Available at: https://edu.google.com/jamboard/. Accessed on: 21 aug. 2023.

GOOGLE. **Our approach to Search**. [*S. l.*], 2023j. Available at: https://www.google.com/search/howsearchworks/our-approach/. Accessed on: 14 aug. 2023.

GOOGLE. **Política de Privacidade**. [*S. l.*], 2023d. Available at: https://policies.google.com/privacy?hl=pt-BR. Accessed on: 1 oct. 2023.

GOOGLE. **Services Summary** . [*S. l.*], 2023k. Available at: https://workspace.google.com/intl/en/terms/user_features.html. Accessed on: 13 aug. 2023.

GOOGLE. **Termos de Serviço**. [*S. l.*], 2022. Available at: https://policies.google.com/terms?hl=pt-BR. Accessed on: 1 oct. 2023.

GOOGLE. **Termos de Serviço do Google Cloud Platform**. [*S. l.*], 2023e. Available at: https://cloud.google.com/terms?hl=pt-br. Accessed on: 1 oct. 2023.

GOOGLE. **Termos de Serviço do Google Workspace for Education**. [*S. l.*], 2023f. Available at: https://workspace.google.com/intl/pt-BR/terms/education_terms/. Accessed on: 1 oct. 2023.

GOOGLE. **Transform education with a project you care about as a Certified Innovator**. [*S. l.*], 2023l. Available at: https://edu.google.com/intl/ALL_be/for-educators/certification-programs/professional-expertise/certified-innovator/?modal_active=none. Accessed on: 10 aug. 2023.

GRABOW, Chip; ROSE, Lisa. The US has had 57 times as many school shootings as the other major industrialized nations combined. **CNN**, [*s. l.*], 21 mai 2018. Available at:

https://edition.cnn.com/2018/05/21/us/school-shooting-us-versus-world-trnd/index.html. Accessed on: 26 dec. 2023.

GRAND VIEW RESEARCH. **Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 - 2030**. [*S. l.: s. n.*], 2023. Available at: https://www.grandviewresearch.com/industry-analysis/education-technology-market. Accessed on: 12 nov. 2023.

GROHMANN, Rafael. No MTST, a soberania digital de que fala Morozov. **Outras Palavras**, [*s. l.*], 1 sep. 2023. Available at: https://outraspalavras.net/tecnologiaemdisputa/no-mtst-a-soberania-digital-de-que-fala-morozov/. Accessed on: 23 dec. 2023.

GRONDWETTELIJK HOF. Arrest nr. 26/2023 van 16 februari 2023. Rolnummers : 7494, 7505, 7526 en 7606. 2023. Available at: https://www.const-court.be/public/n/2023/2023-026n.pdf. Accessed on: 14 dec. 2023.

HALEY, Keltie. Sharenting and the (Potential) Right to Be Forgotten. **Indiana Law Journal**, [*s. l.*], v. 95, n. 3, p. 105–1020, 2020. Available at: https://www.theguardian.com/technology.

HANSON, Karl; LUNDY, Laura. Does Exactly What it Says on the Tin? A Critical Analysis and Alternative Conceptualisation of the So-called "General Principles" of the Convention on the Rights of the Child. **International Journal of Children's Rights**, [*s. l.*], v. 25, n. 2, p. 285–306, 2017.

HARTZOG, Woodrow. **Privacy's Blueprint: The Battle to Control the Design of New Technologies**. Cambridge: Harvard University Press, 2018-. ISSN 1744-2567.

HARWELL, Drew. Cheating-detection companies made millions during the pandemic. Now students are fighting back. **The Washington Post**, [*s. l.*], 12 nov. 2020. Available at: https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/. Accessed on: 28 mai 2023.

HASKINS, Caroline. Gaggle Knows Everything About Teens And Kids In School. **BuzzFeed.News**, [*s. l.*], 1 nov. 2019. Available at: https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education. Accessed on: 23 mai 2023.

HEIDEBRECHT, Sebastian. From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. **JCMS: Journal of Common Market Studies**, [*s. l.*], v. 62, n. 1, p. 205–223, 2024. https://doi.org/10.1111/jcms.13488.

HEIMANS, Stephen; SINGH, Parlo; KWOK, Henry. Pedagogic rights, public education and democracy. **European Educational Research Journal**, [*s. l.*], v. 21, n. 1, p. 71–82, 2022.

HELD, William B *et al.* A Material Lens on Coloniality in NLP. *In*: , 2023. **Anais [...]**. [*S. l.: s. n.*], 2023. Available at: https://arxiv.org/abs/2311.08391. Accessed on: 16 nov. 2023.

HENRIQUES, Isabela. **Direitos Fundamentais da Criança no Ambiente Digital: O dever de garantia da absoluta prioridade**. São Paulo: Thompson Reuters Brasil, 2023.

HENRIQUES, Isabella; MEIRA, Marina; HARTUNG, Pedro. A nova LGPD, o seu relevante artigo 14 e as práticas de mercado. *In*: LIMA, Stephane (org.). **Educação, dados e plataformas: análise descritiva dos termos de uso G Suite for Education e Microsoft 365**. São Paulo: Iniciativa Educação Aberta, 2020. p. 11–12. Available at: https://zenodo.org/records/4012539#.X1EOdpNKi-4. Accessed on: 3 nov. 2023.

HENRIQUES, Isabella; MEIRA, Marina; HARTUNG, Pedro. A proibição do directionamento de publicidade microssegmentada para crianças e adolescente e a abusividade do uso de dados pessoais para fins de exploração comercial infanto-juvenil. *In*: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Obliq; ITS Rio, 2021. p. 427–453. Available at: https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf. Accessed on: 3 nov. 2023.

HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2020.

HERLO, Bianca; ULLRICH, André; VLADOVA, Gergana. **Sustainable Digital Sovereignty: Interdependencies Between Sustainable Digitalization and Digital Sovereignty**. Berlin: [*s. n.*], 2023. Available at: Accessed on: 23 dec. 2023.

HEROLD, Benjamin. Google Under Fire for Data-Mining Student Email Messages. **Education Week**, [*s. l.*], 13 mar. 2014. Available at: https://www.edweek.org/policy-politics/google-under-fire-for-data-mining-student-email-messages/2014/03. Accessed on: 10 aug. 2023.

HEROLD, Benjamin. What Is Personalized Learning?. **EducationWeek**, [*s. l.*], 5 nov. 2019. Available at: https://www.edweek.org/technology/what-is-personalized-learning/2019/11. Accessed on: 9 mai 2023.

HESS, Abigail Johnson. Bill and Melinda Gates have spent billions trying to fix U.S. public education but say it's not having the impact they want. **CNCB make it**, [*s. l.*], 12 feb. 2020. Available at: https://www.cnbc.com/2020/02/12/bill-and-melinda-gates-say-education-philanthropy-is-not-having-impact.html. Accessed on: 2 jul. 2023.

HESSEL, Stefan. FAQ about telemetry and diagnostic data in Microsoft 365. **Reusch Law**, [*s. l.*], 17 sep. 2022. Available at: https://www.reuschlaw.de/en/news/faq-about-telemetry-and-diagnostic-data-in-microsoft-365/. Accessed on: 27 sep. 2023.

HIGH, Peter. How 174 Year Old Pearson Is Developing The Netflix Of Education. **Forbes**, [*s. l.*], 20 aug. 2018. Available at: https://www.forbes.com/sites/peterhigh/2018/08/20/how-174-year-old-pearson-is-developing-the-netflix-of-education/. Accessed on: 26 dec. 2023.

HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge?. *In*: HILDEBRANDT, M.; GUTWIRTH, S. (org.). **Profiling the European Citizen**. [*S. l.*]: Springer, 2008. p. 17–45. Available at: www.BioinformaticsWorld.info/feature.

HILDEBRANDT, Mireille. **Smart Technologies and the End(s) of Law**. [*S. l.*]: Edward Elgar, 2015.

HILLIS, Ken; PETIT, Michael; JARRETT, Kylie. **Google and the Culture of Search**. [*S. l.*]: Routledge, 2013.

HILLMAN, Velislava. **Edtech procurement matters: It needs a coherent solution, clear governance and market standards**. [*S. l.: s. n.*], 2022.

HILLMAN, Velislava *et al.* Global transformation, local choices: Navigating the impacts of Artificial Intelligence on education. *In*: 2022 ICT IN EDUCATION. SURVEY ON THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN BRAZILIAN SCHOOLS. [*S. l.: s. n.*], 2023. p. 263–275. Available at: https://cetic.br/media/docs/publicacoes/2/20231122132216/tic_educacao_2022_livro_completo.pdf. Accessed on: 11 dec. 2023.

HLOSTA, Martin *et al.* Predictive learning analytics in online education: A deeper understanding through explaining algorithmic errors. **Computers and Education: Artificial Intelligence**, [*s. l.*], v. 3, p. 100108, 2022. https://doi.org/10.1016/j.caeai.2022.100108.

HOF, Simone Van Der. I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World. **Wisconsin International Law Journal**, [*s. l.*], v. 32, n. 2, p. 409–445, 2017. Available at: http://unicef-irc.org/publications/pdf/evolving-eng.pdf.

HOF, Simone van der; LIEVENS, Eva. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. **Communications Law: The Journal of Computer, Media and Telecommunications Law**, [*s. l.*], v. 23, n. 1, p. 33–43, 2018. Available at: https://infolawcentre.blogs.sas.ac.uk/files/2018/03/Comms_Law_23.1.pdf. Accessed on: 16 jul. 2023.

HOGAN, Anna; THOMPSON, Greg. Introduction: the "publicness" of schooling. *In*: PRIVATISATION AND COMMERCIALISATION IN PUBLIC EDUCATION: HOW THE PUBLIC NATURE OF SCHOOLING IN CHANGING. [*S. l.*]: Routledge, 2021.

HOLMES, Wayne *et al.* **Artificial intelligence and education: a critical view through the lens of human rights, democracy and the rule of law**. Strasbourg: [*s. n.*], 2022. Available at: https://rm.coe.int/prems-092922-gbr-2517-ai-and-education-txt-16x24-web/1680a956e3. Accessed on: 9 oct. 2023.

HOLMES, Wayne *et al.* **Technology-enhanced Personalised Learning: Untangling the Evidence**. Stuttgart: [*s. n.*], 2018. Available at: https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2018-08/Study_Technology-enhanced%20Personalised%20Learning.pdf. Accessed on: 25 dec. 2023.

HOLMES, Wayne. **The Unintended Consequences of Artificial Intelligence**. [*S. l.: s. n.*], 2023. Available at: https://www.ei-ie.org/en/item/28115:the-unintended-consequences-of-artificial-intelligence-and-education. Accessed on: 21 oct. 2023.

HOLMES, Wayne; BIALIK, Maya; FADEL, Charles. **Artificial Intelligence in Education. Promises and Implications for Teaching and Learning**. Boston: [*s. n.*], 2019. Available at: https://curriculumredesign.org/our-work/artificial-intelligence-in-education/. Accessed on: 12 oct. 2023.

HOLONIQ EDUCATION INTELLIGENCE UNIT. **Global EdTech market to reach $404B by 2025 - 16.3% CAGR**. [*S. l.*], 2020. Available at: https://www.holoniq.com/notes/global-education-technology-market-to-reach-404b-by-2025. Accessed on: 12 nov. 2023.

HOOPER, L.; LIVINGSTONE, S.; POTHONG, K. **Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo**. [*S. l.: s. n.*], 2022. Available at: https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf. Accessed on: 27 oct. 2022.

HUMAN RIGHTS WATCH. **"How dare they peep into my private life?": Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic**. [*S. l.: s. n.*], 2022.

ICO. **Age appropriate design: a code of practice for online services**. [*S. l.*], 2020. Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf. Accessed on: 9 jul. 2023.

ICO. **How to use AI and personal data appropriately and lawfully**. [*S. l.*], 2022. Available at: https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf . Accessed on: 19 jul. 2023.

ICO. **The Children's code and education technologies (edtech)**. [*S. l.*], 2023a. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/. Accessed on: 19 jul. 2023.

ICO. **The Children's code and education technologies (edtech)**. [*S. l.*], 2023b. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/. Accessed on: 17 jul. 2023.

IMY. **Beslut efter tillsyn enligt dataskyddsförordningen - Barn- och utbildningsnämnden i Östersunds kommun**. [*S. l.: s. n.*], 2023a. Available at: https://www.imy.se/globalassets/dokument/beslut/2023/beslut-om-tillsyn-barn-och-utbildningsforvaltningen-ostersunds-kommun.pdf. Accessed on: 4 dec. 2023.

IMY. **Sanktionsavgift mot kommun som inte bedömt konsekvenser innan Google Workspace infördes**. [*S. l.*], 2023b. Available at: https://www.imy.se/nyheter/sanktionsavgift-mot-kommun-som-inte-bedomt-konsekvenser-innan-google-workspace-infordes/. Accessed on: 4 dec. 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Achieving universal and meaningful digital connectivity. Setting a baseline and targets for 2030**. [*S. l.: s. n.*], 2022.

Available at: https://www.itu.int/itu-d/meetings/statistics/wp-content/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf. Accessed on: 11 dec. 2023.

ISAAC, Mike. Facebook Renames Itself Meta. **The New York Times**, [*s. l.*], 28 oct. 2021. Available at: https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html. Accessed on: 18 mar. 2023.

JARKE, Juliane; MACGILCHRIST, Felicitas. Dashboard stories: How narratives told by predictive analytics reconfigure roles, risk and sociality in education. **Big Data and Society**, [*s. l.*], v. 8, n. 1, 2021.

JOHNSTON, Scott. Introducing Google Drive, the newest member of Google Apps. **Google Cloud Official Blog**, [*s. l.*], 24 apr. 2012. Available at: https://cloud.googleblog.com/2012/04/introducing-google-drive-newest-member.html. Accessed on: 8 aug. 2023.

KEIERLEBER, Mark. Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'. **The 74**, [*s. l.*], 12 oct. 2021. Available at: https://www.the74million.org/article/gaggle-surveillance-minnesapolis-families-not-smart-ai-monitoring/. Accessed on 15 jan. 2024.

KERSSENS, Niels K; DIJCK, José van. Governed by Edtech? Valuing Pedagogical Autonomy in a Platform Society. **Harvard Educational Review**, [*s. l.*], v. 92, n. 2, p. 284–303, 2022.

KIECZA, Daniel. Practice sets: a more personal path to learning. **Google - The Keyword**, [*s. l.*], 16 mar. 2022. Available at: https://blog.google/outreach-initiatives/education/introducing-practice-sets/. Accessed on: 15 jan. 2024.

KIM, Nancy S. **Consentability: Consent and Its Limits**. 1. ed. Cambridge: Cambridge University Press, 2019-. ISSN 1556-5068.

KING, Pippa; PERSOON, Jen. **The State of Biometrics 2022: A Review of Policy and Practice in UK Education**. [*S. l.: s. n.*], 2022. Available at: https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf. Accessed on: 27 jul. 2023.

KITCHIN, Rob. **The Data Revolution: Big Data, Open Data, Data Infrascturctures & their Consequences**. [*S. l.*]: SAGE Publications, 2014.

KLEEMAN, David. As Kids Kickstart The Metaverse, Is Public Service Media Ready?. **The Children's Media Foundation**, [*s. l.*], mar. 2021. Available at: https://www.thechildrensmediafoundation.org/public-service-media-report/articles/as-kids-kickstart-the-metaverse-is-public-service-media-ready. Accessed on: 18 mar. 2023.

KNOX, Jeremy. Artificial intelligence and education in China. **Learning, Media and Technology**, [*s. l.*], v. 45, n. 3, p. 298–311, 2020.

KOHL, Uta. The Pixelated Person: Humanity in the Grip of Algorithmic Personalisation. *In*: DATA-DRIVEN PERSONALISATION IN MARKETS, POLITICS AND LAW. [*S. l.*]: Cambridge University Press, 2021. p. 3–36.

KOHN, Alfie. Four Reasons to Worry About "Personalized Learning". **Psychology Today**, [*s. l.*], 24 feb. 2015. Available at: https://www.psychologytoday.com/intl/blog/the-homework-myth/201502/four-reasons-worry-about-personalized-learning. Accessed on: 14 mai 2023.

KOMLJENOVIC, Janja *et al.* When public policy 'fails' and venture capital 'saves' education: Edtech investors as economic and political actors. **Globalisation, Societies and Education**, [*s. l.*], 2023.

KOSTA, Eleni. Article 8. Conditions applicable to child's consent in relation to information society services. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation (GDPR): A Commentary**. [*S. l.*]: Oxford Academic Press, 2020. p. 355–364.

KOTSCHY, Waltraut. Article 6. Lawfulness of processing. *In*: KUNER, Christopherc *et al.* (org.). **The EU General Data Protection Regulation (GDPR): A Commentary**. [*S. l.*]: Oxford University Press, 2020. p. 321–344.

KRANENBORG, Herke. Article 8. *In*: PEERS, Steve *et al.* (org.). **The EU Charter of Fundamental Rights: A Commentary**. 2. ed. [*S. l.*]: Hart Publishing, 2021. p. 231–289.

KRUTKA, Daniel G; SMITS, Ryan M; WILLHELM, Troy A. Don't Be Evil: Should We Use Google in Schools? **TechTrends**, [*s. l.*], v. 65, p. 421–431, 2021.

KUCIRKOVA, Natalia. OPINION: Some warning flags for those embracing personalized learning powered by education technology. **The Hechinger Report**, [*s. l.*], 14 oct. 2021. Available at: https://hechingerreport.org/opinion-some-warning-flags-for-those-embracing-personalized-learning-powered-by-education-technology/. Accessed on: 16 mar. 2023.

KUCIRKOVA, Natalia. The promise and pitfalls of personalised learning with new EdTech. *In*: LIVINGSTONE, Sonia; POTHONG, Kruakae (org.). **Education Data Futures: Critical, Regulatory and Practical Reflections**. [*S. l.*]: Digital Futures Commission, 5Rights Foundation, 2022. p. 221–229. Available at: https://cms.educationdatafutures.digitalfuturescommission.org.uk/wp-content/uploads/2022/11/Education-Data-Futures.pdf. Accessed on: 1 aug. 2023.

KUCIRKOVA, Natalia; BROD, Garvin; GAAB, Nadine. Applying the science of learning to EdTech evidence evaluations using the EdTech Evidence Evaluation Routine (EVER). **npj Science of Learning**, [*s. l.*], v. 8, n. 1, p. 35, 2023. Available at: https://www.nature.com/articles/s41539-023-00186-7.

KÜHNE, Thomas. What is a Model?. *In*: , 2005, Wadern. **Dagstuhl Seminar Proceedings**. Wadern: Schloss Dagstuhl Leibniz Zentrum für Informatik, 2005. p. 1–10. Available at: https://drops.dagstuhl.de/volltexte/2005/23/pdf/04101.KuehneThomas1.Paper.pdf. Accessed on: 15 oct. 2023.

LA CHAMBRE DES REPRÉSENTANTS. **Question et réponse écrite n° 55-473: Accord de coopération entre l'APD et la VTC.** [*S. l.*], 2023. Available at: https://www.stradalex.com/nl/sl_src_publ_div_be_chambre/document/QRcrb_55-b107-1263-0473-2022202319113. Accessed on: 14 dec. 2023.

LAET, Tinne De. Een kritisch constructief perspectief op Learning Analytics. **Tijdschrift voor Hoger Onderwijs**, [*s. l.*], v. 41, n. 1, p. 48–60, 2023.

LAET, Tinne De *et al.* Explainable Learning Analytics: challenges and opportunities. *In*: , 2020. **Companion Proceedings of the 10th International Conference on Learning Analytics & Knowledge LAK20**. [*S. l.*]: Society for Learning Analytics Research (SoLAR), 2020. p. 500–510. Available at: https://www.solaresearch.org/wp-content/uploads/2020/06/LAK20_Companion_Proceedings.pdf. Accessed on: 3 aug. 2023.

LAET, Tinne de *et al.* **"Learning Analytics" in het Vlaams Hoger Onderwijs**. [*S. l.: s. n.*], 2018. Available at: https://kvab.be/sites/default/rest/blobs/2122/tw_learninganalytics.pdf. Accessed on: 18 jan. 2023.

LAI, Mei Kuin; SCHILDKAMP, Kim. Data-based Decision: an overview. *In*: SCHILDKAMP, Kim; KUIN LAI, Mei; EARL, Lorna (org.). **Data-based Decision Making in Education: Challenges and Opportunities**. [*S. l.*]: Springer, 2013. v. 17, p. 9–21. Available at: http://www.springer.com/series/6543.

LAIRD, Elizabeth; DWYER, Madeliene; GRANT-CHAPMAN, Hugh. **Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI**. [*S. l.: s. n.*], 2023. Available at: https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/. Accessed on: 30 nov. 2023.

LAIRD, Elizabeth; QUAY-DE LA VALLEE, Hannah. **Protecting privacy while supporting students who change schools**. [*S. l.: s. n.*], 2019.

LAMONT, Ruth. Article 24. *In*: PEERS, Steve *et al.* (org.). **The EU Charter of Fundamental Rights: A Commentary**. 2. ed. [*S. l.*]: Hart Publishing, 2021. p. 693–724.

LANGREO, Lauraine. Google Executive: AI Could 'Transform' School Into a 'Personal Learning Experience'. **EducationWeek**, [*s. l.*], 06 jul. 2023. Available at: https://www.edweek.org/technology/google-executive-ai-could-transform-school-into-a-personal-learning-experience/2023/07. Accessed on: 15 jan. 2024.

LANSDOWN, Gerison. **The evolving capacities of the child**. [*S. l.*]: Save the Children, 2005. Available at: https://www.unicef-irc.org/publications/384-the-evolving-capacities-of-the-child.html. Accessed on: 24 jun. 2023.

LAVAL, Christian. **A escola não é uma empresa: o neoliberalismo em ataque ao ensino público**. [*S. l.*]: Boitempo, 2019.

LAWN, Martin. Voyages of measurement in education in the twentieth century: Experts, tools and centres. **European Educational Research Journal**, [*s. l.*], v. 12, n. 1, p. 108–119, 2013.

LAWSON, R. Frederic *et al.* **Education**. *In*: ENCYCLOPAEDIA BRITANNICA. [*S. l.: s. n.*], 2023. Available at: https://www.britannica.com/topic/education. Accessed on: 19 mar. 2023.

LAZARE, Melanie. A peek at what's next for Google Classroom. **Google - The Keyword**, [*s. l.*], 17 feb. 2021a. Available at: https://blog.google/outreach-initiatives/education/classroom-roadmap/. Accessed on: 8 aug. 2023.

LAZARE, Melanie. **Learning with Google 2021**. [*S. l.*], 2021b. Available at: https://youtu.be/oGEy4PfcdZ8?t=2449. Accessed on: 8 aug. 2023.

LEFÈVRE, Flávia. Soberania e Segurança negligenciadas. **Flávia Lefèvre: Liberdade e direitos na Internet e nas telecomunicações**, [*s. l.*], 11 mar. 2023. Available at: https://flavialefevre.com.br/pt/soberania-e-seguranca-negligenciadas. Accessed on: 23 dec. 2023.

LEI DE DIRETRIZES E BASES DA EDUCAÇÃO NACIONAL. Brazil: 20 dec. 1996. Available at: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Accessed on: 17 nov. 2023.

LEINONEN, T. **(Critical) history of ICT in education – and where we are heading?**. [*S. l.*], [*s. d.*]. Available at: https://teemuleinonen.fi/2005/06/23/critical-history-of-ict-in-education-and-where-we-are-heading/. Accessed on: 11 mar. 2023.

LEMAY, David J.; BAEK, Clare; DOLECK, Tenzin. Comparison of learning analytics and educational data mining: A topic modeling approach. **Computers and Education: Artificial Intelligence**, [*s. l.*], v. 2, 2021.

LEME, Valdir. Cresça com o Google 2019: Transformando o Brasil a partir da capacitação digital. **O Blog do Google Brasil**, [*s. l.*], 25 feb. 2019. Available at: https://brasil.googleblog.com/2019/02/cresca-com-o-google-2019.html. Accessed on: 2 nov. 2023.

LEMOS, Ronaldo *et al.* **Translation of the Brazilian General Data Protection Law**. [*S. l.: s. n.*], 2020. Available at: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. Accessed on: 17 nov. 2023.

LEVIN, Robert A.; HINES, Laurie Moses. Educational Television, Fred Rogers, and the History of Education. **History of Education Quarterly**, [*s. l.*], v. 43, n. 2, p. 262–275, 2003. Available at: https://www.jstor.org/stable/3218313. Accessed on: 16 mai 2023.

LIEVENS, Eva *et al.* Children's Rights and Digital Technologies. *In*: KILKELLY, Ursula; LIEFAARD, Ton (org.). **International Human Rights of Children**. Singapore: Springer, 2019. p. 487–513.

LIEVENS, Eva. Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights. **Nordic Journal of Human Rights**, [*s. l.*], v. 39, n. 2, p. 128–145, 2021.

LIEVENS, Eva. Wanted: evidence base to underpin a children's rights-based implementation of the GDPR. **Media@LSE**, [*s. l.*], 14 oct. 2016. Available at:

https://blogs.lse.ac.uk/medialse/2016/11/10/wanted-evidence-base-to-underpin-a-childrens-rights-based-implementation-of-the-gdpr/. Accessed on: 14 jul. 2023.

LIEVENS, Eva; VERDOODT, Valerie. Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. **Computer Law and Security Review**, [*s. l.*], v. 34, n. 2, p. 269–278, 2018.

LIM, Weng Marc *et al.* Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators. **International Journal of Management Education**, [*s. l.*], v. 21, n. 2, 2023.

LINDH, Maria; NOLIN, Jan. Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. **European Educational Research Journal**, [*s. l.*], v. 15, n. 6, p. 644–663, 2016.

LIPWORTH, Laurence. **Differences between personalization, customization & individualization**. [*S. l.*], 2015. Available at: https://www.linkedin.com/pulse/differences-between-personalization-customization-laurence-lipworth/. Accessed on: 25 apr. 2023.

LIVINGSTONE, Sonia; LIEVENS, Eva; CARR, John. **Handbook for policy makers on the rights of the child in the digital environment**. [*S. l.: s. n.*], 2020. Available at: https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8. Accessed on: 26 jun. 2023.

LIVINGSTONE, Sonia; ÓLAFSSON, Kjartan. **Children's commercial media literacy: new evidence relevant to UK policy decisions regarding the GDPR**. [*S. l.: s. n.*], 2017. Available at: https://blogs.lse.ac.uk/medialse/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/. Accessed on: 14 jul. 2023.

LIVINGSTONE, Sonia; O'NEILL, Brian. Children's Rights Online: Challenges, Dilemmas and Emerging Directions. *In*: HOF, Simone van der; BERG, Bibi van den; SCHERMER, Bart (org.). **Minding Minors Wandering the Web: Regulating Online Child Safety**. [*S. l.*]: Springer, 2014. p. 19–38.

LIVINGSTONE, Sonia ; STOILOVA, Mariya. **The 4Cs: Classifying Online Risk to Children**. Hamburg: [*s. n.*], 2021. Available at: www.ssoar.infoEvidence.https://doi.org/10.21241/ssoar.71817. .

LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. **Children's data and privacy online. Growing up in a digital age: An evidence review**. [*S. l.: s. n.*], 2018. Available at: https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf. Accessed on: 25 jul. 2023.

LOCATELLI, Rita. **Education as a public and common good: reframing the governance of education in a changing context**. [*S. l.: s. n.*], 2018. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000261614. Accessed on: 1 jul. 2023.

LONGPRE, Shayne *et al.* The Data Provenance Initiative: A Large Scale Audit of Dataset Licensing & Attribution in AI. [*s. l.*], 2023. Available at: https://arxiv.org/abs/2310.16787v3. Accessed on: 16 nov. 2023.

LOPES, Gabriel Henrique de Oliveira. **Um olhar sobre as big techs na educação pública: o caso Google for Education na rede de educação básica paulista**. 2023. Dissertação - Universidade Estadual Paulista (UNESP), Marília, 2023. Available at: https://repositorio.unesp.br/server/api/core/bitstreams/78e16f8c-a2b8-42bb-9c41-149fd96430a6/content. Accessed on: 16 feb. 2024.

LUBIENSKI, Christopher. What "good" is schooling? The new edu-philanthropies and education reform. *In*: HOGAN ANNA; THOMPSON, Greg (org.). **Privatisation and Commercialisation in Public Education: How the Public Nature of Schooling in Changing**. [*S. l.*]: Routledge, 2021.

LUNA, Florencia. Elucidating the Concept of Vulnerability: Layers Not Labels. **International Journal of Feminist Approaches to Bioethics**, [*s. l.*], v. 2, n. 1, p. 121–139, 2009. Available at: https://www.jstor.org/stable/40339200.

LUNDIE, David; ZWITTER, Andrej; GHOSH, Dipayan. Corporatized education and State sovereignty. **Brookings**, [*s. l.*], 31 jan. 2022. Available at: https://www.brookings.edu/articles/corporatized-education-and-state-sovereignty/. Accessed on: 1 jul. 2023.

LUNDY, Laura; BYRNE, Bronagh. The four general principles of the United Nations Convention on the Rights of the Child: the potential value of the approach in other areas of human rights law. *In*: BREMS, Eva; DESMET ELLEN; VANDENHOLE, Wouter (org.). **Children's Rights Law in the Global Human Rights Landscape: Isolation, Inspiration, Integration?** [*S. l.*]: Routledge, 2017. p. 52–70.

LUNDY, Laura; TOBIN, John. Article 29. The Aims of Education. *In*: TOBIN, John (org.). **The UN Convention on the Rights of the Child**. Oxford: Oxford University Press, 2019.

LUPTON, Deborah; WILLIAMSON, Ben. The datafied child: The dataveillance of children and implications for their rights. **New Media and Society**, [*s. l.*], v. 19, n. 5, p. 780–794, 2017.

MACENAITE, Milda. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. **New Media and Society**, [*s. l.*], v. 19, n. 5, p. 765–779, 2017.

MACENAITE, Milda; KOSTA, Eleni. Consent for processing children's personal data in the EU: following in US footsteps? **Information and Communications Technology Law**, [*s. l.*], v. 26, n. 2, p. 146–197, 2017.

MADDOX, Bryan. **The uses of process data in large-scale educational assessments - OECD Education Working Paper No. 286**. [*S. l.: s. n.*], 2023. Available at: https://dx.doi.org/10.1787/5d9009ff-en. .

MADIEGA, Tambiama. **Artificial Intelligence Act**. [*S. l.: s. n.*], 2023. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf. Accessed on: 21 oct. 2023.

MAGALHÃES, João Carlos; COULDRY, Nick. Giving by Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good. **International Journal of Communication**, [*s. l.*], v. 15, p. 343–362, 2021. Available at: https://ijoc.org/index.php/ijoc/article/view/15995/3322. Accessed on: 30 jun. 2023.

MAGID, Larry. Google Classroom Offers Assignment Center for Students and Teachers. **Forbes**, [*s. l.*], 6 mai 2014. Available at: https://www.forbes.com/sites/larrymagid/2014/05/06/google-classroom-offers-control-center-for-students-and-teachers/. Accessed on: 8 aug. 2023.

MALGIERI, Gianclaudio; NIKLAS, Jędrzej. Vulnerable data subjects. **Computer Law and Security Review**, [*s. l.*], v. 37, 2020.

MARRAFON, Marco Aurélio; FERNANDES, Elora Raad. A, B, C, Google: Riscos ao Direito Fundamental à Proteção de Dados de Crianças e Adolescentes no G Suite for Education. **Revista Direito Público**, [*s. l.*], v. 17, n. 95, p. 202–229, 2020.

MARSH, Julie A; PANE, John F; HAMILTON, Laura S. **Making Sense of Data-Driven Decision Making in Education: Evidence from Recent RAND Research**. [*S. l.: s. n.*], 2006. Available at: https://www.rand.org/pubs/occasional_papers/OP170.html. Accessed on: 18 mai 2023.

MASCHERONI, Giovanna. Datafied childhoods: Contextualising datafication in everyday life. **Current Sociology**, [*s. l.*], v. 68, n. 6, p. 798–813, 2020. https://doi.org/10.1177/0011392118807534

MASSÉ, Estelle. **Four Years Under the EU GDPR: How to Fix its Enforcement**. [*S. l.: s. n.*], 2022. Available at: https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf. Accessed on: 29 sep. 2023.

MATSUMI, Hideyuki; SOLOVE, Daniel J. **The Prediction Society: AI and the Problems of Forecasting the Future**. [*S. l.: s. n.*], 2024. http://dx.doi.org/10.2139/ssrn.4453869.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: A Revolution that will transform how we live, work and think**. E-booked. [*S. l.*]: Houghton Mifflin Harcourt Publishing, 2013.

MAZZUCATO, Mariana. **Governing Missions in the European Union**. [*S. l.: s. n.*], 2019. Available at: https://www.kowi.de/de/Portaldata/2/Resources/Horizon2020/mazzucato_report_2019.pdf. Accessed on: 27 sep. 2023.

MAZZUCATO, Mariana. **Mission Economy: A Moonshot Guide to Changing Capitalism**. [*S. l.*]: Allen Lane, an imprint of Penguin Books, 2021.

MAZZUCATO, Mariana. **Mission-oriented public procurement: international examples**. [*S. l.: s. n.*], 2020. Available at: https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/final_mission-oriented_public_procurement_international_examples.pdf. Accessed on: 27 sep. 2023.

MAZZUCATO, Mariana; COLLINGTON, Rosie. **The Big Con: How the Consulting Industry Weakens Our Businesses, Infantilizes Our Governments, and Warps Our Economies**. New York: Penguin Press, 2023.

MCGREGOR, Sean. **Incident 43: Racist AI behaviour is not a new problem**. [*S. l.*], [*s. d.*]. Available at: https://incidentdatabase.ai/cite/43/. Accessed on: 18 oct. 2023.

MCMULLAN, Scott. More great apps for Google Apps. **Google Cloud Official Blog**, [*s. l.*], 9 mar. 2010. Available at: https://cloud.googleblog.com/2010/03/more-great-apps-for-google-apps.html. Accessed on: 8 aug. 2023.

MEANS, Alexander J. Platform learning and on-demand labor: sociotechnical projections on the future of education and work. **Learning, Media and Technology**, [*s. l.*], v. 43, n. 3, p. 326–338, 2018.

MEC. **Define critérios e procedimentos para a produção, recepção, avaliação e distribuição de recursos educacionais abertos ou gratuitos voltados para a educação básica em programas e plataformas oficiais do Ministério da Educação**. 16 mai 2018. Available at: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/14729210/do1-2018-05-17-portaria-n-451-de-16-de-maio-de-2018-14729206. Accessed on: 17 nov. 2023.

MEJIAS, Ulises A.; COULDRY, Nick. Datafication. **Internet Policy Review**, [*s. l.*], v. 8, n. 4, 2019.

MENDONÇA, Júlia; RIELLI, Mariana. A LGPD no Congresso após 4 anos de promulgação e 2 anos de vigência. **Jota**, [*s. l.*], 7 sep. 2022. Available at: https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-no-congresso-apos-4-anos-de-promulgacao-e-2-anos-de-vigencia-07092022. Accessed on: 5 oct. 2023.

MENEZES, Joyceane Bezerra de; RODRIGUES, Francisco Luciano Lima; BODIN DE MORAES, Maria Celina. A capacidade civil e o sistema de apoios no Brasil. **civilistica.com**, [*s. l.*], v. 10, n. 1, 2021. Available at: https://civilistica.emnuvens.com.br/redc/article/view/705. Accessed on: 4 oct. 2023.

MEYER, Marisa *et al.* How educational are "educational" apps for young children? App store content analysis using the Four Pillars of Learning framework. **Journal of Children and Media**, [*s. l.*], v. 15, n. 4, p. 526–548, 2021.

MEYER, Anneke. The moral rhetoric of childhood. **Childhood**, [*s. l.*], v. 14, n. 1, p. 85–104, 2007.

MIAO, Fengchun *et al.* **AI and education: guidance for policy-makers**. [*S. l.*]: UNESCO, 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000376709. Accessed on: 29 jul. 2023.

MILAN, Stefania; TRERÉ, Emiliano. Big Data from the South(s): Beyond Data Universalism. **Television and New Media**, [*s. l.*], v. 20, n. 4, p. 319–335, 2019.

MILKAITE, Ingrida. **A children's rights perspective on privacy and data protection in the digital age: A critical and forward-looking analysis of the EU General Data Protection Regulation and its implementation with respect to children and youth**. 2021. - Ghent University. Faculty of Law and Criminology, Ghent, 2021. Available at: http://hdl.handle.net/1854/LU-8714018. Accessed on: 26 jun. 2023.

MILKAITE, Ingrida; LIEVENS, Eva. Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. **Journal of Children and Media**, [*s. l.*], v. 14, n. 1, p. 5–21, 2020.

MINISTERIE VAN ONDERWIJS, Cultuur en Wetenschap. **Stand van zaken DPIA Google Workspace for Education**. [*S. l.: s. n.*], 2023. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2023/04/20/stand-van-zaken-dpia-google-workspace-for-education. Accessed on: 27 sep. 2023.

MINISTÉRIO DA CIÊNCIA, Tecnologia, Inovações e Comunicações. **Estratégia Brasileira para a Transformação Digital. E-Digital**. Brazil: 2018. Available at: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf. Accessed on: 17 nov. 2023.

MINISTÉRIO DA TRANSPARÊNCIA, Fiscalização e Controladoria-Geral da União. **3o Plano de Ação Nacional**. [*S. l.: s. n.*], 2016. Available at: https://www.gov.br/cgu/pt-br/governo-aberto/noticias/2017/3o-plano-de-acao-nacional-na-parceria-para-governo-aberto/plano_port_web-3.pdf/@@download/file/plano_port_web-3.pdf. Accessed on: 17 nov. 2023.

MINISTRY OF EDUCATION, Culture and Science. **Re: Advice from the Dutch Data Protection Authority on Google G Suite for Education**. [*S. l.: s. n.*], 2021. Available at: https://dataethics.eu/wp-content/uploads/2021/06/Advies_Autoriteit_Persoonsgegevens_inzake_Google_G_Suite_for_Education-_EN-1.pdf. Accessed on: 27 sep. 2023.

MITCHELL, Clark. Students of color are getting flagged to their teachers because testing software can't see them. **The Verge**, [*s. l.*], 9 apr. 2021. Available at: https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning. Accessed on: 18 oct. 2023.

MITTELSTADT, Brent Daniel. From Individual to Group Privacy in Big Data Analytics. **Philosophy & technology**, Dordrecht, v. 30, n. 4, p. 475–494, 2017. https://doi.org/10.1007/s13347-017-0253-7.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. **Big Data & Society**, v. 3, n. 2, p. 1-21, 2016. https://doi.org/10.1177/2053951716679679.

MOHAMED, Shakir; PNG, Marie Therese; ISAAC, William. Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence. **Philosophy and Technology**, [*s. l.*], n. 405, p. 1–28, 2020.

MOLENAAR, Inge. Personalisation of learning: Towards hybrid human-AI learning technologies. *In*: OECD DIGITAL EDUCATION OUTLOOK 2021 PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS. [*S. l.*]: OECD, 2021. p. 57–77.

MONDRAGON RUIZ, Sofia. **The Effects of Childhood Nostalgia on Brand Loyalty**. 2021. - University of Kent, [*s. l.*], 2021.

MOSCO, Vincent. **Becoming Digital: Toward a Post-Internet Society**. [*S. l.*]: Emerald Publishing, 2017.

MOWBRAY, Jacqueline. Is there a right to public education?. *In*: ADAMSON, Frank *et al.* (org.). **Realizing the Abidjan Principles on the Right to Education**. [*S. l.*]: Edward Elgar Publishing, 2021.

MRTEE. Beschluss des OVG NRW zum Google Workspace for Education Fall veröffentlicht. **Datenschutz – Schule – News**, [*s. l.*], 26 jul. 2023a. Available at: https://news.datenschutz-schule.info/2023/07/26/beschluss-des-ovg-nrw-zum-google-workspace-for-education-fall-veroeffentlicht/. Accessed on: 27 sep. 2023.

MRTEE. **Dortmunder Gymnasium erhält Weisung der Bezirksregierung, die Nutzung von Google Workspace for Education einzustellen**. [*S. l.*], 2023b. Available at: https://news.datenschutz-schule.info/2023/03/24/dortmunder-gymnasium-erhaelt-weisung-der-bezirksregierung-die-nutzung-von-google-workspace-for-education-einzustellen/. Accessed on: 27 sep. 2023.

MUKHERJEE, S.,; POTHONG, K.,; LIVINGSTONE, S. **Child Rights Impact Assessment: A tool to realise children's rights in the digital environment**. London: [*s. n.*], 2021.

MUMFORD, Densua. Data colonialism: compelling and useful, but whither epistemes? **Information Communication and Society**, [*s. l.*], v. 25, n. 10, p. 1511–1516, 2022.

MURAILLE, Marcel. **From emergency remote learning to a new digital education action plan: an EU attempt to mainstream equality into education**. [*S. l.: s. n.*], 2020. Available at: https://www.egmontinstitute.be/from-emergency-remote-learning-to-a-new-digital-education-action-plan/. Accessed on: 4 nov. 2023.

NAS, Sjoera. Google mitigates 8 high privacy risks for Workspace for Education. [*s. l.*], 9 aug. 2021. Available at: https://www.privacycompany.eu/blogpost-en/google-mitigates-8-high-privacy-risks-for-workspace-for-education. Accessed on: 27 sep. 2023.

NAS, Sjoera; TERRA, Floor. **DPIA on the use of Google G Suite (Enterprise) for Education. For the University of Groningen and the Amsterdam University of Applied Sciences**. [*S. l.: s. n.*], 2021. Available at: https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf. Accessed on: 27 sep. 2023.

NAS, Sjoera; TERRA, Floor. **Update DPIA report Google Workspace for Education 2 August 2021**. [*S. l.: s. n.*], 2021. Available at: https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf. Accessed on: 27 sep. 2023.

NAS, Sjoera; TERRA, Floor. **Verification report Google remediation measures Workspace for Education. For SURF and SIVON**. [*S. l.: s. n.*], 2023. Available at: https://sivon.nl/wp-content/uploads/2023/07/20230724-clean-Workspace-for-Education.pdf. Accessed on: 27 sep. 2023.

NASCIMENTO, Houldine. Governo faz parceria com Google para ferramentas educacionais. **Poder 360**, [*s. l.*], 20 jun. 2022. Available at: https://www.poder360.com.br/governo/governo-faz-parceria-com-google-para-ferramentas-educacionais. Acesso em 11 dec. 2023.

NATIONS UNIES. **Chapitre IV Droits de L'homme. 11. Convention relative aux droits de l'enfant. New York, 20 novembre 1989**. [*S. l.*], 2023. Available at: https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4. Accessed on: 5 jul. 2023.

NEGRI, Sérgio Marcos Carvalho de Ávila. Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. **Frontiers**, [*s. l.*], v. 8, p. 1–10, 2021.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Decisões automatizadas e a proteção de crianças e adolescentes. *In*: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. [*S. l.*]: Obliq; ITS Rio, 2021.p. 107–137. Available at: https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf. Accessed on: 28 oct. 2023.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora. Portabilidade e proteção de dados pessoais: tensões entre pessoa e mercado. **civilistica.com**, [*s. l.*], v. 10, n. 1, p. 1–39, 2021. Available at: https://civilistica.emnuvens.com.br/redc/article/view/532/527. Accessed on: 28 oct. 2023.

NICHOLS, T Philip; GARCIA, Antero. Platform Studies in Education. **Harvard Educational Review**, [*s. l.*], v. 92, n. 2, p. 209–230, 2022. Available at: http://meridian.allenpress.com/her/article-pdf/92/2/209/3117145/i1943-5045-92-2-209.pdf.

NIEMCZYK, Jerzy; TRZASKA, Rafał. Klasyfikacja modeli biznesowych w Industry 4.0 [Business models classification in Industry 4.0]. *In*: URBANEK, Grzegorz; GREGORCZYK, Sylwester (org.). **Zarządzanie strategiczne w dobie cyfrowej gospodarki sieciowej [Strategic management in the digital age of the networked economy]**. [*S. l.*]: Wydawnictwo Uniwersytetu Łódzkiego, 2020.

NIESTADT, Maria. **The new European strategy for a better internet for kids (BIK+)**. [*S. l.: s. n.*], 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733663/EPRS_BRI(2022)733663_EN.pdf. Accessed on: 4 nov. 2023.

NOLAN, Jason; RAYNES-GOLDIE, Kate; MCBRIDE, Melanie. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. **Journal of Childhood Studies**, [*s. l.*], v. 36, n. 2, p. 24–32, 2011.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Educação em um cenário de plataformização e de economia de dados: parcerias e assimetrias**. São Paulo: [*s. n.*], 2022. Available at: https://cgi.br/media/docs/publicacoes/1/20221129114057/educacao_em_um_cenario_de_plataformiza%C3%A7ao_e_de_economia_de_dados_parcerias_e_assimetrias.pdf. Accessed on: 31 oct. 2023.

NÚCLEO DE TECNOLOGIA DO MTST. **Homeless Worker Movement in Brazil and the struggle for digital sovereigtny**. [*S. l.: s. n.*], 2023. Available at: https://nucleodetecnologia.com.br/docs/Cartilha-MTSTec-ENG.pdf. Accessed on: 23 dec. 2023.

NYST, Carly; GOROSTIAGA, Amaya; GEARY, Patrick. **Industrial Toolkit. Children's Online Privacy and Freedom of Expression**. [*S. l.: s. n.*], 2018. Available at: https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf. Accessed on: 3 aug. 2023.

OBSERVATÓRIO EDUCAÇÃO VIGIADA. **Aboct.** [*S. l.*], [*s. d.*]. Available at: https://educacaovigiada.org.br/en/aboct.html. Accessed on: 1 nov. 2023.

OECD. **OECD Digital Education Outlook 2021. Pushing the frontiers with AI, blockchain, and robots**. Paris: OECD Publishing, 2021. (OECD Digital Education Outlook). Available at: https://www.oecd-ilibrary.org/education/oecd-digital-education-outlook-2021_589b283f-en. Accessed on: 30 jul. 2023.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy**. New York: Crown Publishers, 2016.

O'REILLY, Tim; STRAUSS, Ilan; MAZZUCATO, Mariana. **Algorithmic Attention Rents: A theory of digital platform market power**. [*S. l.: s. n.*], 2023. Available at: https://www.ucl.ac.uk/bartlett/public-purpose/wp2023-10. .

PALMER, Jason. Why I'm Still Bullish About the State of Edtech. **EdSurge**, [*s. l.*], 1 apr. 2022. Available at: https://www.edsurge.com/news/2022-04-01-why-i-m-still-bullish-about-the-state-of-edtech. Accessed on: 20 dec. 2023.

PANE, John F. **Strategies for Implementing Personalized Learning While Evidence and Resources Are Underdeveloped**. [*S. l.: s. n.*], 2018. Available at: https://www.rand.org/pubs/perspectives/PE314.html. Accessed on: 7 jun. 2023.

PANGARKAR, Tajammul. Eye-Opening EdTech Statistics: Opportunities and Obstacles. **Market.US**, [*s. l.*], 9 mai 2023. Available at: https://scoop.market.us/edtech-statistics/. Accessed on: 12 nov. 2023.

PANGRAZIO, Luci *et al*. Datafcation Meets Platformization: Materializing Data Processes in Teaching and Learning. **Harvard Educational Review**, [*s. l.*], v. 92, n. 2, 2022. Available at: http://meridian.allenpress.com/her/article-pdf/92/2/257/3117141/i1943-5045-92-2-257.pdf.

PANGRAZIO, Luci; SELWYIN, Neil; CUMBO, Bronwyn. A patchwork of platforms: mapping data infrastructures in schools. **Learning, Media and Technology**, [*s. l.*], 2022.

PAPAMITSIOU, Zacharoula; ECONOMIDES, Anastasios A. Learning Analytics and Educational Data Mining in Practice: A Systematic Literature Review of Empirical Evidence. **Educational Technology & Society**, [*s. l.*], v. 17, n. 4, p. 49–64, 2014.

PAPPANO, Laura. The year of the MOOC. **The New York Times**, [*s. l.*], 2 nov. 2012. Available at: https://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html. Accessed on: 18 mar. 2023.

PATIL, Lara. The business of development: The institutional rationales of technology corporations in educational development. **International Journal of Educational Development**, [*s. l.*], v. 97, 2023.

PAYNE, Lisa. Child rights impact assessment as a policy improvement tool. **International Journal of Human Rights**, [*s. l.*], v. 23, n. 3, p. 408–424, 2019.

PECKHAM, Erik. A multiverse, not the metaverse. **Techcrunch**, [*s. l.*], 25 feb. 2020. Available at: https://techcrunch.com/2020/02/25/virtual-worlds-intro/?guce_referrer=aHR0cHM6Ly93d3cudGhlY2hpbGRyZW5zbWVkaWFmb3VuZGF0aW9uLm9yZy8&guce_referrer_sig=AQAAAID7jbCgK35d7vQt6HGpaPMn-1KzyoGS4qPB62SemPoCJHxG6siT4ZxXE05gzJx3SsuA1wyNEuPxk56g87VYqQw3TnpYZvIMRCuwUbTA3EymQRlRpCBz_BDkTB6ZE2je3eAHWgZuwoPbEgSbGd32CtlsyeQgGVmFyij9C3s-XveE&guccounter=2. Accessed on: 18 mar. 2023.

PEDRÓ, Francesc *et al*. **Working Papers on Education Policy. Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development**. Paris: [*s. n.*], 2019. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000366994. Accessed on: 17 dec. 2023.

PEREIRA, Fábio Queiroz; LARA, Mariana Alves; RODRIGUES, Anna Luísa Braz. A autonomia progressiva de crianças e adolescentes e a busca por um sistema de apoios. **civilistica.com**, [*s. l.*], v. 12, n. 2, p. 1–23, 2023. Available at: https://civilistica.emnuvens.com.br/redc/article/view/889. Accessed on: 4 oct. 2023.

PERERA, Ayesh. **The Pygmalion Effect: Definition & Examples**. [*S. l.*], 2023. Available at: https://simplysociology.com/pygmalion-effect.html. Accessed on: 19 mai 2023.

PEREZ, Sarah. Google Expands Its Educational Platform “Classroom” With A New API, Share Button For Websites. **Tech Crunch**, [*s. l.*], 29 jun. 2015. Available at:

https://techcrunch.com/2015/06/29/google-expands-its-educational-platform-classroom-with-a-new-api-share-button-for-websites/. Accessed on: 8 aug. 2023.

PEREZ, Sarah; LARDINOIS, Frederic. Google rebrands its business apps as G Suite, upgrades apps & announces Team Drive. **Tech Crunch**, [*s. l.*], 29 sep. 2016. Available at: https://techcrunch.com/2016/09/29/google-rebrands-its-business-apps-as-g-suite-launches-team-drive-upgrades-apps/. Accessed on: 8 aug. 2023.

PERROTTA, Carlo *et al.* Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. **Critical Studies in Education**, [*s. l.*], v. 62, n. 1, p. 97–113, 2021.

PERROTTA, C.; EVANS, M. A. Orchestration, power, and educational technology: A response to Dillenbourg. **Computers and Education**, [*s. l.*], v. 69, p. 520–522, 2013.

PERROTTA, Carlo; WILLIAMSON, Ben. The social life of Learning Analytics: cluster analysis and the 'performance' of algorithmic education. **Learning, Media and Technology**, [*s. l.*], v. 43, n. 1, p. 3–16, 2018.

PETERS, Michael A. The New Prudentialism in Education: Actuarial Rationality and the Entrepreneurial Self. **Educational Theory**, [*s. l.*], v. 55, n. 2, p. 123–137, 2005.

PINTO, Renata Ávila. Digital Sovereignty or Digital Colonialism?. **Sur**, [*s. l.*], v. 15, n. 27, p. 15–27, 2018. Available at: https://sur.conectas.org/soberania-digital-ou-colonialismo-digital/. Accessed on: 14 sep. 2023.

POORTVLIET, Jos. Microsoft and Telekom no longer offer cloud storage under German jurisdiction. **Nextcloud**, [*s. l.*], 4 sep. 2018. Available at: https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction/. Accessed on: 27 sep. 2023.

POWLES, Julia; NISSENBAUM, Helen. The Seductive Diversion of 'Solving' Bias in Artificial Intelligence. **OneZero Medium**, [s. l.], 7 dec. 2018. Available at: https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53. Accessed on: 18 jan. 2024.

PROJECT GUTENBERG. **Aboct.** [*S. l.*], [*s. d.*]. Available at: https://www.gutenberg.org/about/. Accessed on: 11 mar. 2023.

PURTOVA, Nadya; MAANEN, Gijs van. Data as an economic good, data as a commons, and data governance. **Law, Innovation, and Technology (Advance online publication)**, [*s. l.*], v. 16, n. 1, 2023.

QINGDAO DECLARATION, 2015: SEIZE DIGITAL OPPORTUNITIES, LEAD EDUCATION TRANSFORMATION. . [*S. l.: s. n.*], 2015. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000233352. Accessed on: 17 dec. 2023.

REQUIÃO, Maurício; MENDONÇA, Júlia. O caminho mais adequado para o tratamento de dados pessoais de crianças e adolescentes: aplicação do artigo 11 da LGPD e a equiparação com dados sensíveis. **Diké**, [*s. l.*], v. 22, n. 22, p. 291–304, 2023. Available at: https://www.dataprivacybr.org/wp-.

RICAURTE, Paola. Data Epistemologies, The Coloniality of Power, and Resistance. **Television and New Media**, [*s. l.*], v. 20, n. 4, p. 350–365, 2019.

RIEDER, Gernot; SIMON, Judith. Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences. *In*: BERECHENBARKEIT DER WELT? [*S. l.*]: Springer Fachmedien Wiesbaden, 2017. p. 85–105.

RIVAS, Axel. **In-Progress Reflection No. 46 On Current and Critical Issues in Curriculum, Learning and Assessment. The Platformization of Education: A framework to Map the New Directions of Hybrid Education Systems. IBE/2021/WP/CD/46Learning and Assessment**. [*S. l.: s. n.*], 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000377733. Accessed on: 11 dec. 2023.

ROONEY, Tanya. Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility. **Surveillance & Society**, [*s. l.*], v. 7, n. 3/4, p. 344–355, 2010.

SAETTLER, L. Paul. **The evolution of American educational technology**. 2. ed. [*S. l.*]: Information Age Publishing, 2004.

SAHA, Debanjan. How The World Became Data-Driven, And What's Next. **Forbes** , [*s. l.*], 20 mai 2020. Available at: https://www.forbes.com/sites/googlecloud/2020/05/20/how-the-world-became-data-driven-and-whats-next/. Accessed on: 21 jul. 2023.

SALOMON, Jean Jacques. What is technology? The issue of its origins and definitions. **History and Technology**, [*s. l.*], v. 1, n. 2, p. 113–156, 1984.

SANDBERG, Kirsten. The convention on the rights of the child and the vulnerability of children. **Nordic Journal of International Law**, [*s. l.*], v. 84, n. 2, p. 221–247, 2015.

SARTOR, Giovanni. **The impact of the General Data Protection Regulation (GDPR) on artificial intelligence**. Brussels: [*s. n.*], 2020. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf. Accessed on: 18 jan. 2024.

SARWAR, Moizza Binat. Reading Audrey Watters: A reflection on personalised learning via education technology through a decolonial lens. [*s. l.*], 21 apr. 2022. Available at: https://edtechhub.org/2022/04/21/personalised-learning/. Accessed on: 14 mai 2023.

SAVILLO, Lia. A Chinese School Made Students Wear Brainwave-Detecting Headgear. **Vice**, [*s. l.*], 4 nov. 2019. Available at: https://www.vice.com/en/article/a359w4/chinese-school-made-students-wear-brainwave-detecting-headgear. Accessed on 15 jan. 2014.

SCHAEFER, Joe. A Data-Driven Approach Could Be the Next Great Innovation for Education. **Wired**, [*s. l.*], [*s. d.*]. Available at: https://www.wired.com/sponsored/story/a-data-driven-approach-could-be-the-next-great-innovation-for-education/. Accessed on: 5 mai 2023.

SCHILDKAMP, Kim; KUIN LAI, Mei. Introduction. *In*: SCHILDKAMP, Kim; KUIN LAI, Mei; EARL, Lorna (org.). **Data-based Decision Making in Education: Challenges and Opportunities**. [*S. l.*]: Springer, 2013. v. 17, p. 1–8.

SCHMAHL, Stefanie. **United Nations Convention on the Rights of the Child: Article-by-Article Commentary**. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2021.

SCHNEIER, Bruce. Surveillance Kills Freedom By Killing Experimentation. **Wired**, [*s. l.*], 16 nov. 2018. Available at: https://www.wired.com/story/mcsweeneys-excerpt-the-right-to-experiment/. Accessed on: 28 jun. 2023.

SCHWARTZ, Oscar. Untold History of AI: Algorithmic Bias Was Born in the 1980s A medical school thought a computer program would make the admissions process fairer—but it did just the opposite. **IEE Spectrum**, [*s. l.*], 15 apr. 2019. Available at: https://spectrum.ieee.org/untold-history-of-ai-the-birth-of-machine-bias. Accessed on: 18 oct. 2023.

SCHYNS, Camille. **The Lobbying Ghost in the Machine: Big Tech's covert defanging of Europe's AI Act**. [*S. l.: s. n.*], 2023. Available at: https://corporateeurope.org/sites/default/files/2023-03/The%20Lobbying%20Ghost%20in%20the%20Machine.pdf. Accessed on: 27 sep. 2023.

SCOTTISH SCHOOL PUPILS HAVE RESULTS UPGRADED. **BBC**, [*s. l.*], 11 aug. 2020. Available at: https://www.bbc.com/news/uk-scotland-53740588?intlink_from_url=https://www.bbc.co.uk/news/topics/c6n96k71wq0t/scottish-exam-results&link_location=live-reporting-story. Accessed on: 18 oct. 2023.

SEBRIAM, Debora; GONSALES, Priscila. **CIEB Estudos #2. Inovação aberta em educação: Conceitos e modelos de negócios**. [*S. l.: s. n.*], 2017. Available at: https://estudocieb.educadigital.org.br/wp-content/uploads/2017/02/CIEB-Estudos-2-Inovacao-Aberta-em-Educacao.pdf. Accessed on: 25 oct. 2023.

SEKI, Allan Kenji; VENCO, Selma Borghi. Política Nacional de Educação Digital: Uma análise de seus rebatimentos na educação pública brasileira. **Germinal: Marxismo e Educação em Debate**, [*s. l.*], v. 15, n. 2, p. 448–471, 2023.

SELWYN, Neil. Data entry: towards the critical study of digital data and education. **Learning, Media and Technology**, [*s. l.*], v. 40, n. 1, p. 64–82, 2015.

SELWYN, Neil; GAŠEVIĆ, Dragan. The datafication of higher education: discussing the promises and problems. **Teaching in Higher Education**, [*s. l.*], v. 25, n. 4, p. 527–540, 2020.

SHAH, Dhawal. By The Numbers: MOOCs in 2021. **The Report**, [*s. l.*], 1 dec. 2021. Available at: https://www.classcentral.com/report/mooc-stats-2021/. Accessed on: 30 jul. 2023.

SIEMENS, George *et al.* **Open Learning Analytics: an integrated & modularized platform proposal to design, implement and evaluate an open platform to integrate heterogeneous learning analytics techniques**. [*S. l.: s. n.*], 2011. Available at: https://solaresearch.org/wp-content/uploads/2011/12/OpenLearningAnalytics.pdf. Accessed on: 16 mar. 2023.

SIIBAK, Andra; MASCHERONI, Giovanna. **Children's data and privacy in the digital age**. Hamburg: [*s. n.*], 2021. Available at: https://www.ssoar.info/ssoar/bitstream/handle/document/76251/ssoar-2021-siibak_et_al-

Childrens_data_and_privacy_in.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-siibak_et_al-Childrens_data_and_privacy_in.pdf. Accessed on: 30 dec. 2023.

SINGER, Natasha. How Google Took Over the Classroom. **The New York Times**, [*s. l.*], 13 mai 2017. Available at: nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html. Accessed on: 14 aug. 2023.

SINGER, Natasha. How the Netherlands Is Taming Big Tech. **The New York Times**, [*s. l.*], 18 jan. 2023. Available at: https://www.nytimes.com/2023/01/18/technology/dutch-school-privacy-google-microsoft-zoom.html. Accessed on: 14 sep. 2023.

SINGH, Kishore. **Report of the Special Rapporteur on the Right to Education, Kishore Singh: protecting the right to education against commercialization. A/HRC/29/30**. [*S. l.: s. n.*], 2015a. Available at: https://digitallibrary.un.org/record/797838. Accessed on: 25 dec. 2023.

SINGH, Kishore. **Report of the Special Rapporteur on the right to education on Public Private Partnerships and the right to education. A/70/342**. [*S. l.: s. n.*], 2015b. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/264/89/PDF/N1526489.pdf?OpenElement. Accessed on: 1 nov. 2023.

SINHA, Shantanu. New education features to help teachers save time and support students. **Google - The Keyword**, [*s. l.*], 22 jan. 2024. Available at: https://blog.google/outreach-initiatives/education/bett-2024-google-for-education-updates/. Accessed on: 14 aug. 2023.

SINHA, Shantanu. New Google for Education tools for how you teach, learn and manage. **Google - The Keyword**, [*s. l.*], 22 jun. 2023. Available at: https://blog.google/outreach-initiatives/education/google-for-education-iste-2023/. Accessed on: 14 aug. 2023.

SIVON. **Over ons**. [*S. l.*], [*s. d.*]. Available at: https://sivon.nl/over-ons/. Accessed on: 27 sep. 2023.

SIVON. **Stand van zaken DPIA Google Workspace: update privacymaatregelen**. [*S. l.*], 2023. Available at: https://sivon.nl/2023/04/stand-van-zaken-dpia-google-workspace-update-privacymaatregelen/. Accessed on: 27 sep. 2023.

SKINNER, B. F. Teaching Machines: From the experimental study of learning come devices which arrange optimal conditions for self-instruction. **Science**, [*s. l.*], v. 128, n. 3330, p. 969–977, 1958.

SMUHA, Nathalie. Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective. *In*: , 2023a. **Working paper - ERA Conference Proceedings**. [*S. l.: s. n.*], 2023.

SMUHA, Nathalie *et al.* **How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act**. [*S. l.: s. n.*], 2021. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991. Accessed on: 21 oct. 2023.

SMUHA, Nathalie. Pitfalls and pathways for Trustworthy Artificial Intelligence in education. *In*: HOLMES, Wayne; PORAYSKA-POMSTA, Kaśka (org.). **The Ethics of Artificial Intelligence in Education: Practices, Challenges, and Debates**. [*S. l.*]: Routledge, 2023b.

SOLOVE, Daniel J. **Artificial Intelligence and Privacy**. 2024. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111. Accessed on: 6 feb. 2024.

SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law. **Boston University Law Review (Advance online publication)**, [*s. l.*], 2023. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743. Accessed on: 1 aug. 2023.

SOLOW-NIEDERMAN, Alicia. Information Privacy and the Inference Economy. **Northwestern University Law Review**, [*s. l.*], v. 117, n. 2, p. 357–424, 2022. Available at: https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1. Accessed on: 12 dec. 2023.

SORKIN, Andrew Ross; PETERS, Jeremy W. Google to Acquire YouTube for $1.65 Billion. **The New York Times**, [*s. l.*], 9 oct. 2006. Available at: https://www.nytimes.com/2006/10/09/business/09cnd-deal.html. Accessed on: 8 aug. 2023.

SPECTOR, J Michael. **The SAGE encyclopedia of educational technology**. Thousand Oaks, California: SAGE Publications, 2015.

STANDAERT, Michael. Chinese primary school halts trial of device that monitors pupils' brainwaves. **The Guardian**, [*s. l.*], 1 nov. 2019. Available at: https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves. Accessed on 15 jan. 2014.

STATZ, Pamela. Google Announces Office Suite, Takes Aim at Microsoft. **Wired**, [*s. l.*], 28 aug. 2006. Available at: https://www.wired.com/2006/08/google-announces-office-suite-takes-aim-at-microsoft/. Accessed on: 8 aug. 2023.

STRAUSS, Valerie. Bill Gates: 'It would be great if our education stuff worked but…'. **The Washington Post**, [*s. l.*], 27 sep. 2013. Available at: https://www.washingtonpost.com/news/answer-sheet/wp/2013/09/27/bill-gates-it-would-be-great-if-our-education-stuff-worked-but/. Accessed on: 2 jul. 2023.

STRINGER, Eleanor; LEWIN, Cathy; COLEMAN, Robbie. **Using Digital Technology to Improve Learning: Guidance Report**. [*S. l.: s. n.*], 2019. Available at: https://educationendowmentfoundation.org.uk/public/files/Publications/digitalTech/EEF_Digital_Technology_Guidance_Report.pdf. Accessed on: 10 mai 2023.

SUJON, Zoetanya. Disruptive play or platform colonialism? The contradictory dynamics of Google expeditions and educational virtual reality. **Digital Culture & Education**, [*s. l.*], v. 11, n. 1, p. 1–21, 2019. Available at: https://static1.squarespace.com/static/5cf15af7a259990001706378/t/5ebe94dcc4b8b2207a72b2e6/1589548261728/Cover-merged.pdf. Accessed on: 10 aug. 2023.

SURF. **Agreement with Google on privacy risks**. [*S. l.*], 2021a. Available at: https://www.surf.nl/en/agreement-with-google-on-privacy-risks. Accessed on: 27 sep. 2023.

SURF. **Essential Services**. [*S. l.*], [*s. d.*]. Available at: https://www.surf.nl/files/2023-07/bijlage-list-of-essential-services.pdf. Accessed on: 27 sep. 2023 a.

SURF. **Google Workspace for Education support package**. [*S. l.*], 2021b. Available at: https://www.surf.nl/en/google-workspace-for-education-support-package. Accessed on: 27 sep. 2023.

SURF. **Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved**. [*S. l.*], 2023a. Available at: Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved. Accessed on: 27 sep. 2023.

SURF. **Status of Google Workspace DPIA: update on privacy measures**. [*S. l.*], 2023b. Available at: https://www.surf.nl/en/status-of-google-workspace-dpia-update-on-privacy-measures. Accessed on: 27 sep. 2023.

SURF. **SURF and SIVON discuss privacy risks with Google**. [*S. l.*], 2021c. Available at: https://www.surf.nl/en/surf-and-sivon-discuss-privacy-risks-with-google. Accessed on: 27 sep. 2023.

SURF. **SURF is the collaborative organisation for IT in Dutch education and research**. [*S. l.*], [*s. d.*]. Available at: https://www.surf.nl/en. Accessed on: 27 sep. 2023 b.

SURF. **SURF, SIVON and Google reach agreement Terms of Service Google Chrome**. [*S. l.*], 2023c. Available at: https://www.surf.nl/en/surf-sivon-and-google-reach-agreement-terms-of-service-google-chrome. Accessed on: 27 sep. 2023.

SURF; SIVON. **Final improvement plan Google ChromeOS and Chrome browser on Chrome devices.** [*S. l.*], 2023. Available at: https://sivon.nl/wp-content/uploads/2023/07/Improvement-plan-Google-for-ChromeOS-on-managed-devices.pdf. Accessed on: 27 sep. 2023.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy, and manipulation. **Internet Policy Review**, [*s. l.*], v. 8, n. 2, 2019.

SWIST, Teresa *et al.* **As more biometric data is collected in schools, parents need to ask these 10 questions**. [*S. l.*], 2022. Available at: https://theconversation.com/as-more-biometric-data-is-collected-in-schools-parents-need-to-ask-these-10-questions-191263. Accessed on: 27 jul. 2023.

TAEKEMA, Sanne. Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice. **Law and Method**, [s. l.], 2018. https://doi.org/10.5553/REM/.000031.

TEFFÉ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. *In*: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. [*S. l.*]: Obliq Livros; ITS Rio, 2021. p. 342–395. Available at: https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf. Accessed on: 4 oct. 2023.

TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélogo, 2020.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Contratação em redes sociais e proteção de dados de crianças e adolescentes. *In*: ROQUE, Andre Vasconcelos; OLIVA, Milena Donato (org.). **Direito na era digital: aspectos negociais, processuais e registrais**. [*S. l.*]: Editora Jus Podivm, 2022. p. 97–122.

TERRA, Floor; NAS, Sjoera; ROOSENDAAL, Arnold. **Inspection results Google Chrome for Education. SIVON**. [*S. l.: s. n.*], 2023. Available at: https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf. Accessed on: 27 sep. 2023.

TERWANGNE, Cécile de. Article 5. Principles relating to processing of personal data. *In*: KUNER, Christopher; BYGRVE, Lee A.; DOCKSEY, Christopher (org.). **The EU General Data Protection Regulation: A Commentary**. [*S. l.*]: Oxford University Press, 2020a. p. 309–320.

TERWANGNE, Cécile de. Article 16. Right to rectification. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary**. [*S. l.*]: Oxford University Press, 2020b. p. 469–474.

THATCHER, Jim; O'SULLIVAN, David; MAHMOUDI, Dillon. Data colonialism through accumulation by dispossession: New metaphors for daily data. **Environment and Planning D: Society and Space**, [*s. l.*], v. 34, n. 6, p. 990–1006, 2016.

THE EDITORS OF ENCYCLOPAEDIA BRITANNICA. **Technology**. *In*: ENCYCLOPAEDIA BRITANNICA. [*S. l.: s. n.*], 2022. Available at: https://www.britannica.com/technology/technology. Accessed on: 19 mar. 2023.

THE EDUCATION COALITION. **History of Telecourses**. [*S. l.*], [*s. d.*]. Available at: https://www.tecweb.org/eddevel/telecon/de92.html. Accessed on: 16 mai 2023.

TIETOSUOJAVALTUUTETTU. **Tietosuojavaltuutetun päätös käsittelyn lainmukaisuutta ja henkilötietojen siirtoa kolmansiin maihin koskevassa asiassa**. [*S. l.*], 2021. Available at: https://finlex.fi/fi/viranomaiset/tsv/2021/20211503?search%5Btype%5D=pika&search%5Bpika%5D=google. Accessed on: 4 dec. 2023.

TOBIN, John; FIELD, Sarah M. Article 16. The Right to Protection of Privacy, Family, Home, Correspondence, Honour and Reputation. *In*: TOBIN, John (org.). **The UN Convention on the Rights of the Child: A Commentary**. Oxford: Oxford University Press, 2019. p. 551–599.

TOMAŠEVSKI, Katarina. **Human rights obligations: making education available, accessible, acceptable and adaptable**. [*S. l.: s. n.*], 2001. Available at: https://www.right-to-education.org/resource/primer-no-3-human-rights-obligations-making-education-available-accessible-acceptable-and. Accessed on: 11 jul. 2023.

TOSONI, Luca. Article 4(25). Information society service. *In*: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). **The EU General Data Protection Regulation (GDPR): A Commentary**. [*S. l.*]: Oxford University Press, 2020. p. 292–302.

TRZASKOWSKI, Jan. Data-driven business models - Privacy and marketing. *In*: KOSTA, Eleni; LEENES, Ronald; KAMARA, Irene (org.). **Research Handbook on EU Data Protection Law**. [*S. l.*]: Edward Elgar, 2022. p. 206–239.

UNDERSTANDING DIGITAL CREDENTIALS BUILDING VALUE FROM AN ECOSYSTEM OF OPEN STANDARDS. [*S. l.*], [*s. d.*]. Available at: https://www.imsglobal.org/understanding-digital-credentials. Accessed on: 4 mai 2023.

UNESCO. **An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19**. Paris: [*s. n.*], 2023a. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000386701. Accessed on: 24 sep. 2023.

UNESCO. **Global Education Monitoring Report. Technology in education: A Tool in Whose Terms?** Paris: [*s. n.*], 2023b. Available at: https://www.unesco.org/gem-report/en/technology. Accessed on: 30 jul. 2023.

UNESCO. **Rethinking education: towards a global common good?** Paris: [*s. n.*], 2015.

UNESCO INSTITUTE FOR STATISTICS (UIS). **Guide to measuring information and communication technologies (ICT) in education**. [*S. l.*]: UNESCO Institute for Statistics, 2009. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000186547. Accessed on: 29 jul. 2023.

UNICEF. **Convention on the Rights of the Child: For every child, every right.** [*S. l.*], [*s. d.*]. Available at: https://www.unicef.org/child-rights-convention. Accessed on: 5 jul. 2023.

UNICEF. **Early Warning Systems for Students at Risk of Dropping Out: Policy and Practive for Enrolling All Children and Adolescents in School and Preventing Dropoct.** [*S. l.: s. n.*], 2018. Available at: https://www.unicef.org/eca/sites/unicef.org.eca/files/2018-11/Early%20warning%20systems%20for%20students%20at%20risk%20of%20dropping%20out_0.pdf. Accessed on: 12 nov. 2023.

UNICEF. **Implementation handbook for the Convention on the Rights of the Child**. [*S. l.*]: UNICEF, 2007. Available at: https://www.unicef.org/reports/implementation-handbook-convention-rights-child. Accessed on: 13 jul. 2023.

UNICEF. **Policy guidance on AI for children 2.0**. [*S. l.: s. n.*], 2021. Available at: https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children. Accessed on: 30 jul. 2023.

UNICEF. **The State of the World's Children 2017: Children in a Digital WorldUnicef**. [*S. l.: s. n.*], 2017. Available at: https://www.unicef.org/reports/state-worlds-children-2017. Accessed on: 31 oct. 2022.

UNITED NATIONS HUMAN RIGHTS. OFFICE OF THE HIGH COMMISSIONER. **Guiding Principles on Business and Human rights. Implementing the United Nations**

“Protect, Respect and Remedy” Framework. HR/PUB/11/04. [*S. l.: s. n.*], 2011. Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf. Accessed on: 9 jul. 2023.

UNITED NATIONS HUMAN RIGHTS TREATY BODIES. **Committee on the Rights of the Child**. [*S. l.*], [*s. d.*]. Available at: https://www.ohchr.org/en/treaty-bodies/crc. Accessed on: 30 dec. 2023.

UPSON, Linus. A new kind of computer: Chromebook. **Google Official Blog**, [*s. l.*], 11 mai 2011. Available at: https://googleblog.blogspot.com/2011/05/new-kind-of-computer-chromebook.html?+. Accessed on: 8 aug. 2023.

VAIDHYANATHAN, Siva. **The Googlization of everything (and why we should worry)**. [*S. l.*]: University of California Press, 2011.

VANCE, Amelia; SEXTON, Morgan; KALPOS, Katherine Sledge. Tis the Season for Rulemaking: FTC Announces New COPPA NPRM. **Public Interest Privacy Center**, [*s. l.*], 20 dec. 2023. Available at: https://pipc.substack.com/p/tis-the-season-for-rulemaking-ftc?r=26ap01. Accessed on: 25 dec. 2023.

VARADAN, Sheila. The principle of evolving capacities under the UN convention on the rights of the child. **International Journal of Children’s Rights**, [*s. l.*], v. 27, n. 2, p. 306–338, 2019.

VEDDER, Anton. KDD: The challenge to individualism. **Ethics and Information Technology**, [*s. l.*], v. 1, p. 275–281, 1999.

VELIZ, Carissa. Digitization, Surveillance, Colonialism. **Liberties**, [*s. l.*], v. 3, n. 1, 2022. Available at: https://libertiesjournal.com/articles/digitization-surveillance-colonialism/. Accessed on: 31 oct. 2022.

VERDOODT, Valerie. **Children’s rights and commercial communication in the digital era: Towards an empowering regulatory framework for commercial communication**. [*S. l.*]: Intersentia, 2020.

VERTESI, Janet. My Experiment Opting Out of Big Data Made Me Look Like a Criminal. **Time**, [*s. l.*], 1 mai 2014. Available at: https://time.com/83200/privacy-internet-big-data-opt-out/. Accessed on: 24 jun. 2023.

VICENTINI, Letizia *et al.* **Future opportunities for education technology in England**. [*S. l.: s. n.*], 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1080930/Future_opportunities_for_education_technology_in_England_June_2022.pdf. Accessed on: 19 oct. 2023.

VINCENT-LANCRIN, Stéphan. Frontiers of smart education technology: Opportunities and challenges. *In*: OECD DIGITAL EDUCATION OUTLOOK 2021: PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS. Paries: OECD Publishing, 2021. p. 19–42.

VOGIATZOGLOU, Plixavra; VALCKE, Peggy. Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law. *In*: KOSTA, Eleni; LEENED RONALD; KAMARA, Irene (org.). **Research Handbook on EU Data Protection Law**. [*S. l.*]: Edward Elgar, 2022. p. 11–49.

VTC. **Aanbeveling VTC bij de Digisprong in het onderwijs**. [*S. l.*], 2021. Available at: https://overheid.vlaanderen.be/digitale-overheid/digisprong-in-het-onderwijs. Accessed on: 13 dec. 2023.

VTC. **Over de Vlaamse Toezichtcommissie**. [*S. l.*], [*s. d.*]. Available at: https://overheid.vlaanderen.be/vlaamse-toezichtcommissie. Accessed on: 14 dec. 2023.

VTC. **Standpunt VTC i.v.m. gebruik Google for Education door basis- en secundair onderwijs**. [*S. l.: s. n.*], 2023a.

VTC. **Vragen VTC aan Google na Overleg met Google en na Brief aan Minister van Onderwijs**. [*S. l.: s. n.*], 2023b. Available at: https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_O_2023_01_vragen_aan_Google_deel_2_naVTC_def.pdf?timestamp=1689170403. Accessed on: 13 dec. 2023.

WACHTER, Sandra; MITTELSTADT, Brent Daniel. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, [*s. l.*], n. 2, p. 494–620, 2019. https://doi.org/10.7916/cblr.v2019i2.3424.

WAGNER, Alan; BORENSTEIN, Jason; HOWARD, Ayanna. Overtrust in the robotic age. **Communications of the ACM**, NEW YORK, v. 61, n. 9, p. 22–24, 2018.

WALKER, Christopher. Unlocking the impact of edtech. **impactInvestor**, [*s. l.*], 15 dec. 2023. Available at: https://impact-investor.com/unlocking-the-impact-of-edtech/. Accessed on: 23 dec. 2023.

WATTERS, Audrey. **How Steve Jobs Brought the Apple II to the Classroom**. [*S. l.*], 2015. Available at: http://hackeducation.com/2015/02/25/kids-cant-wait-apple. Accessed on: 27 jul. 2023.

WATTERS, Audrey. School Work and Surveillance. **HackEducation**, [*s. l.*], 30 apr. 2020. Available at: https://hackeducation.com/2020/04/30/surveillance. Accessed on: 28 mai 2023.

WATTERS, Audrey. **Teaching Machines**. [*S. l.*]: The MIT Press, 2021.

WATTERS, Audrey. The Teleology of Ed-Tech. **oeb Insights**, [*s. l.*], 11 apr. 2019. Available at: https://oeb.global/oeb-insights/the-teleology-of-ed-tech/. Accessed on: 13 mai 2023.

WEBB, P. Taylor; SELLAR, Sam; GULSON, Kalervo N. Anticipating education: governing habits, memories and policy-futures. **Learning, Media and Technology**, [*s. l.*], v. 45, n. 3, p. 284–297, 2020.

WELLER, Martin. **25 Years of Ed Tech**. [*S. l.: s. n.*], 2020.

WELLER, Martin. **The Battle For Open: How openness won and why it doesn't feel like victory**. London: Ubiquity Press, 2014. Available at:

https://library.oapen.org/bitstream/id/3b361bf2-c5e4-4bcd-8b69-3cdcbab008c5/533876.pdf. Accessed on: 18 mar. 2023.

WELLER, Martin. **Virtual Learning Environments: Using, Choosing and Developing Your VLE**. New York: Routledge, 2007.

WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business and Society**, [*s. l.*], v. 58, n. 1, p. 20–41, 2019.

WHO WATCHES AI WATCHING STUDENTS? [AUDIO PODCAST EPISODE]. Apresentado por Jennifer Strong. [*S. l.*]: MIT Technology Review, 2022. Available at: https://www.technologyreview.com/2022/06/29/1057103/podcast-who-watches-ai-watching-students/. Accessed on: 5 mai 2023.

WILLIAMSON, Ben. Datafication of Education: A Critical Approach to Emerging Analytics Technologies and Practices. *In*: BEETHAM, Helen; SHARPE, Rhona (org.). **Rethinking Pedagogy for a Digital Age: Principles and Practices of Design**. 3. ed. [*S. l.*]: Routledge, 2019.

WILLIAMSON, Ben. Digital education governance: data visualization, predictive analytics, and 'real-time' policy instruments. **Journal of Education Policy**, [*s. l.*], v. 31, n. 2, p. 123–141, 2016.

WILLIAMSON, Ben. Google's plans to bring AI to education make its dominance in classrooms more alarming. **Fast Company**, [*s. l.*], 28 mai 2021. Available at: https://www.fastcompany.com/90641049/google-education-classroom-ai. Accessed on: 14 aug. 2023.

WOLFF, Josephine; LEHR, William; YOO, Christopher, S. **Public Law and Legal Theory Research Paper Series Research Paper No. 23-32. Lessons from GDPR for AI Policymaking**. 2023. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4528698. Accessed on: 6 feb. 2024.

WOLFSON, Lisa. Venture Capital Needed for 'Broken' U.S. Education, Thrun Says. **Bloomberg**, [*s. l.*], 18 jun. 2013. Available at: https://www.bloomberg.com/news/articles/2013-06-18/venture-capital-needed-for-broken-u-s-education-thrun-says#xj4y7vzkg. Accessed on: 12 nov. 2023.

WOLVERS, Andrea *et al*. Introduction. *In*: CONCEPTS OF THE GLOBAL SOUTH: VOICES FROM AROUND THE WORLD. [*S. l.*]: Global South Studies Center, University of Cologne, 2015. p. 1–2. Available at: https://kups.ub.uni-koeln.de/6399/1/voices012015_concepts_of_the_global_south.pdf. Accessed on: 20 jun. 2023.

WP29. **Opinion 02/2013 on apps on smart devices**. [*S. l.: s. n.*], 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Accessed on: 18 jul. 2023.

WP29. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. [*S. l.: s. n.*], 2016. Available at: https://ec.europa.eu/newsroom/article29/items/612053/en. Accessed on: 27 oct. 2023.

WP29. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679**. [*S. l.: s. n.*], 2017. Available at: https://ec.europa.eu/newsroom/article29/items/611236/en. Accessed on: 19 jul. 2023.

WP29. **Guidelines on the right to "data portability"**. [*S. l.: s. n.*], 2017. Available at: https://ec.europa.eu/newsroom/article29/items/611233. Accessed on: 28 oct. 2023.

WP29. **Guidelines on transparency under Regulation 2016/679**. [*S. l.: s. n.*], 2018. Available at: https://ec.europa.eu/newsroom/article29/items/622227/en. Accessed on: 19 jul. 2023.

WP29. **Opinion 03/2013 on purpose limitation**. [*S. l.: s. n.*], 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Accessed on: 18 jul. 2023.

WP29. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. [*S. l.: s. n.*], 2014. Available at: http://ec.europa.eu/justice/data-protection/index_en.htm. Accessed on: 17 jul. 2023.

YOUNG, Andrew; VERHULST, Stephan G. Why we need responsible data for children. **The Conversation**, [*s. l.*], 23 mar. 2020. Available at: https://theconversation.com/why-we-need-responsible-data-for-children-134052. Accessed on: 24 jun. 2023.

ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Julia. Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. *In*: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Obliq; ITS Rio, 2021. Available at: https://itsrio.org/pt/publicacoes/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes/. Accessed on: 5 oct. 2023.

ZANFIR-FORTUNA, Gabriela. Article 21. Right to object. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary**. [*S. l.*]: Oxford University Press, 2020. p. 506–521.

ZEIDE, Elana. Robot Teaching, Pedagogy, and Policy. *In*: THE OXFORD HANDBOOK OF ETHICS OF AI. [*S. l.*]: Oxford University Press, 2020. p. 788–803.

ZHANG, Xinli *et al.* The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics. **Frontiers in Psychology**, [*s. l.*], v. 13, 2022.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019. v. E-book.

16 de agosto de 2024

Por arquivamento eletrônico

Sr. Rodrigo Santana dos Santos
Autoridade Nacional de Proteção de Dados (ANPD)
Coordenação-Geral de Normatização
Setor Comercial Norte - SCN, Quadra 6, Conjunto "A", Edifício Venâncio 3000, Bloco "A", 9º andar,
Brasília, DF, 70.716-900

RE: Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes

Prezado Sr. Santos:

A *Entertainment Software Association* (aqui definido como "ESA") envia estes comentários em resposta à solicitação da Autoridade Nacional de Proteção de Dados (ANPD) para que o público contribua com a "Tomada de Subsídios: Tratamento de Dados Pessoais de Crianças e Adolescentes.

I - Princípio do melhor interesse

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

A *Entertainment Software Association* (ESA) é a associação comercial dos EUA que representa quase todas as principais editoras de videogames e fabricantes de consoles de videogame e dispositivos portáteis. Seus membros oferecem experiências interativas de alta qualidade que promovem a contação de histórias, competição e comunicação, mantendo a segurança de todos os jogadores de videogame como prioridade máxima. Por pelo menos 30 anos, o setor tem se empenhado em esforços contínuos para desenvolver e oferecer ferramentas que ajudem pais, responsáveis e jogadores a criar uma experiência de jogo on-line segura, conforme detalhado no documento Confiança e Segurança (vide anexo).

No Brasil, o sistema Classind atribui classificações de idade e conteúdo aos videogames. Sob a atribuição do Ministério da Justiça, Classind tem 6 categorias de classificação etária, descritores de conteúdo para explicar as razões por trás da indicação e elementos interativos para destacar recursos como compras no jogo ou comunicação com o usuário. Classind faz parte da *International Age Rating Coalition*, uma coalizão formada por autoridades de diversos países. O Classind fornece às famílias informações necessárias para escolher a experiência de videogame adequada, incluindo informações essenciais para proteger crianças e adolescentes de conteúdo inadequado. Ele define critérios para a análise de obras audiovisuais e observa os princípios do ECA.

ESA compartilha os objetivos da ANPD de proteger crianças e adolescentes e recomenda que a ANPD considere as questões de transparência e minimização de dados como indicadores-chave do respeito aos seus melhores interesses. Seus membros têm sido líderes em garantir a transparência na forma como informações pessoais são tratadas para experiências de jogos on-line e em oferecer ferramentas para a tomada de decisões informadas sobre configurações de privacidade, inclusive para pais e responsáveis para gerenciar as escolhas de entretenimento de seus filhos e garantir experiências adequadas à idade em videogames. Veja informações sobre transparência no item III.1. Em apoio à minimização, membros da ESA usam configurações padrão de proteção à privacidade para jogadores menores de idade, incluindo, por exemplo, limitação da coleta de dados, desativação do bate-papo e de outras comunicações no jogo, exigência de permissão dos pais para adicionar amigos ou jogar jogos com vários jogadores e desativação da coleta de dados de localização por padrão.

A ESA incentiva a ANPD a apoiar a flexibilidade contínua na proteção de crianças e adolescentes ao invés de adotar uma abordagem única para todos. Especificamente, a ESA recomenda que a ANPD publique uma orientação de conformidade voluntária sobre os princípios de melhor interesse (incluindo transparência e minimização de dados) ao invés de adotar uma regulamentação prescritiva que poderia desincentivar inovações contínuas para proteger as crianças em todas as tecnologias, plataformas e contextos. A ESA recomenda, de forma enfática, que a ANPD permita que as partes interessadas analisem e forneçam comentários sobre qualquer minuta de regulamentação formal antes de sua finalização, isso porque regulamentações tem o potencial de interromper uso de uma variedade de tecnologias popular voltadas para o consumidor, caso as diferenças no uso de tecnologia entre plataformas e setores não sejam completamente levadas em consideração.

Por fim, ESA incentiva a ANPD a garantir que tais orientações estejam alinhadas com outras iniciativas em curso no momento. Por exemplo, em nível nacional, ANPD deve coordenar com outros órgãos brasileiros envolvidos em questões de segurança e bem-estar das crianças, a nível nacional, como aquelas vinculadas à Secretaria de Comunicação Social da Presidência. ANPD também deve dialogar com legisladores para evitar criação políticas conflitantes. A nível global, ANPD deve considerar alinhamento com novas medidas de proteção de dados com frameworks globais, como o Regulamento Geral de Proteção de Dados da UE e, nos EUA, a Lei de Proteção à Privacidade Online das Crianças. ESA entende que tal alinhamento promoveria ainda mais sua conformidade.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indique quais situações ou contextos foram identificados e as principais questões a serem abordadas.

A indústria de videogames prioriza a segurança das crianças e procura minimizar a coleta de dados de menores, ao mesmo tempo em que garante a coleta apropriada de informações pessoais para administrar os esforços de confiança e segurança on-line, e garantir que o ambiente para os jogadores seja adequado à faixa etária. Algumas dessas práticas estão detalhadas abaixo e no

documento anexo sobre Confiança e Segurança (*Trust and Safety*, em inglês) (Anexo: O Setor de Videogames Prioriza a Confiança e a Segurança (*The Video Games Sector Prioritizes Trust and Safety*, em inglês)). A ESA incentiva a ANPD a apoiar esses esforços como parte do princípio do melhor interesse, incluindo onde tais práticas possam exigir a coleta de certos dados.

As empresas membros da ESA desenvolveram e implantaram tecnologias e medidas para ajudar a manter os jogadores seguros, evitar o ódio, o assédio e outros comportamentos inadequados, além de capacitar os jogadores e seus responsáveis. Algumas empresas, por exemplo, implementaram monitoramento automatizado de bate-papo, silenciamento automático e/ou moderação humana para limitar ou filtrar conteúdo ou comportamento indesejado e, quando apropriado, tomar medidas contra malfeitores para fazer cumprir os padrões da comunidade de jogos ou seus termos de serviço para proteger outros jogadores. Algumas empresas de videogame também usam aprendizado de máquina para identificar comportamentos de trapaça e garantir que os jogadores possam participar de uma competição de forma justa e positiva.

Os membros da ESA também tomam várias medidas para combater a exploração infantil. Algumas empresas utilizam tecnologias de aprendizado de máquina para detectar, abordar e denunciar predadores on-line que tentam aliciar menores. A indústria de videogames atua em conjunto com terceiros reconhecidos nessa frente, como o *National Center for Missing and Exploited Children* (NCMEC), uma organização não governamental dos Estados Unidos, e com as autoridades policiais para combater imagens e conteúdos inadequados. Por exemplo, algumas empresas membro que permitem o envio de imagens pelos usuários utilizam tecnologias de "hashing" de imagens para combater a exploração infantil. Assinaturas digitais, ou "impressões digitais" de imagens conhecidas de exploração infantil são obtidas junto ao NCMEC com o objetivo de identificar e detectar tais imagens antes que possam ser publicadas. A indústria de videogames leva a sério sua responsabilidade de compartilhar informações relevantes sobre exploração infantil com o NCMEC e com as autoridades policiais para apoiar a investigação de quaisquer imagens recentemente identificadas por eles.

Os jogos educativos também são outro exemplo de esforços para apoiar um ambiente seguro e adequado à faixa etária para o aprendizado. Por exemplo, um jogo educativo pode processar dados de jogabilidade para reconhecer que o jogador está com dificuldades em matemática, mas se sai bem em leitura, e recomendar mais conteúdos relacionados à matemática. . É fundamental que as empresas de videogame continuem a ter flexibilidade para apoiar e inovar nesses e outros esforços no futuro.

II - Consentimento

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento “específico e em destaque” de pais ou responsáveis legais?

Incentivamos a ANPD a fornecer orientações adicionais voluntárias (e não regulamentação formal) sobre possíveis abordagens para obter o consentimento “específico e destacado” de pais ou responsáveis. Essas orientações devem ser práticas e adaptáveis a uma variedade de tecnologias e experiências, e estar alinhadas com outros frameworks globais, como o GDPR e a

COPPA. Entendemos que qualquer nova orientação deve também evitar determinar mecanismos de consentimento específicos, linguagem, timing, localização ou frequência. Qualquer determinação de tipos específicos e limitados de tecnologias pode impor um grande ônus às empresas que teriam que alocar recursos para criar padrões potencialmente inadequados, ao mesmo tempo em que restringiria a liberdade das empresas de criar ou adotar tecnologias mais eficientes para obter consentimentos.

Como mencionado também nos itens II.2 abaixo, a relação entre operadores de plataformas de videogame (por exemplo, celulares, PCs, consoles e portáteis) e editores de videogames, editores esses que podem oferecer múltiplos jogos em diferentes plataformas, é única para a indústria de videogames. A ESA incentiva a ANPD a permitir que operadores de plataformas e editores de jogos considerem voluntariamente soluções apropriadas à luz da funcionalidade técnica da plataforma e dos jogos disponíveis, seja (a) implementando mecanismos de consentimento baseados na plataforma, (b) confiando nos mecanismos de consentimento implementados pelos editores dos jogos em suas plataformas, ou (c) uma combinação de ambos. A ESA incentiva a ANPD a apoiar a flexibilidade para desenvolver quaisquer abordagens desse tipo. Ao oferecer orientações que permitam aos provedores de videogames ajustar a combinação desses mecanismos de acordo com seus serviços específicos, a ANPD garantirá aos pais e responsáveis que o princípio geral do consentimento esteja em vigor e, ao mesmo tempo, que eles mantém a capacidade de decidir o tipo de sistema mais adequado para as crianças e adolescentes sob seus cuidados. Esse tipo de flexibilidade tem se mostrado bem-sucedida nos Estados Unidos, onde a COPPA prevê múltiplos métodos aprovados para a obtenção do consentimento parental.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

A ESA sugere que a ANPD considere a possibilidade de publicar orientações voluntárias sobre as principais características que devem ser reconhecidas na obtenção do consentimento, ao invés de exigir medidas e mecanismos tecnológicos específicos que possam ser aplicados de forma especifica a determinados setores ou tipos de plataformas, ou que estejam sujeitos a mudanças em função de futuras inovações tecnológicas.

Além disso, as recomendações de orientação e política da ANPD devem permanecer flexíveis para se adaptarem às boas práticas, tecnologias e mecanismos disponíveis, bem como à exigência legal de adotar "todos os esforços razoáveis" para garantir o consentimento válido dos pais ou responsáveis pela criança. Isso é fundamental para garantir que a indústria de videogames continue a ter a capacidade de inovar e melhorar a segurança on-line e proteger a privacidade dos jogadores menores de idade ao longo do tempo e em diferentes plataformas e tipos de jogos.

Como detalhado no item II.1 acima, a relação entre operadores de plataformas de videogame (por exemplo, celulares, PCs, consoles e aparelhos portáteis) e editores de videogames, editores esses que podem oferecer múltiplos jogos em diferentes plataformas, é única para a indústria de videogames. A ESA incentiva a ANPD a permitir que operadores de plataformas e editores de jogos considerem voluntariamente soluções que sejam apropriadas em função da funcionalidade

técnica da plataforma e dos jogos disponíveis, seja (a) implementando mecanismos de consentimento baseados na plataforma, (b) respeitando os mecanismos de consentimento implementados pelos editores dos jogos em suas plataformas, ou (c) uma combinação de ambos. A ESA defende uma abordagem flexível ao consentimento, pois a viabilidade de qualquer mecanismo de consentimento dependerá fortemente dos requisitos técnicos específicos da plataforma e dos jogos associados.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

A ESA incentiva a ANPD a apoiar autonomia um pouco maior para os adolescentes mais velhos em sua ao interação com videogames. Entendemos que legisladores reconheceram a importância de respeitar as escolhas dos pais com relação às informações pessoais de seus filhos pequenos e os direitos dos adolescentes de exercerem esses direitos de forma mais direta.

III - Jogos e aplicativos da Internet

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Os membros da ESA são comprometidos com a promoção da transparência sobre as práticas de tratamento de dados na indústria e a minimização da coleta de dados de menores. Esses dois princípios devem ser o foco de qualquer orientação da ANPD e essa orientação deve ser voluntária para incentivar os pais e responsáveis a tomarem decisões informadas e promover o desenvolvimento de ferramentas inovadoras.

ESA fornece ferramentas para informar os pais e ajudá-los a entender e gerenciar as interações de suas crianças e adolescentes com seus videogames, consoles e dispositivos portáteis. A ESA têm sido líder em garantir transparência na forma como informações pessoais são tratadas para experiências de jogos on-line e em oferecer ferramentas para tomada de decisões informadas sobre configurações de privacidade, inclusive para que pais e responsáveis possam gerenciar as escolhas de entretenimento de seus filhos e garantir experiências adequadas à idade em videogames. Informar pais e responsáveis, incluindo por meio de avisos de privacidade e fornecimento de informações facilmente acessíveis sobre as classificações e descritores da ClassInd para explicar as razões por trás das indicações atribuídas permite que eles tomem decisões informadas antes de fazer configurações de privacidade e seleções de jogos.

A ESA apoia os princípios de minimização e procura coletar e tratar somente os dados sobre menores que sejam estritamente necessários para garantir a segurança do jogador e um ambiente adequado à idade. Como parte desses esforços, seus membros usam configurações padrão de

proteção à privacidade para jogadores menores, desativando bate-papo e outras comunicações dentro do jogo, exigindo permissão dos pais para adicionar amigos ou jogar em modo multijogador, e desativando coleta de dados de localização por padrão.

A ESA implantou tecnologias e medidas para ajudar a manter os jogadores seguros, prevenir o ódio, assédio e outros comportamentos inadequados e empoderar jogadores e seus responsáveis. Algumas empresas implementaram monitoramento automatizado de bate-papo, silenciamento automático e/ou moderação humana para limitar ou filtrar conteúdo ou comportamento indesejado e, quando apropriado, tomar medidas contra malfeitores para fazer cumprir os padrões da comunidade de jogos ou seus termos de serviço para proteger outros jogadores. Essas medidas importantes de confiança e segurança podem incluir o tratamento de dados pessoais de menores sendo que seus membros procuram limitar esse tratamento ao estritamente necessário.

Medidas de design de videogames variam de acordo com o tipo de recursos e funcionalidades oferecidos no jogo ou na plataforma. Ressaltamos que qualquer orientação voluntária da ANPD deve ser flexível o suficiente para ser prática em todos os contextos. Ex. muitos jogos e consoles oferecem configurações padrão de proteção de privacidade para jogadores menores e controles parentais que limitam o acesso à comunicação no jogo e outros recursos interativos. Esse tipo de autorregulação e inovação deve ser incentivado.

As plataformas de videogames já implementaram ferramentas robustas de privacidade, controles parentais e outras proteções, limitando o tempo que as crianças podem passar jogando videogames, restringindo comunicações on-line com outros usuários, gerenciando a quantidade de dinheiro que as crianças podem gastar, instituindo controles parentais por senha ou PIN para que as crianças não possam contornar as configurações de segurança. Como essas ferramentas estão disponíveis no nível do dispositivo, ANPD deve permitir que os editores de jogos confiem nas seleções de privacidade e controle parental feitos em consoles, PCs e celulares. Esse sistema incentiva e apoia pais e responsáveis a tomarem decisões consistentes e informadas de maneira simplificada. Ao mesmo tempo, os editores podem ter a liberdade de adotar medidas adicionais para proteger a privacidade e a segurança dos menores.

Conclusão no item III.6 abaixo.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

A ESA solicita à ANPD que adote uma abordagem flexível para a verificação de idade em plataformas digitais, permitindo uma variedade de técnicas adequadas que protejam efetivamente crianças e adolescentes (por exemplo, (a) uma empresa deve realizar uma avaliação de risco obrigatória do processo pretendido e (b) a implementação de medidas eficazes para garantir a minimização de dados). Além disso, mecanismos neutro de verificação de idade é um método menos oneroso para as famílias do que outras técnicas de estimativa de idade que exigem identificadores físicos. Recomendamos que a ANPD forneça orientações claras e voluntárias sobre métodos aceitáveis que possam atender às preferências de privacidade, segurança e conveniência do usuário.

É importante ressaltar que a ANPD deve encarar com ceticismo as recomendações de abordagens excessivamente prescritivas, como a exigência de que os usuários forneçam documento de identidade emitidas pelo governo (como RG) para jogar videogames. Essa abordagem é desnecessária, pode ser excessivamente intrusiva e onerosa para os usuários e gerar preocupações adicionais com a privacidade (incluindo a privacidade das crianças e adolescentes, bem como dos pais e responsáveis). Em suma, uma exigência para que as empresas utilizem credenciais de identificação violaria o princípio da minimização de dados, que estabelece que os provedores devem tratar apenas os dados estritamente necessários para atingir o objetivo comercial. Ao adotar soluções flexíveis e práticas, a ANPD poderá garantir uma proteção robusta para jovens usuários sem criar barreiras desnecessárias para as famílias.

Além disso, a ESA adverte contra o uso de técnicas de estimativa de idade com relação ao público-alvo. Embora aparentemente bem-intencionadas, essas técnicas são potencialmente invasivas à privacidade e, inadvertidamente, podem fazer com que os operadores coletem mais informações pessoais dos consumidores do que seria necessário para fornecer o serviço, além de serem difíceis de implementar na prática. A ESA também adverte contra o uso de avaliações de usuários e da idade dos usuários em sites e serviços similares como evidência da composição ou do público-alvo que pretende avaliar. Nenhum desses dados serve como evidência confiável da idade dos usuários. As avaliações de usuários de um videogame, por exemplo, podem entrar em conflito umas com as outras e podem mudar ao longo do tempo, à medida que o jogo se torna popular entre diferentes públicos e se torna mais nostálgico com o passar do tempo. Além disso, dois serviços podem ser semelhantes sem que ambos sejam direcionados ao mesmo público. Por exemplo, um jogo de corrida de carros pode ser direcionado a jogadores mais velhos com base em seu design visual e de áudio, enquanto outro pode ser direcionado a crianças.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

A flexibilidade contínua para lidar com contextos específicos é especialmente importante para os videogames.

Durante várias décadas, os membros da ESA têm se esforçado para desenvolver processos adequados de minimização de dados, configurações de privacidade e controles parentais, incluindo configurações padrão, que são adaptados à indústria de videogames. Eles buscam acomodar os diferentes contextos nos quais as empresas de videogame podem tratar informações pessoais e as diferentes funcionalidades de jogos que os consumidores podem optar por usar. Incentivamos a ANPD a continuar apoiando esses esforços.

Entendemos que a ANPD não deve impor proibições absolutas sobre a coleta de determinadas categorias de dados. Dependendo do contexto, um provedor pode ter interesse em realizar a coleta e a retenção de dados com o objetivo de identificar comportamentos inadequados. Para exemplos de iniciativas relacionadas à confiança e à segurança, veja o documento Confiança e Segurança (*Trust and Safety*, em inglês) anexo (Anexo: O setor de videogames prioriza a confiança e a segurança (*The Video Games Sector Prioritizes Trust and Safety*, em inglês)). Ao

invés de limitações específicas, a ANPD deve reforçar o princípio geral de minimização de dados, que estabelece que os provedores devem tratar apenas os dados estritamente necessários para atingir o objetivo comercial.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

Conforme observado na resposta ao item III.3, a indústria de videogames dos EUA desenvolveu configurações de privacidade e controles parentais personalizados que se adaptam aos diferentes contextos em que as empresas de videogames podem tratar informações pessoais e às diferentes funcionalidades dos jogos que as crianças e seus pais ou responsáveis podem optar por usar.

Muitos membros da ESA usam mecanismos como configurações padrão de proteção à privacidade para jogadores menores de idade, incluindo a minimização da coleta de dados, a desativação do bate-papo e de outras comunicações dentro do jogo, a exigência de permissão dos pais para adicionar amigos ou jogar jogos multijogador (*multiplayer*, em inglês) e a desativação da coleta de dados de localização por padrão para aumentar o controle dos pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital. Esses controles parentais geralmente são protegidos por pin ou senhas para garantir que sejam usados apenas pelos pais e não sejam burlados pelas crianças.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Os membros da ESA estão comprometidos em proporcionar aos consumidores transparência e controle sobre suas informações pessoais. Juntamente com seus membros, a ESA tem estado na vanguarda da promoção da privacidade e da segurança dos consumidores, incluindo menores de idade, por quase três décadas. Por meio de práticas voluntárias e em conformidade com a legislação existente, os provedores de videogames fornecem aos jogadores e responsáveis divulgações sobre a coleta de dados que são facilmente acessíveis e escritos de forma clara. Quando apropriado, os avisos de privacidade são adaptados à faixa etária do público, por exemplo, para públicos mais jovens, os avisos são adequados para crianças e escritos em linguagem fácil de entender.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

Conclusão do item III.1 acima. Com base em sua experiência, ESA solicita à ANPD que assegure que qualquer orientação voltada para a proteção de dados pessoais e mitigação de riscos provenientes do uso de plataformas digitais permaneça flexível para acomodar diferenças importantes entre (a) indústrias e contextos, (b) preferências e expectativas razoáveis dos consumidores, (c) ferramentas de privacidade e as configurações de controle parental que já existem nas plataformas (ou seja, se uma empresa desenvolve um jogo que só pode ser jogado em uma determinada plataforma e essa já implementou esses controles de proteção de privacidade, o desenvolvedor do jogo não deveria ter que incorporar esses controles como nativos, pois os jogadores/pais/responsáveis podem acessar esses controles na plataforma) e (d)

em tecnologias em evolução. Essa orientação deve ser consistente com os frameworks globais - GDPR e COPPA.

A ESA agradece os esforços contínuos da ANPD para criar um ambiente seguro e de apoio para as crianças no espaço digital. Como uma das principais partes interessadas nesse espaço, a ESA testemunhou o desenvolvimento de práticas confiáveis no setor que fornecem ferramentas inovadoras para os pais.

As práticas estabelecidas pelos membros da ESA, que provaram ser seguras e adaptáveis, mostraram que a flexibilidade concedida à indústria foi fundamental para promover esses avanços. Essa flexibilidade permite que as empresas continuem evoluindo e criando novas soluções que atendam às necessidades tanto de pais quanto de crianças, ao mesmo tempo em que permanecem alinhadas com os objetivos do marco legislativo de proteção de dados.

Acreditamos firmemente que a inovação contínua nessa área é essencial. Para isso, é fundamental evitar regulamentações excessivamente prescritivas que possam complicar a conformidade à medida que o tempo e a indústria evoluem. Em vez disso, defendemos uma abordagem que promova a inovação e, ao mesmo tempo, garanta a adesão às metas regulatórias.

Apoiamos a abordagem da ANPD de consultar a sociedade sobre esse importante tópico. Pedimos que a ANPD considere a importância de manter uma abordagem flexível ao estabelecer uma orientação voluntária sobre esse importante assunto. A proteção adequada dos dados pessoais de crianças e adolescentes e seu acesso a conteúdo apropriado em plataformas digitais tem sido discutida em várias jurisdições (por exemplo, EUA, Reino Unido, França, Irlanda), especificamente sobre a questão da garantia de idade. Dada a variedade de métodos e tecnologias atualmente disponíveis, a ESA recomenda que a ANPD adote uma abordagem educacional em vez de uma abordagem regulatória para essas questões e evite emitir uma regulamentação formal que poderia exigir uma revisão a cada poucos meses devido às mudanças na tecnologia e nas considerações empresariais sobre os meios mais eficazes e eficientes de promover o processamento de dados com proteção de privacidade.

A ESA solicita que a ANPD (1) publique orientações voluntárias sobre os padrões minimamente aceitos de verificação de idade (por exemplo, (a) uma empresa deve realizar uma avaliação de risco obrigatória do processo pretendido, (b) implementação de medidas eficazes para garantir a minimização de dados) e (2) conduza estudos adicionais e envolva mais partes interessadas em relação à verificação e garantia de idade, promovendo melhores práticas na proteção de dados em plataformas digitais. A ANPD poderá também promover uma cultura de proteção de dados, tomando medidas para envolver pais e responsáveis e incentivá-los a se manterem informados à medida que as práticas evoluem.

A ESA e seus membros estão profundamente comprometidos com os objetivos de proteger os dados de crianças e adolescentes e garantir a transparência, a verificação efetiva da idade, o controle parental e as melhores práticas. Estamos ansiosos para colaborar com a ANPD em sua avaliação de possíveis orientações voluntárias nessas áreas.

Amanda Denton
Consultora Sênior, Políticas Globais
Entertainment Software Association (ESA)

O Setor de Videogames Prioriza a Segurança do Jogador

Por cerca de 30 anos, a indústria de videogames tem sido líder na promoção da segurança dos jogadores. Essa liderança decorre de um forte compromisso de aperfeiçoar continuamente as nossas políticas de apoio à criação de espaços que sejam positivos e acolhedores para todos.

1

A indústria tem uma longa história de sucesso em autorregulação.

No Brasil, o sistema de Classificação Indicativa (Classind), criado em 1990, atribui classificações de faixa etária e conteúdo para jogos eletrônicos. Sob atribuição do Ministério da Justiça, o Classind possui 6 faixas de **Classificação Etária** (livre, não recomendado para menores de 10, 12, 14, 16 e de 18 anos), **Descritores de Conteúdo** para explicar as razões por trás da indicação atribuída, e **Elementos Interativos** para destacar recursos como compras no jogo ou comunicação entre usuários.

O Classind ainda:

- Garante às famílias o direito escolha, fornecendo-lhes insumos.
- Protege a criança e o adolescente contra conteúdos inadequados.
- Define critérios de análise de obras audivisuais.
- Observa os preceitos do Estatuto da Criança e do Adolescente (ECA).

O Classind é membro da International Age Rating Coalition (IARC), uma coalizão composta por autoridades de diferentes países.

2

Os sistemas dos jogos são desenvolvidos para colocar os pais no controle.

Os membros da ESA oferecem aos pais uma variedade de controles para gerenciar o jogo. Os controles para pais, responsáveis e jogadores incluem:

- Filtro por classificação etária
- Gerenciamento do tempo de jogo
- Controle de gastos do usuário
- Limite - ou bloqueio - da comunicação com outros jogadores
- Configurações de senha para prevenir modificações não desejadas
- Relatórios de tempo de jogo

	Nintendo Switch	PlayStation.	XBOX
Contas gerenciadas pelos pais	✔	✔	✔
Bloqueio de gastos	✔	✔	✔
Notificação dos pais sobre gastos	✔	✔	✔
Restrição do tempo de jogo	✔	✔	✔
Restrição da comunicação	✔	✔	✔
Restrição por classificação indicativa	✔	✔	✔

3

As empresas utilizam tecnologia de ponta para proteger ainda mais os jogadores.

Além da autorregulação, do controle parental e de ferramentas nos jogos como silenciar, bloquear e reportar jogadores, as empresas incorporam a segurança na concepção dos jogos e adotam medidas concretas para promover o bom comportamento em seus jogos. Aqui estão apenas alguns exemplos de como empresas de jogos eletrônicos estão trabalhando para manter os jogadores seguros:

A **tecnologia de filtragem de comunicação** detecta conteúdo inapropriado e previne que outros jogadores tenham contato com ele. A **tecnologia *de hash de imagem*** ajuda a combater a exploração infantil criando "impressões digitais" de imagens conhecidas de materiais de abuso infantil, permitindo que as empresas identifiquem rapidamente e impeçam a exibição desse tipo de conteúdo. A indústria também trabalha com o Centro Nacional de Crianças Desaparecidas e Exploradas (NCMEC) – uma entidade sem fins lucrativos norte-americana – e com órgãos de segurança pública norte-americanos para combater imagens e conteúdos inapropriados.

A Epic Games lançou as Contas com Cabine (*Cabined Accounts,* em inglês), contas especiais que oferecem um espaço seguro e inclusivo para jovens jogarem *Fortnite*, *Rocket League* ou *Fall Guys* sem acesso a determinados recursos, tais como bate-papo e compras, até que os seus pais deem o devido consentimento.

O Controle Parental da Epic permite aos pais escolher como os seus filhos jogam e interagem com outros. Esses controles funcionam independentemente ou em adição a restrições já definidas previamente pelos pais. Os pais podem gerenciar configurações de voz, exigir senhas para compras e também solicitar relatórios semanais de tempo de jogo.

O Valorant, da Riot Games, inclui um **recurso de silenciamento automático,** que intercepta linguagem nociva em seus bate-papos antes que ela seja vista por outros jogadores. Jogadores que tentam enviar mensagens abusivas são automaticamente silenciados e informados sobre a perda da capacidade de comunicação no jogo.

Apex Legends, um jogo da Electronic Arts (EA), oferece o Sistema Ping, uma ferramenta interna de comunicação. O Sistema permite que os jogadores se comuniquem de maneira eficaz sem ter que usar bate-papo por voz (*voice chat*, em inglês) (por exemplo, através de dicas visuais na tela). Ao fazê-lo, o Sistema não somente oferece uma **alternativa para os jogadores** que desejam evitar o chat durante o jogo, mas também oferece acessibilidade para jogadores que têm dificuldade de se comunicarem por voz.

O *Call of Duty*, da Activision, lançou um novo **sistema de moderação de bate-papo por voz** para identificar em tempo real linguagem tóxica – incluindo discurso de ódio, linguagem discriminatória, assédio etc. A solução já está disponível na América do Norte para jogadores de língua inglesa *Modern Warfare II* e *Warzone*. Uma expansão global do Sistema (exceto para a Ásia) chegará em novembro de 2023 com o *Modern Warfare III*.

A Ubisoft lançou o seu Programa *Fair Play* ("Jogo Limpo") visando **conscientizar** a comunidade de jogos eletrônicos sobre comportamentos inadequados e ajudar os jogadores a entenderem e superarem comportamentos negativos. O programa consiste em módulos de aprendizado com vídeos, *quizzes* e uma autoavaliação. O Programa também traz entrevistas com um jogador e treinador profissional de *e-sports* (*Rainbow Six Siege*) que falam sobre como o comportamento positivo ajuda a maximizar o potencial da equipe e reforça a competição.

esa entertainment software association

Para mais informações e outros exemplos de como a indústria de videogames está protegendo sua comunidade de usuários, visite theESA.com/trust-and-safety

Proteção dos Dados Sensíveis de Crianças e Adolescentes: Estratégias para um Ambiente Digital Seguro

Chiara Spadaccini de Teffé

Agosto/2024

Sumário:

Introdução.
1. Crianças e adolescentes em ambientes digitais: interações online e exposição nas redes.
2. Qualificação e proteção dos dados pessoais sensíveis de crianças e adolescentes.
3. Instrumentos para a garantia do melhor interesse dos menores no tratamento de suas informações sensíveis.
Considerações finais

Chiara de Teffé é Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Graduada em Direito pela Universidade Federal do Rio de Janeiro. Atualmente, é coordenadora de pesquisa e publicações da pós-graduação em Direito Digital do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a UERJ, e professora de Direito Civil e Direito Digital na faculdade de Direito do IBMEC. Leciona em cursos de pós-graduação e extensão do CEPED-UERJ, da PUC-Rio, da EMERJ e do ITS Rio. Membro Titular do Conselho Municipal de Proteção de Dados Pessoais e Privacidade do Rio de Janeiro. Membro da Comissão de Proteção de Dados e Privacidade da OABRJ. Membro da Comissão de Direito Civil do Conselho Seccional do Rio de Janeiro da OAB. Membro do Fórum Permanente de Liberdade de Expressão, Liberdades Fundamentais e Democracia da EMERJ. Membro do Fórum permanente de inovações tecnológicas no Direito da EMERJ. Foi professora de Direito Civil na UFRJ. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Autora do livro "Dados pessoais sensíveis: qualificação, tratamento e boas práticas". Advogada. E-mail: chiaradeteffe@gmail.com

Como citar o artigo: TEFFÉ, Chiara Spadaccini de. Proteção dos Dados Sensíveis de Crianças e Adolescentes: Estratégias para um Ambiente Digital Seguro. In: FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. 2.ed. revisada e atualizada. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro. 2024. No prelo.

BY NC ND

Atribuição-SemDerivações-SemDerivados
CC BY-NC-ND

Introdução

Conforme os mecanismos de comunicação e interação online avançam, o ambiente digital vem se tornando cada vez mais relevante na vida das pessoas. Nos últimos anos, diversas atividades foram intensificadas nesse ambiente, como cursos e aulas particulares, prestação de serviços governamentais, comercialização de bens e disponibilização de canais de comunicação, entretenimento e jogos. Não há dúvidas de que a Internet, em razão das potencialidades e recursos que oferece, apresenta relevantes oportunidades para crianças e adolescentes. O acesso consciente e equilibrado a tecnologias digitais pode ajudá-los a conhecer, realizar e exigir uma série de direitos garantidos pela Constituição Federal e normas internacionais.

No entanto, resta igualmente importante lembrar que, diante dos diversos sujeitos que interagem no ambiente virtual e das sofisticadas formas de tratamento de dados hoje disponíveis, também se verificam riscos de violações e abusos a crianças e adolescentes. Conteúdos que estimulam violência, automutilação[1] , uso de drogas, vazamento de imagens íntimas[2], tratamentos indevidos de dados pessoais[3], *cyberbullying* e aliciamento sexual são exemplos de riscos significativos a menores na rede e que precisam de grande atenção por parte das famílias, Estados, plataformas digitais e organizações.

A relação das crianças e dos adolescentes com a Internet é marcada pela conectividade e pela mobilidade no acesso à rede, sendo o smartphone um dos principais dispositivos para essa conexão. Segundo a pesquisa *TIC Kids Online Brasil 2023*, 95% da população de 9 a 17 anos é usuária de Internet no país, representando 25 milhões de pessoas. O celular foi apontado como um dispositivo de acesso para 97% dos usuários, sendo o único meio de conexão à rede para 20% dos entrevistados. Outro dado interessante destaca que 88% da população brasileira de 9 a 17 anos disse manter perfis em plataformas digitais, sendo que a proporção foi de 99% entre sujeitos de 15 e 17 anos. Conforme o levantamento, 88% das crianças e adolescentes ouvidos afirmaram ter acesso à plataforma de vídeos YouTube. Já 78% disseram ter WhatsApp, 66% ter Instagram, 63% TikTok e 41% Facebook.[4]

Mostra-se, assim, necessário analisar os diversos instrumentos de proteção a crianças e adolescentes, bem como destacar a importância de um uso ético e

responsável das redes e dos dispositivos conectados. No presente artigo, busca-se analisar a proteção dos dados pessoais sensíveis de crianças e adolescentes, especialmente em contextos digitais, observando-se concretamente desafios e ferramentas de tutela aos seus direitos. Adicionalmente, serão exploradas possibilidades de aplicação e interpretação da Lei Geral de Proteção de Dados brasileira (LGPD - Lei nº 13.709/18) a respeito da temática, com base em entendimentos doutrinários e posições da Autoridade Nacional de Proteção de Dados brasileira (ANPD).

1. Crianças e adolescentes em ambientes digitais: interações online e exposição nas redes

Promover um ambiente seguro e uma educação digital de qualidade para crianças, adolescentes, pais e professores resultará em um melhor e mais saudável uso das redes. Nessa dinâmica, é importante que tanto os responsáveis quanto as plataformas estabeleçam canais abertos com os menores, onde eles se sintam acolhidos o suficiente para tirarem dúvidas e relatarem situações de abuso. Ainda, o *design* de dispositivos direcionados a crianças e adolescentes deve ser informado pelas mais atualizadas pesquisas e práticas nos campos da educação e da tecnologia, sendo centrado por padrão na proteção das informações das crianças e dos adolescentes.

O controle e a mediação parental devem ser aplicados em intensidades compatíveis com as idades das crianças e dos adolescentes, respeitando seus graus de autonomia e discernimento, bem como seus processos individuais de aquisição de competências e entendimentos.[5] Sendo possível e seguro, entende-se adequado conferir determinados espaços de liberdade e privacidade para o adolescente, para que desenvolva sua autonomia e comunicação, tendo os seus pontos de vista devidamente considerados.

Outros instrumentos igualmente relevantes, a depender da idade e da maturidade do menor, são a realização de atividades em conjunto com os pais, o estabelecimento de determinadas limitações quanto ao tempo de uso de tecnologias, a utilização de ferramentas e filtros para restringir atividades dos menores online e o monitoramento de interações diversas realizadas na Internet. Um adequado controle parental, atrelado a uma educação digital de cunho emancipatório, mostra-se essencial para a proteção de crianças e adolescentes. Os primeiros anos de vida da criança são de grande relevância para o seu desenvolvimento cerebral e são

quando o ambiente social se revela crucial para moldar seu desenvolvimento cognitivo, emocional e social.

O ambiente digital deve apoiar e promover um engajamento seguro e equitativo dos menores, sendo relevante o desenvolvimento de políticas e ações que visem a uma efetiva inclusão digital. Caso isso não ocorra, as desigualdades existentes provavelmente aumentarão e outras poderão surgir, como no acesso à educação e à informação. O direito a não discriminação deve garantir que crianças e adolescentes — especialmente meninas[6] — tenham um acesso de qualidade ao ambiente digital. Nesse sentido, mostram-se relevantes políticas públicas que facilitem o acesso a dispositivos conectados, uma internet aberta e serviços digitais. Além disso, com base no direito a não discriminação, deve-se proteger crianças e adolescentes de dados tendenciosos, falsos ou parciais, de tratamentos indevidos ou ilícitos de informações e de perfis voltados ao direcionamento de publicidade.

Todas as ações direcionadas a crianças e adolescentes devem necessariamente visar ao seu melhor interesse, como, por exemplo, no fornecimento, regulamentação, design, gestão e uso do ambiente digital. O reconhecimento e a tutela de sua hipervulnerabilidade[7] podem ser inferidos do artigo 227 da Constituição Federal, o qual dispõe acerca do princípio da prioridade absoluta aos direitos da criança e do adolescente.[8] Caminha, assim, o Direito buscando harmonizar o respeito à capacidade e autodeterminação da pessoa e a necessária proteção jurídica que deve ser conferida a determinados grupos, para que gozem plenamente de seus direitos fundamentais. Longe de uma ótica paternalista, busca-se garantir efetividade e aplicação direta das normas constitucionais.[9]

A construção da doutrina da proteção integral e prioritária das crianças e dos adolescentes, segundo a qual tais pessoas em desenvolvimento devem receber total amparo e proteção do sistema jurídico[10], remonta à *Declaração dos Direitos da Criança* adotada pela Assembleia-Geral das Nações Unidas no ano de 1959.[11] Posteriormente, em 1989, através da *Convenção das Nações Unidas sobre os Direitos da Criança*[12], houve a ampliação dos direitos da criança no cenário internacional. Este documento considerou como criança todo ser humano com menos de 18 anos, salvo quando, conforme a lei aplicável à criança, a maioridade seja alcançada antes.

A referida Convenção foi ratificada pelo Brasil em 1990 e influenciou diretamente a elaboração do *Estatuto da Criança e do Adolescente* (Lei 8.069/90 - ECA), que em seus artigos 3º e 4º destaca que todas[13] as crianças (pessoa com menos de doze anos) e adolescentes (aquela entre doze e dezoito anos de idade incompletos) gozam dos direitos fundamentais inerentes à pessoa humana, sem

prejuízo da proteção integral de que trata esta Lei, assegurados a eles todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.[14]

Ato contínuo, o ECA dispõe que a criança e o adolescente têm direito à liberdade, ao respeito e à dignidade como *pessoas humanas em processo de desenvolvimento* e como sujeitos de direitos civis, humanos e sociais garantidos na Constituição e nas leis (Art. 15). O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais (Art. 17). A lei não menciona expressamente a proteção de dados pessoais dos menores, porém, diante da ampla tutela aplicada, é possível afirmar que o referido direito se encontra contemplado. Observa-se também que eles têm direito à informação, cultura, lazer, esportes, diversões, espetáculos e produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento (Art. 71). Isso é especialmente relevante quando consideramos os novos dispositivos conectados e os serviços disponibilizados na rede, como *games*, mídias sociais e aplicativos interativos.

A tutela diferenciada das crianças e adolescentes em qualquer relação na qual participem justifica-se exatamente por lhes faltar o completo discernimento, estando nesse ponto a *ratio* protetiva. Contudo, deve-se ressaltar que não se trata apenas de uma proteção adequada ao estágio de desenvolvimento em que crianças e adolescentes se encontram, mas de uma proteção prospectiva, a fim de garantir a dignidade deles hoje e no futuro.[15] Temos, nos últimos tempos, a geração mais observada de toda a história. Cada vez mais, o *rastro digital* de menores vem sendo iniciado mais cedo e de forma ampliada, seja por meio de aplicativos para serem usados pelas mães durante a gestação, seja por meio de postagens realizadas pelos próprios pais, em mídias sociais, ainda quando nascituros.

Diante disso, cabe recordar aqui a questão do *oversharenting*: hábito de os pais postarem constantemente e de forma intensa imagens e informações pessoais de seus filhos nas redes.[16] Abarca também situações em que os pais fazem a gestão da vida digital de seus filhos na internet, criando perfis em nome das crianças em redes sociais e postando sempre e em detalhes dados sobre sua rotina. Pesquisas apontam que essa intensa exposição dos menores estaria causando uma verdadeira mudança na caracterização da infância, de forma que a nova geração já cresceria com responsabilidades, anseios e expectativas de uma vida adulta. Ocorre também, nesse cenário, comumente, a divulgação da família e dos filhos menores pelos chamados

"influenciadores digitais", os quais conjugam tal exposição com a divulgação e promoção de marcas, produtos e serviços.

Recomenda-se, portanto, que antes da publicação de conteúdos que envolvam os menores, os responsáveis reflitam criticamente acerca das consequências de suas ações. Além disso, mostra-se relevante incluí-los no processo decisório sobre o que será postado sobre eles nas redes, de forma a educá-los sobre segurança, privacidade e consentimento online.[17] *Oversharenting* pode trazer sérios impactos emocionais e psicológicos às crianças. Dentro das consequências negativas, é possível elencar: bullying em ambientes coletivos; invasão de senhas, falsificação de identidade e fraudes variadas; dificuldade de conseguir vaga de estágio ou mesmo crédito em instituições bancárias; e ser alvo de manipulação (política, comercial ou para qualquer fim de controle). Há, inclusive, uma preocupação acerca das consequências (presentes e futuras) da construção de uma memória pública e de um registro amplo de eventos e momentos que envolvam diretamente menores de idade.

Outro tema que permeia os debates envolve a chamada *Internet dos brinquedos*, com bonecas, bichinhos de pelúcia e robôs conectados e inteligentes.[18] Ela se insere no amplo universo da Internet das Coisas (*Internet of Things*), que representa a integração de objetos físicos e virtuais em redes conectadas à Internet, permitindo que "coisas" tratem uma enorme quantidade de dados em nuvem, sendo possível o gerenciamento de dispositivos, mesmo à distância, para aumentar a eficiência de sistemas e processos. Tais brinquedos podem ser controlados por meio de aplicativos de smartphone, comandos de voz ou conexão Bluetooth. Os dados tratados através desses recursos podem variar desde detalhes pessoais, como idade ou localização do usuário, até conteúdos obtidos por microfones e câmeras, que farão o registro do que os usuários veem e ouvem.

Cada vez mais, percebe-se a incorporação da IOT na vida de adultos, adolescentes e crianças. Relógios, geladeiras, leitores de digitais, vibradores sexuais, detectores de movimento, câmeras, peças de vestuário e brinquedos já se encontram conectados à Internet e presentes nas casas e corpos das mais diversas pessoas, enquanto empresas coletam dados sobre movimentos, preferências, comportamentos e hábitos de seus usuários, que não têm, por vezes, nem mesmo plena capacidade civil.

Dentro da *Internet of Toys*, despontam questões acerca: a) da falta de transparência e informação sobre o tratamento de dados de menores; b) do compartilhamento expressivo de dados com terceiros; c) da ausência de adequação das instituições à LGPD e às boas práticas internacionais em proteção de dados; d)

de tratamentos indevidos de informações pessoais de terceiros presentes na residência, como pais, visitantes e amigos, sendo o brinquedo, por vezes, considerado um verdadeiro dispositivo de vigilância; e) da exposição excessiva da intimidade e de dados sensíveis do menor, a partir da coleta de informações, da interação realizada e das respostas oferecidas pela criança; e f) da qualidade do conteúdo direcionado a quem interage com os dispositivos, tendo em vista a possibilidade de inserção de publicidade implícita de bens durante as interações dos brinquedos com as crianças.

Adicionalmente, ainda na seara relativa à proteção de dados, há sérias preocupações acerca da segurança e da proteção da integridade dos menores. Questiona-se, por exemplo: como fica a responsabilidade dos agentes em casos de incidentes de segurança e de danos? Quais padrões éticos e boas práticas eles deveriam adotar? Como mapear e sanar riscos e vulnerabilidades? O hackeamento de dispositivos, a reidentificação de dados anonimizados, o rastreamento de indivíduos e o *profiling* mostram-se presentes em diversas estruturas de tratamento de dados de crianças e adolescentes. Por fim, destaca-se também o impacto que a relação com o brinquedo conectado pode gerar nas formas de comunicação, interação e expressão das crianças.[19]

Outro tema que vale recordar quando se trata da proteção de crianças e adolescentes em ambientes digitais envolve a idade mínima para o uso de mídias sociais.[20] Como regra, as principais mídias sociais estabelecem, nos termos de uso apresentados no Brasil, a idade mínima de 13 anos para a abertura de contas e a utilização de seus serviços. Ou seja, permitem que adolescentes no Brasil tenham perfis em suas plataformas. Essa determinação tem como base norma norte-americana que considera criança o indivíduo com menos de 13 anos: o *Children's Online Privacy Protection Act* de 1998 (COPPA).[21]

Na Europa, nos termos do artigo 8º do *General Data Protection Regulation* (GDPR), a idade de consentimento, ou seja, quando uma pessoa pode ou é capaz de consentir acerca do tratamento dos seus dados, é de 16 anos, por padrão. No entanto, os Estados-Membros podem determinar a sua idade de consentimento, sendo a idade mínima de 13 anos.[22] No Reino Unido, por exemplo, a idade de consentimento é de 13 anos. Mais recentemente, no ambiente europeu, o *Digital Services Act* (DSA) visou criar um ambiente digital mais seguro e incluiu disposições para reforçar a proteção de menores. Assim, todos os fornecedores de plataformas acessíveis a menores na União Europeia deverão implementar medidas adequadas

e proporcionais para garantir um elevado nível de privacidade, segurança e proteção a esse grupo nos seus serviços.

Tanto a LGPD quanto o GDPR determinam que o responsável pelo tratamento deverá promover todos os esforços razoáveis para verificar se o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais sobre a criança, tendo em conta a tecnologia disponível.[23] O uso de linguagem clara e acessível para os menores nas plataformas também é sempre recordado.[24]

No momento pandêmico, o uso de redes sociais foi substancialmente alargado em razão de *trends* virais, desafios, filtros e práticas de unboxing, o que motivou, inclusive, que crianças buscassem tais plataformas, mesmo diante da vedação de sua presença nos termos de uso. Mas como evitar que crianças acessem serviços e conteúdos inadequados para a sua idade em mídias sociais? Quais mecanismos podem ser utilizados para se verificar a idade real dos sujeitos/usuários?[25]

Atualmente, a autodeclaração do usuário tem se mostrado falha e suscetível a fraudes, exigindo a aplicação de novos parâmetros, como garantia de idade por meio da solicitação de documentos oficiais (como o CPF e o número de um cartão de crédito), identificação com uso de biometria, modelos baseados em *profiling* e inferências, teste de capacidade/aptidão, autenticação entre contas, verificação de idade por serviço de terceiro (*third party age assurance provider*), confirmação dos dados do titular da conta por um adulto, análise de denúncias de terceiros e inserção de controles no próprio dispositivo ou sistema operacional para oferecer experiências mais apropriadas à idade das crianças.

Contudo, será a idade de 13 anos já adequada para o uso desacompanhado de mídias sociais? Proibir ou controlar diretamente o uso seria a solução? As referidas questões desafiam pesquisadores e pais, devendo ser analisadas caso a caso, conforme as características, a autonomia e o discernimento do menor. As diversas e dinâmicas relações desenvolvidas na Internet, que envolvem tratamentos de dados e, por vezes, sua monetização e utilização para fins comerciais, nem sempre são adequadamente compreendidas por adolescentes. Além disso, durante a adolescência o sujeito não goza ainda de plena capacidade civil (a menos que seja emancipado aos 16 anos), o que traz questionamentos acerca da validade do consentimento manifestado em termos de uso, contratos e ferramentas online.

Isso nos faz refletir sobre o processo de tomada de decisões na Internet e a respeito das escolhas jurídicas para a proteção de crianças e adolescentes,

compreendidos em caráter concreto e dentro de sua multiplicidade. A análise do discernimento e da maturidade do sujeito se mostra fundamental, pois, ainda que o critério etário seja importante, ele não deverá ser em todos os casos único e absoluto.

2. Qualificação e proteção dos dados pessoais sensíveis de crianças e adolescentes

A cada segundo, uma infinidade de dados pessoais é extraída, transferida e organizada nos mais variados meios de comunicação e de prestação de serviços. Logins em sites, identificação pessoal por biometria e a utilização de mídias sociais e de objetos conectados fornecem dados pessoais a diversos destinatários sem que, muitas vezes, seja possível ao titular controlar efetivamente a finalidade da utilização de suas informações e quem realizará o tratamento delas.[26]

Conforme aumentam o grau de exposição dos indivíduos e a sua sujeição a estruturas tecnológicas, verifica-se a relevância de serem desenvolvidos instrumentos que coloquem os direitos à proteção de dados e à privacidade em posição de preeminência em face de situações patrimoniais. Nesse sentido, certas categorias de dados – pela sensibilidade e pela qualidade das informações que guardam – deverão receber garantias ampliadas, não devendo ser utilizadas para fins meramente negociais.[27]

A LGPD, ainda que não defina expressamente o que são dados sensíveis, apresenta em seu Art. 5º, inciso II, dados assim considerados, como aqueles que versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São também sensíveis informações pessoais referentes à saúde ou à vida sexual e dados genéticos ou biométricos.[28] A legislação brasileira seguiu, em grande parte, a noção europeia de dados sensíveis, estabelecida em 2016 pelo GDPR, e expandiu o rol de informações sensíveis já desenvolvido pela Lei do Cadastro Positivo (Lei n. 12.414/11).[29]

Mas o que torna um dado pessoal um dado sensível? Quais fundamentos legitimam a categoria? Costuma-se fundamentar o estabelecimento dessa categoria especial de dados com base nos princípios do livre desenvolvimento da personalidade[30] e da não discriminação.[31]

Ao se afirmar a relevância do livre desenvolvimento da personalidade, entende-se que cada pessoa deve eleger o seu modo de vida, podendo desenvolver e expor,

amplamente, seu projeto pessoal. [32] Garante-se autonomia para que cada um constitua sua personalidade de forma livre, sem qualquer imposição ou interferência de terceiros, havendo tanto um direito à individualidade quanto um direito à diferença. O papel do ordenamento deve ser o de garantir à pessoa humana espaço para o desenvolvimento de suas escolhas, em todas as fases da vida, sabendo-se que de toda liberdade decorrerão também responsabilidades. Ao se tutelar os dados pessoais, são resguardadas diretamente a liberdade, a igualdade e a integridade, tanto dos indivíduos quanto das coletividades.

Nesse sentido, a proteção dos dados sensíveis mostra-se especialmente relevante para a garantia dos direitos e liberdades fundamentais de seu titular, devendo ser protegidos de forma mais específica e cuidadosa pelas diversas estruturas normativas.[33] Isso porque, em virtude da qualidade e da natureza das informações que trazem, seu tratamento ou eventual vazamento poderá gerar riscos significativos à pessoa humana, podendo ser fonte para preconceitos e discriminações ilícitas ou abusivas.[34]

Verifica-se na categoria em questão importantes conteúdos relacionados à intimidade, à identidade e à integridade psicofísica da pessoa natural, cabendo a ela determinar a gestão de sua esfera informacional. Há, inclusive, informações sensíveis que integram a esfera pública em que se encontra seu titular, constituindo as convicções que ele deve poder manifestar publicamente e que fazem parte de sua identidade pública.[35] Nas palavras de Rodotà,

> (...) dados sensíveis são aqueles relativos à saúde e vida sexual, às opiniões e ao pertencimento étnico ou racial, com uma lista semelhante às encontradas nas normas relativas a casos de discriminações. Assim, somos confrontados com algo que vai além da simples proteção da vida privada e se apresenta como defensor da mesma igualdade entre as pessoas.[36]

A seleção sobre quais dados são sensíveis demonstra que a circulação de determinadas informações pessoais pode acarretar maior potencial lesivo aos seus titulares, em uma determinada configuração social e política. Diante disso, a compreensão sobre os mecanismos que devem ser empregados na tutela de dados sensíveis perpassa um entendimento substancial sobre as dinâmicas discriminatórias articuladas nas sociedades.

Não há dúvidas de que o tratamento de dados pessoais sensíveis por parte, por exemplo, de empregadores[37], recrutadores, companhias de seguro, planos de saúde e governos demanda uma proteção ampliada, diante dos potenciais riscos a direitos. Outro ponto de preocupação é o desenvolvimento contínuo de análises e perfis comportamentais[38], visando-se direcionar e personalizar com elevada precisão bens e serviços.

O direito constitucional brasileiro compreende a afirmação do direito à igualdade como mandamento de proibição de discriminação. Almeja-se, assim, "(...) afastar toda e qualquer diferenciação injusta, em especial práticas e regimes de subordinação contra indivíduos e grupos histórica e socialmente injustiçados e vítimas de preconceito."[39] Na Constituição Federal de 1988 foi estabelecido que é objetivo fundamental da República a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. Isso resultou na formulação de um "direito da antidiscriminação".***[40]***

O princípio da não discriminação – relevante fundamento para a tutela ampliada dos dados sensíveis – aparece na LGPD duas vezes: na primeira, no inciso IX do art. 6º, que o conceitua como "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos", e na segunda, no § 2º do art. 20, que prevê a possibilidade de a Autoridade Nacional de Proteção de Dados realizar auditoria para a verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.[41]

O fundamento comum para a proteção dos dados pessoais sensíveis gira em torno da necessidade de se evitar formas prejudiciais, ilícitas ou abusivas de discriminação em face dos titulares de dados.[42] Dessa forma, o tratamento de dados sensíveis deve vir acompanhado de garantias adequadas, que considerem os riscos em jogo e os direitos a serem protegidos, como, por exemplo, bases legais específicas e mais restritas (como o art. 11 da LGPD) [43]; obrigações de sigilo profissional; análises de risco; desenvolvimento de relatórios de impacto à proteção de dados; e medidas técnicas e de segurança organizacional específicas. Cuidados adicionais para a proteção de dados sensíveis são essenciais para o seu regular tratamento, uma vez que a tônica de sua tutela é "permitir uma igualdade substancial no tratamento dos dados, vedando a discriminação e o abuso que dele podem surgir."[44]

Como se sabe, a depender da base de dados utilizada para treinar o algoritmo e/ou de como ele foi programado, poderá ser apresentado um resultado discriminatório e enviesado, o que se mostra especialmente preocupante em situações que envolvem segurança pública, tutela da saúde, concessão de crédito e processos seletivos. Inclusive, é importante lembrar que, diante dos avanços tecnológicos e científicos, até mesmo informações pessoais que tradicionalmente não são classificadas como sensíveis - como nome, idade, localização, nacionalidade, dados financeiros e endereço de domicílio - podem causar "tanto (i) um tratamento discriminatório em si quanto (ii) a dedução ou inferência de dados sensíveis obtidos a partir de dados pessoais não sensíveis."[45]

Decisões que, até pouco tempo, eram tomadas exclusivamente por seres humanos vêm sendo delegadas – no todo ou em parte – para sistemas automatizados, algoritmos de ranking e modelos de risco preditivo, que, por sua vez, acabam controlando desde a concessão de crédito a uma pessoa até quem tem mais chances de delinquir, com base na análise computadorizada de estatísticas.[46] Percebe-se, assim, o potencial de algumas decisões automatizadas de violarem direitos fundamentais, se tomadas sem o cumprimento de determinados parâmetros éticos e constitucionais, que garantam sua transparência, possibilidade de controle e segurança. [47]

Nesse contexto, alude-se ao tratamento conferido ao tema na LGPD, que previu o direito de o titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Segundo parte da doutrina, o artigo 20 da LGPD[48] seria, em certa medida, a sede do "direito à explicação"[49], o qual derivaria do princípio da transparência para o tratamento de dados pessoais.

Diante do atual cenário tecnológico, marcado pelo amplo uso de inteligência artificial e em um contexto de web 4.0, não mais parece fazer sentido considerar um dado ou um conjunto de dados pessoais de forma isolada e estática, mas sim dentro de uma perspectiva dinâmica e funcional, que considere diversos fatores, qualidades dos titulares dos dados e possibilidades de tratamentos e inferências. Há cada vez mais formas de análises que podem identificar indivíduos e revelar dados sensíveis sobre eles.

Justamente por isso, mostra-se fundamental avaliar toda relação de tratamento de dados observando-se: (I) a natureza e as características da informação pessoal, além do contexto que determina seu tratamento; (II) interesses específicos do responsável pelo tratamento, assim como dos destinatários potenciais dos dados; (III) finalidade e propósito para os quais os dados serão tratados; (IV) condições do tratamento; (V) relações que podem ser estabelecidas com as demais informações disponíveis sobre o titular e/ou o grupo de que ele faz parte; (VI) as possibilidades tecnológicas atuais e futuras envolvendo dados; (VII) como a informação pode afetar o indivíduo a quem ela diz respeito e o livre desenvolvimento de sua personalidade; e (VIII) a potencialidade do tratamento do dado servir como instrumento de estigmatização ou discriminação ilícita ou abusiva da pessoa.[50]

Quanto ao titular do dado pessoal, merecem atenção suas características e eventuais vulnerabilidades, em uma perspectiva protetiva. Conforme enunciado

aprovado na I Jornada de Direitos Humanos e Fundamentais da Justiça Federal da 2ª Região, ocorrida em abril de 2024, no Rio de Janeiro: "A hipervulnerabilidade do titular de dados pessoais deverá ser considerada para ampliar a proteção conferida a tais dados, especialmente quando se tratar de crianças, adolescentes, idosos e pessoas com deficiência." Como aponta a orientação, parece adequado refletir acerca de garantias e instrumentos de segurança adicionais a certos dados pessoais, especialmente quando eles disserem respeito a pessoas hipervulneráveis. Isso fica ainda mais evidente diante de dados pessoais sensíveis – como genéticos, de saúde, biométricos e raciais – de crianças e adolescentes, titulares que apresentam uma vulnerabilidade agravada. A intensificação da suscetibilidade de dano no caso de menores provém de razões como a idade reduzida e a falta de experiência e discernimento completo.

As doutrinas do melhor interesse e da proteção integral de crianças e adolescentes informam diretamente a tutela dos dados pessoais desses sujeitos. Nesse caso, não se trata apenas de uma proteção adequada ao estágio de desenvolvimento em que crianças e adolescentes se encontram, mas de uma proteção prospectiva, a fim de garantir a dignidade deles hoje e no futuro.

A combinação de vários conjuntos de dados pode aumentar a probabilidade de conclusões de natureza sensível, bem como propiciar cenários para possíveis discriminações ilícitas contra indivíduos e grupos. Em ambientes cada vez mais interconectados, isso pode envolver considerar não apenas dados que estejam diretamente com o controlador, mas também dados que ele possa acessar em outros ambientes. Diante disso, o contexto específico de um tratamento deverá, como regra, ser compreendido de forma dinâmica e mutável. O tratamento de dados que no passado não foi considerado sensível pode muito bem ser assim considerado no futuro.

Conclui-se, assim, que não se mostra possível definir, antecipadamente e de forma absoluta, os efeitos de um tratamento de informações pessoais. Por exemplo, dados que pareçam não relevantes em determinado momento, que não façam referência a alguém diretamente ou, ainda, que não sejam formalmente sensíveis, uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações, inclusive, de caráter sensível sobre ela. Em importante ensinamento, Danilo Doneda destaca que:

> A elaboração desta categoria e de disciplinas específicas a ela aplicadas não foi isenta de críticas, como a que afirma que é impossível, em última análise, definir antecipadamente os efeitos do tratamento de uma informação, seja ela da natureza que for. Desta forma, mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas

> discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo. (...) deve-se ter em conta que o próprio conceito de dados sensíveis atende a uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos. [51]

Além disso, o conteúdo de comunicações pode revelar informações altamente sensíveis sobre as pessoas envolvidas[52], desde experiências pessoais e emoções até condições médicas, preferências sexuais e visões políticas, comunicações essas que hoje ocorrem cada vez mais cedo, havendo crianças conectadas e transmitindo conteúdos desde os seus primeiros passos. Da mesma forma, metadados derivados de comunicações eletrônicas também podem revelar informações muito pessoais. Números chamados, os sites visitados, a localização geográfica e a data e a duração de uma chamada são informações que permitem tirar conclusões precisas sobre a vida privada das pessoas, como suas relações sociais, seus hábitos, atividades da vida cotidiana e seus interesses e gostos.

As complexas e variadas formas de tratar dados pessoais exigem o estabelecimento de novas categorias, relações e tutelas, especialmente quando envolvem crianças e adolescentes. Diante disso, mostra-se fundamental definir critérios e garantias que ampliem a tutela oferecida a dados sensíveis e a tratamentos que revelem informações sensíveis de menores, considerando-se a necessária aplicação da doutrina do melhor interesse e da proteção integral.

3. Instrumentos para a garantia do melhor interesse dos menores no tratamento de suas informações sensíveis

Em 2019, a Autoridade de Proteção de Dados Sueca[53] multou um município em aproximadamente 20.000 euros por usar tecnologia de reconhecimento facial para monitorar a frequência de alunos em escola.[54] A Autoridade entendeu que a escola havia tratado dados biométricos ilegalmente e que deveria ter realizado uma avaliação de impacto adequada, além de consulta prévia à Autoridade. A escola baseou o tratamento na base legal do consentimento, mas a Autoridade considerou que essa não seria uma base válida, dado o claro desequilíbrio entre o titular dos dados e o responsável pelo tratamento.

Em 2020, o Presidente do Gabinete Polonês de Proteção de Dados Pessoais aplicou uma multa de 20.000 PLN por uma violação de dados que consistia no tratamento de informações biométricas de menores para a utilização de cantina escolar.[55] A escola estava tratando categorias especiais de dados (dados biométricos) de 680 crianças, quando, na verdade, poderia usar outros recursos menos invasivos para identificar os alunos. Por essa violação, uma multa administrativa foi imposta à Escola Primária nº 2 em Gdansk. Além disso, foram ordenados o apagamento dos dados pessoais relativos às impressões digitais das crianças e a cessação de qualquer nova coleta de dados.

Foi apurado que a escola utilizava um leitor biométrico na entrada da cantina escolar para identificar as crianças e verificar o pagamento (ou não) da taxa de alimentação. Ela obtinha os dados e os tratava com base no consentimento por escrito dos pais ou responsáveis legais. A solução estava em vigor desde 1 de abril de 2015. No ano letivo de 2019/2020, 680 alunos utilizaram o leitor biométrico, enquanto quatro alunos usaram sistema de identificação alternativo.

Ressaltou-se que o tratamento de dados biométricos não era essencial para se atingir o objetivo de identificar o direito de uma criança ao almoço. A escola poderia realizar a identificação por outros meios que não interferissem tanto na privacidade da criança. Inclusive, de forma alternativa, a própria escola possibilitava a utilização dos serviços da cantina por meio de cartão eletrônico ou através da indicação do nome e do número do contrato. Contudo, de acordo com o regulamento, os alunos que não possuíam identificação biométrica deveriam aguardar no final da fila até que todos os alunos com a referida identificação entrassem na cantina. Na opinião da Autoridade, tais regras introduziam um tratamento desigual aos alunos e sua diferenciação era injustificada, pois favorecia claramente os alunos com identificação biométrica. Além disso, a utilização de dados biométricos, tendo em conta a finalidade para a qual eram processados, era significativamente desproporcional.

O Presidente da Autoridade destacou que os menores necessitam de especial proteção em relação aos seus dados pessoais. O sistema biométrico identifica características que não estão sujeitas a alterações, como no caso dos dados dactiloscópicos. Devido ao caráter único e permanente dos dados biométricos, eles devem ser usados com o devido cuidado, pois seu possível vazamento pode resultar em um alto risco para os direitos e liberdades das pessoas naturais.

No Brasil, em março de 2024, a rede social TikTok foi condenada, em primeira instância, na vara de Interesses Difusos e Coletivos de São Luís/MA, a pagar danos morais coletivos no valor de R$ 23 milhões de reais ao FPDC - Fundo Estadual de

Proteção e Defesa dos Direitos do Consumidor - e R$ 500 reais, a todos os clientes da plataforma, no território nacional, que provem a condição de usuários até a data da atualização da Política de Dados que incluiu a possibilidade de captura de dados biométricos (junho de 2021). O magistrado entendeu, no caso, que a captura de biometria facial, sem autorização dos usuários, configurava violação de direitos e de dados sensíveis. Vale lembrar que na plataforma há usuários, inclusive, a partir de 13 anos de idade (sem contar as crianças que burlam as regras da plataforma e mantém as suas contas ativas).

A ação coletiva foi movida pelo IBEDEC/MA (Instituto Brasileiro de Estudo e Defesa das Relações de Consumo) que apontou violação de dados e ofensas à privacidade, intimidade, honra e imagem por parte do TikTok. O instituto, que alega ter recebido diversas reclamações de usuários da plataforma, afirmou que o TikTok coletaria, armazenaria e compartilharia, sem autorização, a biometria facial dos clientes.

No caso, o magistrado entendeu que o TikTok desrespeitou a inviolabilidade da vida privada, intimidade, honra e imagem, além de dispositivos do Marco Civil da Internet, da LGPD e do Código de Defesa do Consumidor. Pontuou que provas nos autos indicaram que o TikTok, apesar de negar a coleta da biometria facial, firmou acordo com o governo dos Estados Unidos, no valor de U$ 92 milhões, para findar demandas judiciais que tratavam de violações à privacidade de seus usuários, entre as quais, captura de biometria facial.[56]

Ademais, o magistrado ressaltou que, em junho de 2021, a plataforma atualizou sua política de privacidade para incluir a possibilidade de coletar automaticamente dados faciais e da voz dos usuários, à revelia do consentimento dos clientes. Para o juiz, apesar de o TikTok tentar diferenciar detecção e reconhecimento facial, todas as imagens captadas pelo aplicativo deveriam ser tratadas como dados biométricos, pois, do ponto de vista dos usuários e de autoridades reguladoras, haveria grande dificuldade em distinguir as abordagens e determinar quais usos seriam feitos pelo provedor. Em sua decisão, o magistrado afirmou:

> No presente caso, estabelece-se que a mera coleta não autorizada de dados biométricos (sensíveis) causa dano moral. Portanto, diante da violação do dever de informação e do direito à autodeterminação informativa do titular dos dados, o dano moral é presumido, pois a coleta não autorizada de dados biométricos gera, por si só, um abalo à dignidade e à intimidade do indivíduo. Assim, é justificável reconhecer o dano moral *in re ipsa* em casos de coleta indevida de dados biométricos, como no presente caso. Quanto ao dano moral coletivo, enquanto categoria autônoma de dano, caracteriza-se por lesão grave, injusta e intolerável a valores e interesses fundamentais da sociedade, independentemente da comprovação de prejuízos concretos ou de efetivo abalo moral (...).

Na hipótese, após responsabilizar a empresa com base no artigo 14 do Código de Defesa do Consumidor, o magistrado determinou ainda que ela não mais realizasse a coleta e o compartilhamento de dados biométricos de seus usuários sem o necessário consentimento deles; explicitasse ao usuário de que forma o consentimento estaria sendo obtido no procedimento de adesão ao ecossistema do programa; implementasse ferramenta operacional para obter o consentimento dos usuários da plataforma (podendo eles autorizar ou não a coleta de dados biométricos); e excluísse os dados biométricos coletados ilegalmente sem o consentimento dos usuários.[57]

Cabe lembrar que, em agosto de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) brasileira encaminhou à empresa ByteDance, responsável pelo TikTok, uma nota técnica em que recomendou a revisão de sua política de privacidade e dos mecanismos de verificação de idade usados pela rede social. O documento cobrou que o TikTok impedisse o cadastro de menores de 13 anos; informasse as diferenças de tratamento entre os dados pessoais de adultos e de crianças e adolescentes; e garantisse que os menores de 18 anos tivessem representação ou assistência do responsável ao aderirem à rede social.

Esses casos ilustram situações que envolvem tratamentos indevidos de dados pessoais sensíveis de crianças e de adolescentes e como as autoridades – sejam elas administrativas ou judiciais – ao longo do mundo vêm rechaçando comportamentos abusivos e lógicas discriminatórias. Atualmente, 160 países já adotaram normas voltadas à proteção da privacidade e dos dados pessoais. Em quase todos eles, há uma comissão/autoridade de proteção de dados que supervisiona e aplica as respectivas leis.[58] Há, portanto, sistemas protetivos aos dados pessoais se consolidando a nível global, havendo em seu bojo preocupações específicas que envolvem o tratamento de dados de crianças e adolescentes.

Aplicar uma proteção ainda maior a dados sensíveis de crianças e adolescentes requer uma série de instrumentos jurídicos e técnicos, além do estabelecimento de boas práticas. Contar com o comprometimento de instituições públicas e privadas no tema também é de suma importância, havendo tanto a aplicação de severas sanções, por descumprimento das normas de proteção de dados, quanto a adequada orientação dos agentes por meio da publicação de guias e instruções. Nesse sentido, vale recordar os excelentes posicionamentos já estabelecidos pela Autoridade irlandesa de proteção de dados, por meio do *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*[59]; pela Autoridade do Reino Unido (*Information Commissioner's Office* - ICO)[60] , por

meio do *Age appropriate design code*[61]; e pela Autoridade Francesa de Proteção de Dados[62].

Recorda-se também o Código Holandês para os Direitos da Criança e do Adolescente (*Dutch Code for Children's Rights*), elaborado pela Universidade de Leiden e pela organização Waag, a partir de encomenda do Ministério Holandês de Assuntos Internos e Relações do Reino.[63] O Código ajuda desenvolvedores e designers a se concentrarem nos direitos das crianças e dos adolescentes ao desenvolverem serviços digitais. Ele é composto por dez princípios, quais sejam: Princípio 1: Faça do melhor interesse da criança a principal consideração ao projetar; Princípio 2: Envolva as crianças e suas expectativas no processo de design; Princípio 3: Garanta o processamento legítimo de dados pessoais de crianças; Princípio 4: Forneça transparência de forma compreensível e acessível às crianças; Princípio 5: Realize uma avaliação do impacto na privacidade com base nos direitos das crianças; Princípio 6: Forneça um design de privacidade adequado para crianças. Não processe mais dados pessoais do que o estritamente necessário para atingir o objetivo específico do serviço. Inclua privacidade no design e torne as configurações padrão mais amigáveis à privacidade; Princípio 7: Impeça a criação de perfis de crianças. A criação de perfis de usuários é uma forma de tratamento de dados de alto risco; Princípio 8: Evite a exploração econômica de crianças em todos os momentos; Princípio 9: Sempre evite um design prejudicial para crianças. Um serviço digital pode ser prejudicial para crianças se o design abusar da vulnerabilidade delas ou não as proteger adequadamente contra possíveis conteúdos e comportamentos prejudiciais; e Princípio 10: Desenvolva diretrizes do setor voltadas para a proteção dos interesses e direitos das crianças.

Aplicações que envolvam o tratamento de dados de crianças e adolescentes necessitam ser desenvolvidas a partir de orientações que considerem, especialmente, princípios e valores éticos, a lógica do *privacy by design*[64], a feitura de relatórios de impacto à proteção de dados pessoais e medidas técnicas de prestação de contas. A privacidade por *design* garante que os dados pessoais sejam protegidos automaticamente, por padrão, em qualquer sistema de TI ou prática comercial. Assim, alguns procedimentos deverão ser priorizados, como, por exemplo, a minimização dos dados tratados, a anonimização deles (quando possível) e o uso de ferramentas tecnológicas capazes de dar transparência aos critérios utilizados para a tomada de decisões.

De modo a ampliar as garantias aos dados sensíveis e a afirmar a relevância do princípio da não discriminação nas atividades de tratamento, recorda-se que na LGPD o titular dos dados poderá revogar o consentimento manifestado (Art. 18, IX)

ou pleitear o direito à oposição (Art.18 §2º) quando o tratamento ocorrer com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. Ainda, o agente deverá certificar-se de estar tratando apenas o mínimo necessário de dados sensíveis (princípio da necessidade). Devido às restrições legais, havendo dúvidas sobre a necessidade da informação, a solução mais adequada será a sua não coleta ou, se já coletada, a sua eliminação.[65] Outro princípio relevante é o da prevenção, o qual preconiza a adoção de medidas técnicas, organizacionais e jurídicas para prevenir a ocorrência de danos em virtude do tratamento de dados.

Devem ser documentados, de forma ampla, os tratamentos que envolverem dados sensíveis de crianças e adolescentes, as técnicas adotadas e as estruturas de compartilhamento e descarte empregadas. No Brasil, o relatório de impacto à proteção de dados pessoais[66] (RIPD) é claramente considerado uma boa prática em tais relações e representa instrumento de conformidade e prestação de contas. Ele representa uma documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar *alto risco* à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco.

Segundo a ANPD, por "alto risco", para fins de elaboração do RIPD, os controladores podem, no que couber, adotar como parâmetro o conceito de tratamento de alto risco definido no art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022. De acordo com esse dispositivo, o tratamento será de alto risco se verificada, no caso concreto, a presença de, ao menos, um critério geral (“larga escala” ou “afetar significativamente interesses e direitos fundamentais dos titulares”) e de um critério específico (“uso de tecnologias emergentes ou inovadoras”, “vigilância ou controle de zonas acessíveis ao público”, “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais” ou “utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos”).

Considerando esses critérios, recomenda-se elaborar o RIPD se o tratamento de dados pessoais abranger número significativo de titulares (critério geral) e dados pessoas sensíveis (critério específico). Outro exemplo que pode ser mencionado é a decisão tomada unicamente com base em tratamento automatizado de dados pessoais (critério específico), da qual possa resultar a negativa para o exercício de um direito ou para a utilização de um serviço (“afetar significativamente interesses e direitos”, critério geral).

Da mesma forma, autoridades de proteção de dados europeias vêm afirmando a necessidade de se desenvolver um relatório de impacto para tais relações. A Agência Espanhola de Proteção de Dados destaca que precisarão de avaliação de impacto: "Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia."[67] Ela lista também diversos tratamentos que envolvem dados pessoais sensíveis. O "Age appropriate design" do Reino Unido entende que se deve realizar um DPIA (*Data Protection Impact Assessment*) [68] para avaliar e mitigar os riscos aos direitos e liberdades das crianças que provavelmente terão acesso aos serviços ali mencionados. Afirma-se também que o agente deverá levar em consideração as diferentes idades, capacidades e necessidades de desenvolvimento dos menores, além de se certificar de que seu DPIA seja elaborado em conformidade com o referido código.

No cenário brasileiro, quando se advoga pela ampliação das bases legais para o tratamento de dados pessoais de crianças e adolescentes, o relatório de impacto à proteção de dados pessoais representa uma das ferramentas importantes para a tutela dos menores. Conforme dispõe o artigo 14 da LGPD, o pilar central e inegociável em todo tratamento de dados será sempre o melhor interesse da criança e do adolescente. Contudo, levando em conta as práticas de agentes públicos e privados, bem como a experiência europeia positivada no GDPR, expandir o rol de bases legais mostra-se uma tese possível e por vezes necessária nas complexas e múltiplas relações que envolvem tratamentos de dados.

Como se depreende da leitura do artigo 14, o consentimento[69] é uma das bases legais para o tratamento de dados de crianças e adolescentes, mas não a única. Entende-se que podem ser aplicadas, além das normas do Art. 14[70], as disposições dos artigos 7º e 11 da LGPD, quando, respectivamente, se tratar dado pessoal de caráter geral e dado pessoal sensível de criança ou adolescente.

Nesse sentido, inclusive, afirma enunciado publicado em maio de 2023 pela Autoridade Nacional de Proteção de Dados (ANPD): "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei." Igualmente, o enunciado n. 684, aprovado na IX Jornada de Direito Civil do CJF, em maio de 2022, destacou: "O art. 14 da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) não exclui a

aplicação das demais bases legais, se cabíveis, observado o melhor interesse da criança."

Acerca da base legal do consentimento, disposta no parágrafo 1º do Art. 14, mostra-se necessário tecer algumas considerações. Na lei, em relação às crianças, afirma-se que o tratamento dos dados pessoais desses sujeitos deverá ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal, devendo esse consentimento ser também livre, informado e direcionado a tratamento de dados pessoais para finalidade determinada. Diante disso, o consentimento dado por sujeito fora do requisito legal ou pela própria criança sozinha não poderá ser admitido. Optou a lei por oferecer tutela destacada à criança, sujeito hipervulnerável e absolutamente incapaz, o qual deve ser representado sob pena de nulidade absoluta do ato praticado.

Como visto, o referido parágrafo 1º não menciona o adolescente, criando, assim, dúvida se o consentimento manifestado por ele sem assistência ou representação poderia ser considerado válido, como hipótese de capacidade especial, ou se simplesmente o legislador teria optado por não tratar do tema, por já existir legislação geral sobre a matéria no Código Civil (Artigos 3º, 4º e 1.634, VII).

A priori, parece que o legislador pretendeu reconhecer validade ao consentimento manifestado diretamente pelo adolescente no que concerne, especificamente, ao tratamento de seus dados pessoais (quando a base legal adotada para o caso for o consentimento). Como já afirmado, "Tomando-se como base a realidade da utilização da internet e das mídias sociais, que têm entre seus usuários milhares de adolescentes, é possível que se tenha optado por considerar jurídica hipótese fática dotada de ampla aceitação social."[71] Recorda-se, inclusive, que tanto o Código Civil quanto o Estatuto da Criança e do Adolescente trazem em suas normas disposições que valorizam a vontade dos menores e oferecem hipóteses de capacidade especial a eles.[72]

Em sentido contrário[73], porém, parte da doutrina entende que levando em conta as normas do Código Civil e a doutrina do melhor interesse, tanto para o tratamento de dados de crianças quanto de adolescentes, seria necessário ocorrer a manifestação do consentimento de, pelo menos, um dos pais ou responsável legal. No caso de adolescente entre 16 e 18 anos, seria necessário o consentimento dele e de seu responsável.[74]

O contexto tecnológico atual traz diversas oportunidades e recursos para as crianças e adolescentes, auxiliando inclusive na promoção de seus direitos. Contudo, os riscos enfrentados e as diversas situações de tratamentos indevidos e ilícitos de

dados pessoais trazem consigo desafios para a tutela dos referidos sujeitos, o que impõe um estudo constante da temática e uma interpretação das normas centrada na proteção integral de cada criança e adolescente, dentro suas realidades. Nessa dinâmica, a LGPD apresenta normas importantes para o sistema de proteção desenvolvido a esses sujeitos no Brasil, o qual ainda deverá contar, nos próximos anos, com mais disposições acerca do uso de ferramentas de inteligência artificial (IA) e plataformas digitais por menores de idade.

Considerações finais

A análise sobre a proteção dos dados pessoais sensíveis de crianças e adolescentes revela-se fundamental no atual cenário de crescente coleta de informações pessoais, digitalização e conectividade. Este artigo buscou explorar os desafios e oportunidades apresentados por este contexto, enfatizando a importância das doutrinas do melhor interesse e da proteção integral na tutela de relações que envolvem o tratamento de dados de menores em múltiplos contextos digitais e conectados.

Como apresentado, a crescente presença de crianças e adolescentes na Internet destaca a urgência de políticas públicas e educacionais que promovam uma inclusão digital ampla e responsável. Além disso, uma educação digital de qualidade, aliada a um controle parental adequado, pode contribuir significativamente para um uso mais saudável e consciente das tecnologias. Ressalta-se, porém, que essa educação deve respeitar os graus de autonomia e discernimento dos menores, proporcionando-lhes espaços de liberdade para o desenvolvimento de sua autonomia e comunicação.

O estudo aprofundou-se também na qualificação dos dados pessoais sensíveis e na aplicação da Lei Geral de Proteção de Dados (LGPD), demonstrando a importância de uma proteção ampliada para determinadas informações que possam gerar discriminações ou riscos significativos aos titulares. Entende-se que a proteção dos dados sensíveis se mostra essencial para garantir a liberdade, igualdade e integridade dos indivíduos, particularmente no caso de crianças e adolescentes, que possuem uma vulnerabilidade agravada devido à sua idade e falta de experiência.

Os casos internacionais e nacionais analisados exemplificam como a coleta e o tratamento indevidos de dados pessoais sensíveis podem resultar em graves violações de direitos. As multas e sanções impostas a entidades que desrespeitam a

privacidade e a segurança dos menores reforçam a necessidade de um cumprimento rigoroso das normas de proteção de dados. Ademais, a elaboração de relatórios de impacto à proteção de dados e a adoção de boas práticas são instrumentos essenciais para mitigar riscos e garantir a conformidade legal.

É essencial que os dispositivos e plataformas digitais sejam projetados a partir da lógica da privacidade por design, garantindo que as informações pessoais sejam tratadas de maneira ética e segura. Além disso, a educação digital desempenha um papel crucial, capacitando crianças, adolescentes e seus responsáveis a navegarem no ambiente online de forma segura e consciente.

A discussão sobre o uso de dados biométricos e a coleta de informações por brinquedos conectados e plataformas digitais mostrou a complexidade e os riscos envolvidos no tratamento de dados de menores. As implicações éticas, legais e sociais foram abordadas, evidenciando a necessidade de uma abordagem cautelosa e responsável para garantir que as tecnologias não comprometam a privacidade e a segurança das crianças e adolescentes.

Ao longo do texto, a aplicação da doutrina do melhor interesse da criança e do adolescente foi reiteradamente ressaltada como princípio norteador da tutela dos dados pessoais desses sujeitos. Essa proteção não se limita ao estágio de desenvolvimento atual, mas visa garantir a dignidade e os direitos dos menores tanto no presente quanto no futuro. A legislação brasileira, em consonância com normas internacionais, deve continuar evoluindo para acompanhar as rápidas mudanças tecnológicas e as novas formas de tratamento de dados.

Este artigo reforçou a importância de um esforço conjunto entre famílias, educadores, plataformas digitais, autoridades reguladoras e legisladores para construir um ambiente digital seguro e inclusivo. A proteção de dados sensíveis de crianças e adolescentes é um compromisso que demanda atenção constante, educação continuada e a implementação de medidas robustas de segurança e privacidade. Somente assim será possível garantir que os benefícios da era digital sejam plenamente aproveitados, sem comprometer os direitos e a integridade dos menores.

É imperativo, portanto, que a sociedade como um todo se engaje na proteção dos dados pessoais de crianças e adolescentes, o que inclui não apenas a aplicação de leis e regulamentos, mas também a promoção de uma cultura de respeito e responsabilidade digital. Ao priorizar o melhor interesse dos menores e adotar uma abordagem proativa e preventiva, podemos garantir que a era digital se torne um espaço importante para o desenvolvimento pleno e saudável das futuras gerações.

[1] TEFFÉ, Chiara Spadaccini de. Desafio da Baleia Azul: o que se sabe até agora. ITS FEED, 25 abr. 2017. Disponível em: https://feed.itsrio.org/desafio-da-baleia-azul-o-que-se-sabe-at%C3%A9-agora-b4b85ae77a56 Acesso em 04.06.21.

[2] TEFFÉ, Chiara Spadaccini de. Exposição não consentida de imagens íntimas: como o Direito pode proteger as mulheres? In: Nelson Rosenvald; Rafael Dresch; Tula Wesendonck (Org.). *Responsabilidade civil*: novos riscos. 1ed.Indaiatuba: Foco, 2019. p. 91-113.

[3] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira De Direito Civil*, v. 25, p. 83-116, 2020.

[4] 10ª edição da pesquisa TIC Kids Online Brasil 2023. Disponível em: https://cetic.br/pt/noticia/tic-kids-online-brasil-2023-criancas-estao-se-conectando-a-internet-mais-cedo-no-pais/ Acesso em: 19.05.24

[5] O comentário n.25 acerca dos direitos da criança no ambiente digital foi um importante embasamento teórico para o presente artigo. Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment.

[6] O comentário n.25 acerca dos direitos da criança no ambiente digital afirma que: "The Committee calls upon States parties to take proactive measures to prevent discrimination on the basis of sex, disability, socioeconomic background, ethnic or national origin, language or any other grounds, and discrimination against minority and indigenous children, asylum-seeking, refugee and migrant children, lesbian, gay, bisexual, transgender and intersex children, children who are victims and survivors of trafficking or sexual exploitation, children in alternative care, children deprived of liberty and children in other vulnerable situations. Specific measures will be required to close the gender-related digital divide for girls and to ensure that particular attention is given to access, digital literacy, privacy and online safety."

[7] A construção da noção de hipervulnerabilidade pelos Tribunais parece estar associada à ideia de que as pessoas assim qualificadas se encontram em situação de maior desigualdade e, por essa razão, carentes de maior proteção. Nesse sentido, Cláudia Lima Marques explica que a noção foi desenvolvida "como um corolário positivo da proibição de discriminação, logo do princípio da igualdade (um dever ser), e mandamento de pleno desenvolvimento da personalidade, diretamente ligada, pois, a nossa visão de dignidade da pessoa humana." (MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.). *Diálogo das fontes:* do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 46-47.) "Quanto à pergunta sobre se os hipervulneráveis são apenas os mencionados no texto constitucional (crianças, adolescentes, idosos e portadores de deficiência), parece-me cedo para responder de forma definitiva. A diferença está em que os hipervulneráveis mencionados nas normas constitucionais se beneficiam do mandamento de proteção constitucional (com efeitos e força normativa no direito privado), enquanto, por exemplo, os doentes e analfabetos são hipervulneráveis cuja proteção especial dependerá da atuação ativa do Judiciário e das especificidades do caso concreto (por exemplo, conhecimento pelo parceiro contratual de sua condição agravada de vulnerabilidade, tipo de contrato, onerosidade ou gratuidade deste, etc.)." (MARQUES, Cláudia Lima. O diálogo das fontes como método da nova teoria geral do direito: um tributo a Erik Jayme. In.: _____ (coord.) *Diálogo das fontes*: do conflito à coordenação de normas no direito brasileiro novo regime das relações contratuais. São Paulo: RT, 2012, p.17-66, p. 48.)

[8] Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

[9] "10. Configura dano moral coletivo ofensa a direitos coletivos ou difusos de caráter extrapatrimonial associados a sujeitos ou bens vulneráveis e hipervulneráveis - pessoas com deficiência, consumidor, criança e adolescente, idoso, meio ambiente, ordem urbanística, entre

outros." (STJ. REsp 1.793.332/MG, Rel. Ministro Herman Benjamin, Segunda Turma, DJe 26/08/2020)

[10] STJ. REsp 1.587.477. Quarta Turma. Rel. Min. Luis Felipe Salomão, DJe 27/08/2020.

[11] Princípio II - A criança gozará de proteção especial e disporá de oportunidade e serviços, a serem estabelecidos em lei por outros meios, de modo que possa desenvolver-se física, mental, moral, espiritual e socialmente de forma saudável e normal, assim como em condições de liberdade e dignidade. Ao promulgar leis com este fim, a consideração fundamental a que se atenderá será o interesse superior da criança. (Declaração dos Direitos da Criança, 1959).

[12] Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Acesso em: 05.06.21.

[13] Art. 3º, parágrafo único: "Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem."

[14] Recorda-se também a Lei nº 13.257, de 8 de março de 2016, chamada de *Marco Legal da Primeira Infância*: "Art. 1º Esta Lei estabelece princípios e diretrizes para a formulação e a implementação de políticas públicas para a primeira infância em atenção à especificidade e à relevância dos primeiros anos de vida no desenvolvimento infantil e no desenvolvimento do ser humano (...). Art. 2º Para os efeitos desta Lei, considera-se primeira infância o período que abrange os primeiros 6 (seis) anos completos ou 72 (setenta e dois) meses de vida da criança. Art. 3º A prioridade absoluta em assegurar os direitos da criança, do adolescente e do jovem, nos termos do art. 227 da Constituição Federal e do art. 4º da Lei nº 8.069, de 13 de julho de 1990 , implica o dever do Estado de estabelecer políticas, planos, programas e serviços para a primeira infância que atendam às especificidades dessa faixa etária, visando a garantir seu desenvolvimento integral."

[15] Pietro Perlingieri apresenta a definição de igual dignidade social em duas perspectivas convergentes: "como o instrumento que confere a cada um o direito ao respeito inerente à qualidade de homem, assim como a pretensão de ser colocado em condições idôneas a exercer as próprias aptidões pessoais." (PERLINGIERI, Pietro. *Perfis do direito civil*: introdução ao direito civil-constitucional. Rio de Janeiro: Renovar, 1997, p.37.)

[16] Steinberg, S. B. (2017). Sharenting: Children's privacy in the age of social media. *Emory Law Journal*, 66(4), 839–884. TUIKONG, S. Just technopanic or a real risk? Publishing children's pictures online: a review of literature. *International Journal of Child, Youth and Family Studies*, *13*(2-3), 72-87, 2022. SILVA BONARDI; Bianca; ALVES MORAES, Daniele. Oversharenting e os limites ao poder familiar. *Revista Sociedade Científica*, v. 7, n. 1, p. 722–789, 2024.

[17] STEINBERG, Stacey. *Growing Up Shared*: How Parents Can Share Smarter on Social Media-and What You Can Do to Keep Your Family Safe in a No-Privacy World. Sourcebooks, 2020. PLUNKETT, Leah A. *Sharenthood*: Why We Should Think before We Talk about Our Kids Online. The MIT Press, 2019. EBERLIN, Fernando Büscher von Teschenhausen. Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro. *Revista Brasileira de Políticas Públicas*. Brasília, v. 7, nº 3, 2017 p. 255-273.

[18] Cf. TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. In: Comitê Gestor da Internet no Brasil. (Org.). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2018, v. 1, p. 31-40.

[19] "Como regra, a comunicação estabelecida com esses dispositivos é pouco complexa e, muitas vezes, realizada na forma de comandos, sendo desnecessário utilizar expressões como "por favor" e "obrigado" (Lemos, 2017). Isso poderia influenciar negativamente as formas de expressão das crianças, prejudicando a sua interação com outros seres humanos. Em última instância, a diversão se transformou em um processo de criação de bases de dados. Quantas vezes a criança acessou o brinquedo? Quais informações ela trocou com ele? Quem tem acesso a essa comunicação e onde os dados são armazenados? O que pode ser feito com eles, além de melhorar a performance do brinquedo e do jogo? Existe um debate complexo sobre o consentimento dos pais e responsáveis para o tratamento de dados pessoais de seus filhos. Ainda que os pais tenham consentido com o uso do

brinquedo e instalado um aplicativo que permite que eles controlem a brincadeira, há aspectos nebulosos nessa relação que precisam ser mais bem debatidos. O que acontece se uma outra criança brincar junto e se comunicar com a boneca ou jogo? Enquanto cada vez mais brinquedos e jogos se conectam à rede, mais cedo as crianças também passam a utilizar a Internet. Duas certezas provenientes desse cenário são a transformação das práticas de diversão e os desafios constantes para a proteção da privacidade e dos dados pessoais." (TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. In: Comitê Gestor da Internet no Brasil. (Org.). Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018, v. 1, p. 31-40.)

[20] Cf. TEFFÉ, Chiara Spadaccini de; FERNANDES, E. R. Contratações em redes sociais e proteção de dados de crianças e adolescentes. In: Milena Oliva; André Roque. (Org.). *Direito da era digital*. 1ed. São Paulo: JusPodivm, 2022, v. 1, p. 97-122.

[21] Em abril de 2024, a Meta reduziu a idade mínima exigida para usar o WhatsApp na Europa de 16 para 13 anos. A nova idade mínima de 13 anos também foi anunciada para usuários no Reino Unido em fevereiro. O serviço afirma em seu site que as mudanças garantem "um requisito consistente de idade mínima para o WhatsApp em todo o mundo". Fonte: https://faq.whatsapp.com/3539044006356145 Acesso em: 19 de maio de 2024.

[22] O artigo 8º da norma europeia dispõe, em síntese, que, quando for aplicável o artigo 6º, n. 1, "a", que traz a base legal do consentimento, quanto à oferta direta de serviços da sociedade da informação para crianças, o tratamento dos dados pessoais delas será legal quando tiverem pelo menos 16 anos de idade. Caso a criança tenha menos de 16 anos, o tratamento só será lícito se o consentimento for dado ou autorizado pelos titulares da autoridade parental. Contudo, destaca-se que os Estados-Membros poderão estabelecer idade menor para os efeitos referidos, desde que não inferior a 13 anos.

[23] "The GDPR contains a number of specific protections for children's data protection rights, including the specific provisions in Article 8 GDPR, setting out the conditions applicable to obtaining a **child's consent** in relation to **information society services**.10 It should be noted, however, that consent is not the only possible legal basis for the processing of children's personal data, and controllers should assess on a case-by-case basis which is the most appropriate legal basis for any proposed processing. Where such services are offered directly to a child, and the controller seeks to rely on consent as a legal basis, the child's must be at least 16 years old to consent independently, or, if the child is younger, the holder of parental responsibility must have given or authorised the consent. Whilst Article 8(1) does allow for Member States to set the age at a lower level (between 13 and 16), the 2018 Act has maintained the age cut-off for consent to such services at 16 years old in Ireland. In cases involving children under 16, controllers must make **reasonable efforts to verify** that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology."(Autoridade de proteção de dados irlandesa. Guidance Note: Legal Bases for Processing Personal Data. December 2019. p. 09.)

[24] "Additional protection is granted to this type of personal data since children are less aware of the risks and consequences of sharing data and of their rights. Any information addressed specifically to a child should be adapted to be **easily accessible, using clear and plain language**. For most online services **the consent of the parent or guardian** is required in order to process a child's personal data on the grounds of consent up to a certain age. This applies to social networking sites as well as to platforms for downloading music and buying online games. The age threshold for obtaining parental consent is established by each EU Member State and can be between 13 and 16 years. (...) Companies have to make reasonable efforts, taking into consideration available technology, to check that the consent given is truly in line with the law. (...) Preventive or counselling services offered directly to children are exempted from the requirement for parental consent as they seek to protect a child's best interests." Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en> Acesso em: 05.06.21.

[25] "The ongoing debate around age assurance is often centred around restricting access to the internet for children and young people. But done properly, age assurance can drive the development of new products and services to create a richer and more diverse digital ecosystem in which children (one in three internet users) are a recognised user group. (...) Rather than viewing it as simply restricting access, we should be looking at age assurance as a chance to invite children into a digital world that offers them greater privacy, freedom from commercial pressures, content and information in formats and language that they like, protection from misinformation or material that promotes harmful activities (such as suicide, self-harm or disordered eating), alongside supporting digital services in their legal duty not to provide children with age restricted contact and content." (But how

do they know it is a child? Age Assurance in the Digital World. 5Rights Foundation. Março de 2021. Disponível: <https://5rightsfoundation.com/in-action/but-how-do-they-know-it-is-a-child-age-assurance-in-the-digital-world.html> Acesso em: 11.06.21)

[26] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil* , Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

[27] RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje.* Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.19.

[28] TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis*: qualificação, tratamento e boas práticas. 1. ed. indaiatuba: Foco, 2022. v. 1. 280p .

[29] "Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. § 3º Ficam proibidas as anotações de: (...) II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas."

[30] Rodotà nos ensina: "O direito ao livre desenvolvimento da personalidade não é uma descoberta dos últimos tempos. É solenemente reconhecido pelo parágrafo 2º da Constituição alemã (...) e, de forma menos evidente, do artigo 2º da Constituição italiana, onde se afirma "a República reconhece e garante os direitos invioláveis do homem, seja como indivíduo, seja nas formações sociais nas quais se desenvolve sua personalidade." Pode-se legitimamente indagar, portanto, se a escolha de redefinir a própria identidade na internet pode ser considerada como um elemento essencial do desenvolvimento da personalidade e se as comunidades virtuais podem ser consideradas como "formações sociais"." (RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 116.)

[31] TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis*: qualificação, tratamento e boas práticas. 1. ed. indaiatuba: Foco, 2022. v. 1. 280p .

[32] "A exigência do respeito da personalidade, de seu livre desenvolvimento, incide sobre a noção de ordem pública, sobre os limites e sobre a função da autonomia negocial, sobre a interpretação dos atos através dos quais se manifesta – na individuação das fronteiras do ilícito e de seu fundamento, sobre as configurações não apenas das relações familiares, mas também daquelas patrimoniais, sobre a concepção e a tutela da relação de trabalho, sobre o juízo de valor do associativismo e de seus possíveis escopos; incide, em suma, sobre toda a organização da vida em «comunidade»" (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional.* Rio de Janeiro: Renovar, 2008, p. 768-769).

[33] Dispõe o considerando 51 do GDPR que: "Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms." Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT> Acesso em: 11.06.21

[34] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[35] RODOTÀ, Stefano. *A vida na sociedade da vigilância*. A privacidade hoje. Rio de Janeiro: Renovar, 2008. KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. Orientador: Sergio Marcos Carvalho de Ávila Negri. Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2019. p. 43.

[36] Tradução livre de: "È necessario sottolineare, infatti, che i dati sensibile sono quelli che riguardano la salute e la vita sessuale, le opinioni e l'appartenenza etnica o razziale, con una elencazione analoga a quella che si trova nelle norme riguardanti i casi di discriminazione. Siamo così di fronte a qualcosa che eccede la semplice tutela della vita privata e si pone come presidio della stessa eguaglianza tra le persone". (RODOTÀ, Stefano. *Il mondo nella rete*: Quali i diritti, quali i vincoli. Roma: Laterza & Figli – Gruppo Editoriale L'Espresso, 2019.p.36)

[37] "(...) não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado." (RODOTÀ. Op cit., p. 70.)

[38] LGPD, Art. 12. [...] § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

[39] RIOS, Roger Raupp; LEIVAS, Paulo Gilberto Cogo; SCHÄFER, Gilberto. Direito da antidiscriminação e direitos de minorias: perspectivas e modelos de proteção individual e coletivo. Rev. direitos fundam. democ., v. 22, n. 1, p. 126-148, jan./abr. 2017.

[40] Nesse sentido, Roger Rios destaca que: Passa-se a atentar para os prejuízos injustos suportados pelos destinatários de tratamentos desiguais, objetivando enfrentar situações de estigma e subordinação experimentadas por grupos discriminados (RIOS, 2008, p. 36; MOREIRA, 2017, p. 67; SOLANKE, 2017). A discriminação enfrentada pelo direito da antidiscriminação é, portanto, tomada por uma perspectiva mais substantiva que formal: importa enfrentar a desigualdade prejudicial e injusta, pois nem sempre a adoção de tratamentos distintos se revela maléfica, sendo mesmo tantas vezes exigida, como alerta a dimensão material do princípio da igualdade (o de tratar igualmente os iguais e desigualmente os desiguais na medida de suas desigualdades). (RIOS, Roger Raupp. Tramas e interconexões no Supremo Tribunal Federal: Antidiscriminação, gênero e sexualidade. *Rev. Direito Práx.,* Rio de Janeiro, v. 11, n. 2, p. 1332-1357, abril. 2020.)

[41] Como define Cathy O'Neil, algoritmos são opiniões embutidas em código, que repetem práticas e padrões passados e, assim, automatizam o *status quo*. Para que os algoritmos sejam justos, é preciso fiscalizá-los, repará-los e aprimorá-los. Dessa forma, além de se ter uma regulamentação adequada, que privilegie a transparência e a explicação quanto às decisões algorítmicas, o princípio da não discriminação deve estar presente desde a concepção dos sistemas de inteligência artificial, tanto na parte técnica dessa construção quanto na garantia de diversidade dos times responsáveis pelo desenvolvimento dos algoritmos. Mostra-se fundamental exigir responsabilidade e prestação de contas de corporações que tomam decisões capazes de prejudicar pessoas e comunidades. (O'NEIL, Cathy. *Weapons of Math Destruction*: How Big Data Increases Inequality and Threatens Democracy. Crown: 2016.)

[42] Mulholland apresenta dois casos graves em que o perfilamento (*profiling*) gerou tratamentos discriminatórios: "Os casos ocorreram nos EUA e se referiram à contratação de serviços médicos e de seguridade. No primeiro caso, algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez, pois o risco contratado seria muito alto. Em outro caso, relacionado a dados de saúde, "quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados"." (MULHOLLAND, Caitlin. Os contratos de seguro e a proteção dos dados pessoais sensíveis. In:

GOLDBERG, Ilan; JUNQUEIRA, Thiago (Coords.). *Temas atuais de Direito dos Seguros*, tomo I. São Paulo: Thomson Reuters. 2020.)

[43] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Sarlet. (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed.Rio de Janeiro: Forense, 2023.

[44] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. *Migalhas*, publicado em 22 de junho de 2020.

[45] DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 27.

[46] "As decisões automatizadas, referentes a um indivíduo determinado, que se baseiam em um método estatístico para análise de grande volume de dados e informações, podem ter grande impacto sobre os direitos individuais, especialmente no que se refere à autonomia, igualdade e personalidade. Afinal, na sociedade atual, caracterizada pelas relações remotas, os dados pessoais acabam por se constituir na única forma de representação das pessoas perante as mais diversas organizações estatais e privadas, sendo determinantes para "abrir ou fechar as portas de oportunidades e acessos" (LYON, 2003, p. 27). Dessa forma, uma eventual representação equivocada em determinados contextos sociais – por meio de um equívoco do algoritmo ou dos dados em que o algoritmo se baseou – afetaria tanto a forma como o indivíduo se percebe como também o modo como a sociedade o enxerga e o avalia, afetando a sua integridade moral e a sua personalidade (BRITZ, 2008, p. 179). Ademais, se essa representação, conforme alertado por Lyon (2003), acarretar a perda de chances e oportunidades do indivíduo na sociedade, dar-se-á uma restrição indevida à sua autonomia, limitando a sua liberdade de ação, suas escolhas econômicas e até mesmo existenciais. Por fim, destaca-se também a possibilidade de violação do princípio da igualdade, na hipótese de que a classificação e seleção operada por algoritmos produza resultados desiguais para pessoas em situações semelhantes, afetando negativamente as suas oportunidades de vida na sociedade (LYON, 2003, p. 27)." (DONEDA et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-17, 2018.)

[47] Cf. TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Revista estudos institucionais*, v. 6, p. 301-333, 2020.

[48] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

[49] No processo de aprovação da LGPD houve veto a trecho do artigo 20 que determinava o direito de revisão como um direito de revisão humana, ou seja, feito por uma pessoa natural. A crítica que se faz é a possibilidade então de tal revisão ser feita apenas por máquinas, ao contrário do que dispõe o direito europeu sobre a temática. Cf. FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência Artificial e Direito*: Ética, Regulação e Responsabilidade - revisto e atualizado. 2. ed. São Paulo: Revista dos Tribunais, 2020. FRAZÃO, Ana. Algoritmos e inteligência artificial, Jota, publicado em 15 de maio de 2018.

[50] "(...) mais importante do que identificar a natureza própria ou conteúdo do dado, é constatar a potencialidade discriminatória no tratamento de dados pessoais. Isto é, a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados. Não só a natureza de um dado, estruturalmente considerado, deve ser avaliada para sua determinação como sensível, mas deve-se admitir que certos dados, ainda que não tenham a princípio essa natureza especial, venham a ser considerados como tal, a depender do uso que deles é feito no tratamento de dados." (MULHOLLAND, Caitlin. Dados pessoais sensíveis e

consentimento na Lei Geral de Proteção de Dados Pessoais. *Migalhas*, publicado em 22 de junho de 2020.)

[51] DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 26-27

[52] HOF, Simone van der. I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, v. 34, n. 2, p. 409-445, 2016.

[53] Fonte: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en Acesso em: 06.06.21.

[54] Recomenda-se a leitura da Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), adotada em 11 de fevereiro de 2009. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf Acesso em: 06.06.21.

[55] Fonte: https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en . Acesso em: 06.05.24.

[56] Isso foi amplamente noticiado pela imprensa: https://www.forbes.com/sites/joewalsh/2021/02/25/tiktok-settles-privacy-lawsuit-for-92-million/?sh=616138584872 , https://www.bbc.com/news/technology-56210052 , https://www.fklmlaw.com/tiktok-agrees-to-pay-92-million-in-biometric-data-privacy-class-action/ e https://www.cnbc.com/2022/10/28/tiktok-users-paid-over-privacy-violations-google-snap-could-be-next.html Acesso em: 19 de maio de 2024.

[57] TJ/MA. Comarca da Ilha de São Luís. Ação Civil Pública 0816292-73.2020.8.10.0001. Sentença Publicada em 07 de março de 2024. A ACP foi distribuída em junho de 2020.

[58] Dados apresentados pelo professor David Banisar em 27 de janeiro de 2024: https://www.linkedin.com/pulse/data-protection-map-update-2024-david-banisar-j9w5e/ . Acesso em: 19 de maio de 2024.

[59] Disponível em: https://www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-final-version-childrens-fundamentals Acesso em: 19 de maio de 2024.

[60] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/> Acesso em: 06.06.21

[61] Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/ Acesso em: 19 de maio de 2024.

[62] 8 recomendações para reforçar a proteção de menores online. Disponível em: https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne Acesso em: 11.06.21. O tema está na agenda prioritária de 2024 da CNIL, que afirma que "Os menores estão cada vez mais expostos às redes sociais, aos sites de encontros e às plataformas de jogos. Isso pode levar à coleta massiva de informação sobre a sua identidade, preferências e estilo de vida, com repercussões significativas na sua privacidade, bem-estar psicológico e futuro socioprofissional. Durante as suas investigações, a CNIL irá verificar as aplicações e sites mais populares entre crianças e adolescentes para verificar se foram implementados mecanismos de controle de idade, quais as medidas de segurança implementadas e se o princípio da minimização de dados foi respeitado." Disponível em: https://www.cnil.fr/en/cnil-investigations-2024-minors-data-olympic-games-right-access-and-digital-receipts Acesso em: 19 de maio de 2024.

[63] Disponível em: https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf Acesso em: 18.06.22

[64] CAVOUKIAN, Ann. Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Dez. 2012. CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Disponível em: <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/> Acesso em: 09.04.21. EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Adopted on 20 October 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> Acesso em: 10.05.21.

[65] Disponível em: <https://www.cnil.fr/en/sheet-ndeg7-minimize-data-collection> Acesso em: 02.11.20.

[66] Orientação da ANPD acerca do relatório de impacto: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p1 Acesso em: 19 de maio de 2024.

[67] Fonte: <https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf> Acesso em: 06.06.21.

[68] "A DPIA is a defined process to help you identify and minimize the data protection risks of your service – and in particular the specific risks to children who are likely to access your service which arise from your processing of their personal data. You should begin a DPIA early in the design of your service, before you start your processing. It should include these steps: Step 1: identify the need for a DPIA Step 2: describe the processing Step 3: consider consultation Step 4: assess necessity and proportionality Step 5: identify and assess risks arising from your processing Step 6: identify measures to mitigate the risks Step 7: sign off, record and integrate outcomes." (Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/> Acesso em: 06.06.21.)

[69] Sobre o consentimento e suas polêmicas ver: TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e adolescentes. *Revista do Advogado*, v. 39, 2019.

[70] "Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (...) § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo."

Observa-se que tanto o parágrafo 1º quanto o 3º do artigo 14 mencionam apenas "crianças". Diante disso, ampliar as bases legais para o tratamento de dados de crianças pode parecer uma tese um pouco mais arriscada para alguns agentes, tendo em vista que as referidas disposições, ao mencionarem estritamente crianças, poderiam sinalizar uma possível restrição das hipóteses legais de tratamento para esses sujeitos. Por outro lado, tal situação não envolve diretamente a figura do adolescente, o qual apenas é mencionado no *caput* do art. 14 da LGPD.

[71] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira De Direito Civil*, v. 25, p. 83-116, 2020.p.109-110

[72] Exemplos de flexibilização do regime das incapacidades no ECA: art. 16, II; art. 28, §§1º e 2º; art. 100, XII; art. 111, V; e art. 161, §3º. Além desses exemplos, pode-se citar o próprio Código Civil, em seu art. 1.740, III. Existem também atos e negócios que os relativamente incapazes podem praticar, mesmo sem assistência, como se casar, exigindo-se a autorização de ambos os pais ou de seus representantes legais; elaborar testamento; servir como testemunha de atos e negócios jurídicos; e ser eleitor.

[73] TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: Bruno Bioni, Laura

Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de Dados Pessoais*. 1ed. Rio de Janeiro: Forense, 2021. Ebook.

[74] (...) ainda que o §1º não mencione os adolescentes, não faria sentido deixá-los desprovidos da igual e devida proteção, sob pena de se violar as garantias constitucionais dessas pessoas. Há que se defender, nesse caso, a aplicação do Código Civil, a fim de se promover a integralidade de seus direitos. De fato, a proteção de dados pessoais, entendida enquanto parte do contrato civil, reforça a objeção à capacidade legal de crianças e de adolescentes consentirem quanto ao tratamento de seus dados, uma vez que, pelo exercício do poder familiar, compete a mães, pais e responsáveis representá-los até os 16 anos, nos atos da vida civil, e assisti-los, após essa idade, nos atos em que forem partes, suprindo-lhes o consentimento. Não se coadunaria, com efeito, com as garantias legais ao melhor interesse e à absoluta prioridade do adolescente que lhe fosse facultada a outorga de consentimento autônomo ilimitado para o tratamento de seus dados pessoais. Dessa forma, entende-se indispensável o consentimento parental ou de pessoa responsável legal para o tratamento de dados pessoais de crianças e de adolescentes de até 16 anos de idade, observando-se a forma prevista no referido 14, §1º, da LGPD, devendo, assim, o consentimento ser específico e em destaque. No caso de adolescentes entre 16 e 18 anos, será necessário o consentimento de ambos, não bastando o consentimento parental. (HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: Bruno Bioni, Laura Schertel Mendes, Danilo Doneda, Otavio Luiz Rodrigues Jr., Ingo Wolfgang Sarlet. (Org.). *Tratado de Proteção de Dados Pessoais*. 1ed. Rio de Janeiro: Forense, 2021. Ebook.)

Contribuição à Tomada de Subsídios para o Projeto Regulatório da ANPD sobre Crianças e Adolescentes

Elora Fernandes[1]

A regulação específica do tratamento de dados de crianças e adolescentes pela Autoridade Nacional de Proteção de Dados (ANPD) é esperada com expectativa pela sociedade brasileira. O art. 14, da LGPD, apresenta dificuldades interpretativas que, por vezes, pode gerar insegurança jurídica e, eventualmente, prejudicar a proteção especial a que estes sujeitos fazem jus (Fernandes & Medon, 2021). Reconhecendo a importância de prover diretrizes específicas, este tema já estava presente na agenda regulatória da ANPD para o biênio 2023-2024 (ANPD, 2022c). O grau de prioridade para normatização em relação ao tema foi mantido pela Autoridade na revisão da agenda publicada no final de 2023, por meio da Resolução CD/ANPD nº 11, de 27 de dezembro de 2023 (ANPD, 2023d).

Até o momento, a ANPD havia emitido um enunciado relativo às bases legais possíveis para o tratamento de dados de crianças e adolescentes (ANPD, 2023a), além de diretrizes especiais para a implementação do legítimo interesse como base legal (ANPD, 2024a). Ademais, a autoridade vem se manifestando em processos de fiscalização sobre a proteção de dados de crianças e adolescentes, como o referente ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) (ANPD, 2022b, 2023c) ou ao TikTok (Bytedance Brasil Tecnologia Ltda) (ANPD, 2023b).

No final de junho de 2024, a autoridade abriu a "Tomada de Subsídios para o Projeto Regulatório sobre o Tratamento de Dados de Crianças e Adolescentes" (ANPD, 2024b). A chamada tem por objetivo embasar a análise e a proposição de projeto regulatório específico a respeito desse grupo de titulares e as contribuições da sociedade civil são de extrema importância para a tomada de decisão informada por parte da autoridade.

Considerando que as respostas à consulta podem não apenas auxiliar a ANPD, mas também fomentar o debate público sobre o tema, o presente documento apresenta a minha contribuição de forma mais detalhada para a tomada de subsídios, acrescida das referências bibliográficas enviadas para a autoridade em e-mail separado, como solicitado pela chamada. As perguntas feitas pela autoridade estão destacadas em caixa de texto azul, seguidas das minhas respostas.

---

[1] Elora Fernandes é Pesquisadora de Pós-doutorado no KU Leuven Centre for IT and IP Law (CiTiP – Bélgica), onde foca sua pesquisa nos direitos de crianças no ambiente digital. Anteriormente, trabalhou em ONGs de direitos digitais em diferentes países e atuou como Trainee e Legal Officer (Interina) no European Data Protection Supervisor (EDPS). Elora defendeu seu Doutorado em Direito na Universidade do Estado do Rio de Janeiro (UERJ) em cotutela com a KU Leuven, com tese acerca da proteção de dados de crianças em tecnologias educacionais (edtech). Obteve Mestrado em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF, Brasil) e concluiu a Graduação em Direito na mesma instituição, incluindo um período de mobilidade acadêmica na Universidade de Salamanca (Espanha). Além disso, coordenou a equipe de assistentes da Revista de Estudos Empíricos em Direito (REED) e é *alumna* do Deutscher Akademischer Austauschdienst (DAAD).

I - Princípio do melhor interesse

De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança, no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU e no Comentário Geral nº 25, de 2021, do Comitê dos Direitos da Criança. Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz.

Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, questiona-se:

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Como destacado na introdução à pergunta, o princípio do melhor interesse da criança foi detalhado pelo Comitê sobre os Direitos da Criança no Comentário Geral nº 14, de 2013. O Comitê destacou as **três funções** que o princípio do melhor interesse pode desempenhar (**direito fundamental, princípio interpretativo e regra processual**). A partir dessas funções, é preciso discutir o que significa (ou seja, qual o conteúdo) do melhor interesse na prática.

A doutrina especializada em direitos fundamentais de crianças frequentemente caracteriza o princípio do melhor interesse como **indeterminado e dinâmico**, o que muitas vezes causa confusão sobre os contornos da sua aplicação. A sua indeterminação e dinamicidade advêm, porém, da sua **característica de princípio geral** da Convenção sobre os Direitos da Criança (daqui pra frente, Convenção). Isto quer dizer que ele deve ser utilizado na **interpretação e aplicação de outros direitos previstos na Convenção** (Lundy & Byrne, 2017).

Sendo um mandado de otimização com caráter procedimental, não é possível definir o que é de melhor interesse de uma criança ou grupo de crianças em abstrato. O conteúdo do princípio do melhor interesse será sempre o **resultado de um exercício de balanceamento no caso concreto**. Isso não quer dizer que decisões tenham de ser tomadas a nível individual e o próprio Comitê reconhece a possibilidade de uma análise coletiva do melhor interesse de um grupo de crianças (como a nível de legislação, políticas públicas ou mesmo em uma plataforma digital).

A fim de auxiliar a determinação do conteúdo do melhor interesse, o Comitê apresenta alguns parâmetros não exaustivos[2] que devem ser utilizados:

[2] Nesse sentido, a ANPD poderia construir parâmetros a partir destes apresentados e adaptados à realidade do tratamento de dados pessoais.

> a) A natureza universal, indivisível, interdependente e inter-relacionada dos direitos das crianças; b) Reconhecimento das crianças como titulares de direitos; c) A natureza global e o alcance da Convenção; d) A obrigação dos Estados Partes de respeitar, proteger e cumprir todos os direitos na Convenção; e) Efeitos de curto, médio e longo prazo das ações relacionadas ao desenvolvimento da criança ao longo do tempo.

Estes parâmetros mostram que este **não é um exercício subjetivo**. Assim, o primeiro critério aponta para a necessidade de um balanceamento dos impactos negativos e positivos do tratamento de dados em **todos os direitos previstos na Convenção**, considerando a sua **indivisibilidade e interdependência**. Tomadores de decisão não devem, portanto, escolher a dedo alguns direitos que serão analisados, mas abarcar os direitos na Convenção e no ordenamento brasileiro como um todo (assim como determinado pelo *caput* do art. 14 da LGPD). Isso não inclui apenas direitos de proteção (inclusive a proteção à privacidade e à proteção de dados pessoais), mas também direitos de provisão, como o direito à liberdade de expressão ou participação no ambiente digital. Esse **balanceamento para a identificação do melhor interesse deve ser feito através da realização dos chamados *Children Rights Impact Assessments - CRIAs*** (Hof & Lievens, 2018; Mukherjee et al., 2021; Payne, 2019; UNICEF & Danish Institute for Human Rights, 2013), que podem ser holisticamente integrados nos Relatórios de Impacto de Proteção de Dados (RIPD). Essas análises não são importantes apenas para a realização do balanceamento no caso concreto, mas também para fornecer **provas desse exercício com base no princípio da responsabilização e prestação de contas**. Assim, entende-se que os CRIAs são obrigatórios em qualquer ação que concerne uma criança ou grupo de crianças para avaliar qual é o seu melhor interesse no caso concreto.

Os outros princípios gerais da Convenção devem ser considerados neste exercício também, em especial o **direito de crianças a serem ouvidas**, que deve ser implementado sempre que possível na tomada de decisão. Considerando que crianças e adolescentes não possuem autonomia completa e, consequentemente, responsabilidade para tomar decisões sozinhas, a decisão não deve automaticamente estar alinhada com as suas visões. Contudo, especialmente se as crianças envolvidas já tiverem as competências necessárias para expor sua opinião, esta deve ser **levada em consideração** e, caso não esteja alinhada à decisão final, **este raciocínio deve ser fundamentado e registrado no CRIA/RIPD** (Committee on the Rights of the Child, 2009; Digital Futures Commission, 2021).

Destaca-se, também, que, dentre os parâmetros de determinação apresentados pelo Comitê, está a necessidade de considerar os **efeitos de curto, médio e longo prazo das ações relacionadas ao desenvolvimento da criança**. Decisões que levem em consideração o princípio do melhor interesse devem ser sempre **baseadas em evidências científicas**, incluindo o conhecimento das necessidades de desenvolvimento de crianças e os impactos de inovações tecnológicas (Livingstone et al., 2024).

Além dos impactos em seus interesses atuais, é crucial que os controladores considerem os **impactos do tratamento de dados em seus interesses futuros**. Assim, o princípio do melhor interesse também deve ser entendido como um **princípio de precaução**, que requer a avaliação da possibilidade de risco e dano futuros e outras consequências da decisão para os direitos da criança (Committee on the Rights of the Child, 2013, parag. 74). Essa compreensão nos obriga a agir com cautela, mesmo quando o potencial perigo de uma determinada tecnologia não está totalmente estabelecido, mas há indicações de que **não agir neste momento** poderia causar danos. Isso é especialmente importante no caso de tecnologias cujos benefícios não são confirmados por evidências científicas (Lievens, 2021). Assim,

podemos dizer que o princípio de precaução inverte a lógica e acrescenta **peso à prova de que a tecnologia traz benefícios, ao invés de apenas provar que ela realmente causa ou pode causar danos no futuro**.

Após a identificação do que é de melhor interesse da criança em determinado caso concreto (1º passo), é preciso ainda **contrapô-lo com outros interesses e direitos de terceiros** (2º passo). Nesta segunda etapa, o que foi determinado como o melhor interesse da criança no caso deve ser considerado com **absoluta prioridade** (art. 227, da Constituição da República Federativa do Brasil - CRFB) na decisão, inclusive em relação aos interesses dos pais (Brochado Teixeira & Rettore, 2024). Abstratamente, isso não quer dizer que outros direitos (especialmente quando de interesse público), não possam prevalecer sobre os direitos da criança e do adolescente. Contudo, estes últimos devem ser uma **consideração primária e não apenas um dos critérios a serem ponderados** (Committee on the Rights of the Child, 2013, parag. 39–40; Ruggiero, 2022).

Um caso interessante relativo ao balanceamento entre interesse público e o melhor interesse da criança (ou de um grupo de crianças) ocorreu em 2017, quando o Ministério Público Federal ajuizou ação civil pública para identificar crianças que, de acordo com o Censo 2010, não foram regularmente registradas nos cartórios de registro civil da cidade de Bauru. O Supremo Tribunal Federal (STF) entendeu que, apesar da necessidade de se proteger os direitos fundamentais de crianças e adolescentes através da revelação de suas identidades (isto é, **o compartilhamento dos seus dados estaria no seu melhor interesse**), proteger o sigilo estatístico seria indispensável às atividades desempenhadas pelo IBGE e à garantia da fidelidade dos dados estatísticos que subsidiam políticas públicas (Brasil, 2017). A informação acerca do não registro das crianças, por exemplo, muito provavelmente não seria compartilhada pelos pais caso soubessem da possibilidade de quebra desse sigilo. Assim, entendeu-se que **o benefício gerado pelo compartilhamento dos dados não superaria o risco à confiança pública que quebra do sigilo estatístico das atividades do IBGE geraria**.[3]

Destaca-se, ainda, que a dinamicidade do princípio do melhor interesse inclui a necessidade de se considerar a **autonomia progressiva** (cf. Committee on the Right of the Child, 2016) e as capacidades das crianças e dos adolescentes envolvidos. As capacidades específicas (para além da maturidade ou discernimento) não devem ser consideradas apenas ao avaliar o conteúdo do melhor interesse, mas devem também ser usadas como critério para **reavaliar a decisão ao longo do tempo** (Committee on the Rights of the Child, 2013, parag. 84).

[3] A partir do entendimento do STF, as partes resolveram celebrar Termo de Compromisso de Ajustamento de Conduta (TAC) em que o IBGE incluiria, em 2018, um conjunto de perguntas das Pesquisa Municiais envolvendo a infraestrutura de sub-registro de nascimentos em todos os municípios brasileiros (Termo de Ajustamento de Conduta - Autocomposição, 2018). Outro exemplo importante de balanceamento em discussão no âmbito europeu é o relativo a medidas estabelecidas pela proposta de Regulamento prevenir e combater o abuso sexual de crianças apresentada pela Comissão Europeia (2022). Em opinião conjunta, o EDPB e o EDPS (2022) entenderam que, para além do uso de expressões vagas na legislação, que deixavam uma ampla margem de interpretação para os potenciais controladores de dados, a possibilidade de rastreamento das comunicações pessoais e a quebra da criptografia para todos os usuários de determinadas plataformas seriam desnecessárias e desproporcionais em relação à potencial proteção das crianças que essas medidas pretendem garantir.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

A fim de direcionar os agentes de tratamento a tratarem dados de crianças e adolescentes de acordo com o seu melhor interesse, para além das considerações elaboradas na resposta anterior, seria de extrema valia caso a ANPD determinasse, *a priori*, **situações claras em que o melhor interesse da criança sempre prevalecerá**, além de exemplos de situações limítrofes.

Um exemplo claro de situação em que o melhor interesse da criança deve sempre prevalecer é o caso de **interesses comerciais**, que muito frequentemente não coincidem com os interesses e direitos de crianças. Destaca-se que um dos direitos previstos na Convenção, em seu art. 32(1), é o **direito à proteção contra a exploração econômica**. Devemos entender "econômico" como qualquer interesse material, como a busca de ganho ou lucro através da produção, distribuição ou consumo de bens e serviços. Já o conceito de "exploração" se refere a aferir vantagem injustamente de outros em benefício próprio. Isso abrangeria ações como manipulação, uso indevido, abuso, vitimização, opressão ou maus-tratos (Verdoodt, 2020, p. 98).

Estes dois elementos podem ser identificados no ambiente digital e, de forma específica, nos principais modelos de negócio *online*. No seu Comentário Geral 25 (2021), o Comitê destacou como os interesses comerciais podem impactar negativamente os direitos das crianças à informação independente (para. 53), a liberdade de expressão (para. 61) e o direito das crianças de brincar (para. 110). Outros exemplos de direitos afetados pelo tratamento de dados para fins comerciais incluem direito à não discriminação, ao desenvolvimento, à saúde e à educação (Van Der Hof et al., 2020). Isso não significa que as empresas não devam obter retorno financeiro sobre os seus produtos, mas **isso não deve basear-se em dados**, uma vez que **não devem ser vistos como uma mercadoria**, especialmente no caso de crianças.

No âmbito da Global Privacy Assembly, em sua Resolução sobre os Direitos de Crianças no Ambiente Digital, as Autoridades de Proteção de Dados destacaram que os Estados deveriam promover regulações que proibissem a transmissão de dados de crianças para terceiros para fins comerciais, assim como práticas de publicidade que encorajam crianças a fornecer dados pessoais (Global Privacy Assembly, 2021). No âmbito da União Europeia, o Regulamento de Serviços Digitais (DSA, na sigla em inglês) proibiu, em seu art. 28(2), que plataformas perfilassem crianças a partir de seus dados pessoais com a finalidade de publicidade direcionada (o mesmo sendo aplicado para qualquer dado sensível, segundo o art. 26(3)) (União Europeia, 2022).

Isso está diretamente ligado ao **impacto do melhor interesse na caracterização do que é considerada uma finalidade legítima**, a partir do art. 6º, I, da LGPD. O critério de legitimidade vai além da mera existência de base legal na LGPD e deve considerar a legalidade mais ampla do processamento de dados pessoais. Isso inclui, além do art. 14, da LGPD, todo o arcabouço jurídico de proteção de crianças e adolescentes. Assim, só deve ser considerada legítima a finalidade caso ela leve primordialmente em consideração o melhor interesse.

A ANPD pode ter um papel fundamental na definição de situações em que o melhor interesse sempre prevalecerá (como em relação a interesses comerciais),[4] gerando interpretações proibitivas específicas. Ademais, também pode auxiliar agentes de tratamento a partir da elaboração de ferramentas práticas que ajudem controladores a realizar o exercício de balanceamento destacado na pergunta acima, como já feito, por exemplo, pela autoridade do Reino Unido após a elaboração de seu *Age Appropriate Design Code* (Information Commissioner's Office (ICO), 2024).

Por fim, a discussão acerca do uso comercial de dados de crianças está diretamente ligada à necessidade de se regular de forma restrita o uso da base legal da proteção ao crédito para o tratamento de dados destes sujeitos (art. 7º, X, LGPD). Considerando que a **função primordial desta base legal** (que, lembramos, é inexistente em outros ordenamentos jurídicos ao redor do mundo) **é a proteção de credores e interesses financeiros**, não é possível imaginar cenários em que estes superariam a proteção do melhor interesse da criança. O estudo sobre bases legais aplicáveis feito pela ANPD (ANPD, 2022a), apesar de entender, em um primeiro momento, que essa base seria aplicável, carece de exemplos concretos em que isso ocorreria em puro atendimento ao princípio do melhor interesse. Considerando que a autoridade reservou para si o direito de regular de forma específica o uso de certas bases legais, como o fez com o legítimo interesse, **é fundamental reconhecer que o uso da proteção ao crédito é incompatível com o melhor interesse de crianças e adolescentes**.

II - Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

[4] Ver, por exemplo, guia da autoridade irlandesa de proteção de dados: "*The best interests of a child may not always coincide with an organisation's commercial interests, business model or the objective underlying a service offering. In fact, the best interests of the child principle may seriously conflict with or hamper such objectives. Nevertheless the child user's best interests must prevail in any such commercial decision-making*" (DPC, 2021, p. 63).

Assim como o consentimento exigido para o tratamento de dados sensíveis, o consentimento para o tratamento de dados de crianças mencionado no art. 14, §1°, LGPD, não deve apenas apresentar as mesmas características do consentimento para dados pessoais "comuns" (livre, informado e inequívoco), mas também ser **específico e em destaque**. Isso evidencia a intensão do legislador de incluir medidas adicionais de tutela na obtenção do consentimento para o tratamento de dados de crianças.

Para que o consentimento seja **específico**, ele dever não somente estar ligado a uma finalidade determinada, o que já é um requerimento do art. 5º, XII, LGPD, mas, mais restritamente, a **uma atividade de processamento de dados específica e bem definida**. Assim, no caso de múltiplas operações de tratamento de dados para diversos fins, pais ou responsáveis legais deverão fornecer consentimento **separadamente** para cada uma dessas operações, possibilitando uma maior granularidade e implementação da autodeterminação informativa.

Por outro lado, o requerimento de o consentimento ser **em destaque** está relacionado à necessidade de **chamar a atenção** do usuário de forma mais intensa acerca da decisão que ele está prestes a tomar. Isso pode ser feito através de recursos visuais, como cores diferentes, caixas de seleção destacada, pop-ups, ícones ou etiquetas virtuais que podem, inclusive, ser objeto de regulamentação da ANPD.

Destaca-se a necessidade, por parte da ANPD, de esclarecer os requerimentos para o **consentimento de adolescentes**. Embora o legislador tenha permitido que os adolescentes consentissem sem representação ou assistência dos pais, como será defendido abaixo, essas duas salvaguardas adicionais presentes no art. 14, §1º, LGPD, para o tratamento de dados de crianças não parecem ser, em um primeiro momento, aplicáveis a eles.

Considerando que o princípio do melhor interesse deve ser aplicado a toda e qualquer pessoa de até 18 anos incompletos (isto é, a crianças e adolescentes na linguagem do ECA), é indispensável que os adolescentes também contem com essa proteção adicional. Isso é especialmente o caso considerando que eles terão apenas iniciado a sua jornada de maior autonomia na proteção de seus dados pessoais e é preciso considerar que decisões equivocadas poderão ser tomadas ao longo deste caminho. Portanto, considerando a intenção do legislador de oferecer mais proteção a crianças e adolescentes, não faz sentido tratar adolescentes como menos necessitados dos requisitos de um consentimento específico e destacado do que os pais ou responsáveis legais que consentem em nome de crianças.

Por fim, em qualquer caso, é importante ressaltar que o consentimento não deve ser entendido como um mecanismo de legitimação do tratamento de dados de crianças e adolescentes como se adultos fossem. O consentimento é apenas uma das bases legais possíveis e todas as outras regras da LGPD, inclusive o *caput* do art. 14 continuam sendo aplicados. Ademais, **sempre que possível uma análise individual da capacidade da criança poderá ser feita como melhor prática, a fim de verificar as suas capacidades para consentir de forma informada no caso concreto** (DPC, 2021).

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

De maneira geral, as diversas autoridades de proteção de dados ao redor do mundo têm interpretado o conceito de **esforço razoável** a partir de uma abordagem de proporcionalidade baseada em risco (cf. EDPB, 2020; Global Privacy Assembly, 2021). Assim, agentes de tratamento devem analisar todas as opções tecnológicas disponíveis no momento em questão e comparar os riscos e benefícios que elas apresentam com os riscos relativos ao tratamento de dados inicial que requer o consentimento. Esse processo deve estar sempre alinhado aos princípios da LGPD interpretados a partir do princípio do melhor interesse, como o princípio da necessidade.

Caso o tratamento de dados para a atividade em questão gere um risco pequeno aos direitos fundamentais de crianças, os esforços podem se restringir a uma caixa de verificação de idade a partir, por exemplo, da requisição do ano em que o titular de dados nasceu. Após a verificação da faixa de idade, poderia ocorrer uma segunda etapa de envio de e-mail para o pai ou responsável para que este possa fornecer o consentimento. Exemplo claro seria o tratamento de um endereço de e-mail estritamente para o envio de *newsletter* acerca de um artista que a criança acompanha.

Por outro lado, quando o tratamento de dados envolve riscos mais altos para os direitos da criança, os esforços de verificação da idade e, em seguida, do consentimento dado pelo pai ou responsável deve seguir parâmetros mais restritos (para mais detalhes, verificar abaixo a resposta à pergunta 2 da seção "III - Jogos e aplicações de internet"). Este é o caso, por exemplo, da necessidade de tratamento de dados sensíveis em uma situação relacionada à saúde da criança.

Assim como na pergunta anterior, destaca-se a necessidade de a **ANPD esclarecer que as mesmas regras se aplicam para adolescentes**. Defende-se que os mesmos esforços razoáveis devem ser aplicados para a obtenção do consentimento do adolescente, quando este tiver mais de 12 anos, tendo em vista a sua vulnerabilidade.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

O art. 14, §1°, afirma que dados de crianças devem ser tratados com base no consentimento específico e em destaque dado por pelo menos um de seus pais ou representante legal. Essa regra também deve ser interpretada de acordo com o sistema jurídico brasileiro, em especial com o ECA e o regime das incapacidades presente no Código Civil (CC).

O CC apresenta dois níveis de capacidade legal: a chamada capacidade de direito (consequência da personalidade e inerente à condição de ser pessoa) e a capacidade de fato (ligada à capacidade de exercer validamente atos da vida civil por si só, sem a necessidade de um representante ou o assentimento de um assistente).

O CC, define os indivíduos com menos de 16 anos como absolutamente incapazes (art. 3º) e indivíduos com idades entre 16 e 17 anos como relativamente incapazes (art. 4º). Assim, apesar de a Convenção reconhecer as capacidades em evolução e a autonomia progressiva da criança, um modelo estático

puramente baseado na idade prevalece no sistema brasileiro. Todavia, ao longo do tempo, outros dispositivos buscaram mitigar a rigidez do CC, apresentando exceções ao regime geral de incapacidade civil, especialmente quando se trata de **direitos da personalidade**.[5]

Considerando a existência de outras exceções no sistema jurídico brasileiro e o fato de que a LGPD é posterior e especial em relação ao CC, é possível argumentar que **o legislador de fato introduziu uma nova exceção, via *lex specialis*, permitindo que pessoas com 12 anos ou mais consintam para o processamento de seus dados pessoais** sem representação ou assistência.

Apesar de se defender que a LGPD introduziu uma exceção ao regime das incapacidades e que permite que adolescentes deem seu consentimento para o processamento de seus dados pessoais, é preciso recordar que isso se dá ao se privilegiar a **autonomia e o desenvolvimento progressivo das capacidades** da criança e do adolescente. Ao se desenvolver e adquirir novas capacidades, crianças adquirem, também, mais responsabilidade e autonomia para lidar com os seus próprios direitos e matérias relativas à sua vida. Isso é extremamente importante no ambiente digital e o envolvimento de crianças com matérias de proteção de dados pessoais, paulatinamente, é essencial para o desenvolvimento de sua **literacia digital**.

Todavia, é destaca-se que este deve ser enxergado como um **processo que beneficia a própria criança** e não como uma justificativa para o tratamento de dados que seja contrário ao seu melhor interesse. Nesse sentido, com o reconhecimento que adolescentes podem consentir com o tratamento de seus dados pessoais, **métodos de verificação da idade para a introdução de regras mais rígidas e padrões de *design* específicos para a sua navegação online se tornam ainda mais importantes**.

Por fim, importa destacar que a exceção ao regime das incapacidades disposta no art. 14, §1º, da LGPD, deve ser **entendida restritivamente e aplicada exclusivamente ao consentimento fornecido para o processamento de dados pessoais**. Assim, isso não deve impactar a análise de legalidade e o regime de consentimento dado para a celebração de contratos eletrônicos (incluindo Termos de Uso) ou consentimento ético quando, por exemplo, de processamento de dados para finalidade de pesquisas científicas (Teffé & Fernandes, 2022).

Isso demonstra a importância de **momentos separados**, na experiência do usuário, para o consentimento fornecido em contrato eletrônico e o consentimento fornecido para o processamento de dados pessoais. Isso deve ocorrer não apenas pela necessidade de transparência e para que o consentimento seja considerado livre e em destaque, mas também porque pode haver situações em que pais ou responsáveis devem assistir ou representar o adolescente no consentimento para a celebração de contrato, mas em que o adolescente já pode dar consentimento para o processamento de dados pessoais (quando o este tem, por exemplo, entre 12 e 18 anos).

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados

[5] Por exemplo, o art. 1.740, III, do Código Civil, determina que é dever do tutor adimplir os deveres que normalmente cabem aos pais, ouvida a opinião do menor, se este já contar doze anos de idade; e o art. 28, II, do ECA, que prevê a necessidade de consentimento para adoção de adolescentes com mais de doze anos. Cf., também, Teffé e Fernandes (2022).

pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações "estritamente necessárias à atividade".

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de *design*, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

O especial estágio de desenvolvimento de crianças e adolescentes os caracterizam como uma maior vulnerabilidade e demanda que todos os atores da sociedade estejam ativamente envolvidos na **promoção (e não apenas proteção) de seus direitos**, assim como definido pelo art. 227, CRFB. Muitos dos riscos do ambiente online são apenas o resultado de crianças e adolescentes utilizando tecnologias que não foram desenvolvidas para eles (5Rights Foundation, 2021b; Kidron & Rudkin, 2017). Isso faz com que **medidas específicas sejam necessárias por *design* e por padrão não apenas para proteger crianças de riscos, mas para fornecer a elas um ambiente saudável e empoderador para o seu desenvolvimento em todas as áreas**.

Apesar da importância da agência de crianças e adolescentes, assim como de seus pais e responsáveis, a ubiquidade e complexidade das tecnologias atuais faz com que medidas individuais sejam extremamente insuficientes para o controle de dados pessoais. **Essa proteção deve ocorrer de forma coletiva e agir diretamente na arquitetura das plataformas**.

Nesse sentido, propõe-se segmentar potenciais ações como **medidas de restritivas de proteção**, que proíbem ações específicas por parte de agentes de tratamento e **medidas proativas de proteção**, que estão diretamente relacionadas às configurações práticas da aplicação. Embora os limites entre essas categorias não sejam rigorosamente definidos, essa distinção pode ser útil na criação de uma *checklist* de medidas e salvaguardas a serem implementadas. Em ambos os casos, essas medidas podem ser incorporadas no *design* ou configuradas por padrão, diretamente no código da aplicação.

Dentre as **medidas restritivas de proteção** encontram-se proibições específicas de tratamento de dados que são sempre contrários ao princípio do melhor interesse, como para fins de manipulação comercial ou política; publicidade direcionada; exploração da vulnerabilidade e atenção da criança (especialmente através de padrões abusivos e *dark patterns*); direcionamento de conteúdo danoso etc. Também inclui limitações severas ao perfilamento; à vigilância; à coleta de dados específicos como dados sensíveis ou de geolocalização; ao compartilhamento de dados com terceiros; e à retenção de dados pessoais.

Dentre **medidas proativas de proteção** pode-se citar a implementação por padrão das configurações de privacidade mais protetivas; a anonimização ou pseudoanonimização sempre que possível; a minimização extrema do uso de dados pessoais (ver interpretação ao art. 14, §4º, *infra*); a criação de interfaces inclusivas e seguras; a implementação de sistemas de monitoramento de atividades suspeitas ou alertas para controle dos pais; e o ajuste do *design* de acordo com as idades e capacidades da criança e do adolescente.

Estas medidas podem ser consideradas como um resumo do estado da arte existente e já exigido em prática por autoridades e instituições ao redor do mundo (Nesse sentido, cf. Australian eSafety Commissioner, 2024; CNIL, 2021; D4CR Association, 2024; Digital Futures Commission, 2023; DPC, 2021; ICO, 2020; IEEE, 2021; International Telecommunication Union, 2020; Ministerie van Binnenlandse Zaken en Koninkrijsrelaties et al., 2021; Nordic Data Protection Authorities, 2024; Perrino, 2022).

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

A verificação da idade de usuários de serviços digitais é frequentemente vista como necessária e legítima para várias finalidades, incluindo para verificar a legalidade do consentimento como base legal ou da celebração de contrato online; impedir o acesso a conteúdo ou produto não adequados à idade; ou para adaptar o *design* de determinada plataforma e promover melhor proteção. Todavia, é preciso um extremo cuidado com os métodos adotados que podem apresentar **riscos extras aos direitos não só de crianças e adolescentes, mas também ao de adultos em geral** que têm sua idade verificada.

É possível agrupar os processos de **verificação da idade em três categorias**: (i) declaração da idade, (ii) estimação da idade e (iii) verificação a partir de documento oficial, sob as quais estão incluídos diversos métodos diferentes. Cada uma dessas categorias possui **níveis de efetividade e riscos aos direitos fundamentais diferentes** (European Commission et al., 2024) e devem ser analisadas em separado.

A **declaração da idade** pode incluir diversos métodos como clicar em uma caixa em que o usuário declare que possui mais de "x" anos, informar que está em determinada faixa etária (entre "x" e "y" anos) ou fornecer diretamente sua data de nascimento. Esse é o método menos intrusivo, mas a possibilidade de contorna-lo ou burlá-lo é alta e crianças podem mentir a idade. Isso pode ser evitado, por exemplo, através de um segundo fator de verificação como envio de e-mail para pais, *social vouching* (quando um terceiro confirma a idade do usuário), uso de cartão de crédito etc. Ademais, medidas de *design* ou controle parental podem fazer com que essa modalidade seja mais segura.

A **estimação da idade**, como o próprio nome já diz, tem como função estimar a idade do usuário através de métodos como perfilamento de comportamento online, análise de dados biométricos, ou testes de capacidade. Exceto quando se adota o método de teste de capacidade (que é extremamente falho devido à falta de padrões universais de capacidade e da possibilidade de ser contornado), a estimação de idade necessariamente demanda a coleta de mais dados do usuário (Sas & Mühlberg, 2024). Na resposta à próxima pergunta, será discutida, de forma específica, a problemática relativa ao **perfilamento** de crianças e adolescentes, que deve ser evitado e utilizado apenas quando indispensável para a realização do seu melhor interesse. Isso inclui não apenas a mera necessidade (o que poderia ser argumentado no caso da verificação de idade), mas também a **proporcionalidade** deste benefício em relação aos riscos que este método impõe a outros direitos fundamentais.

O tratamento de **dados biométricos** para a estimação de idade apresenta ainda mais desafios devido à sua alta sensitividade. Mesmo nos casos em que empresas afirmam que apenas o dado final relativo à estimação da idade é tratado, dados pessoais biométricos estão disponíveis, mesmo que por um período curto e, com isso, a identificação inequívoca do usuário é possível. Ademais, esse é uma modalidade ainda falha, podendo ser contornada facilmente, funcionando inadequadamente para pessoas negras (European Digital Rights (EDRi), 2023) e não fornecendo uma estimativa precisa da idade do usuário (métodos atuais anunciam uma margem de erro de aproximadamente 1,5 ano — cf. Pôle d'Expertise de la Régulation Numérique (PEReN), 2022). Isso pode gerar resultados falso positivos ou falso negativos, impedindo o acesso de pessoas que deveriam ter permissão e permitindo o acesso a quem não deveria. Por outro lado, a estimativa realizada diretamente no dispositivo do usuário, sem o envio de dados a servidores externos, apesar de menos invasiva, não atenderia adequadamente à necessidade de verificação confiável da idade, devido ao seu caráter altamente probabilístico (Agencia Española de Protección de Datos, 2023).

Por fim, há ainda a possibilidade de **verificação da idade por documento oficial**. Este é o método mais acurado de verificar a idade e geralmente é levado à cabo através do *scan* ou imagem digital do documento (podendo ser integrado com chamada ao vivo com participação de humanos para confirmação — European Commission et al., 2024). Todavia, esse método também apresenta diversos desafios. Isso inclui a exclusão digital daqueles que não possuem acesso a documentação oficial, assim como o fim da anonimidade neste ambiente e da normalização de *age gates* em qualquer interação online. Isso pode minar grande parte dos benefícios da estrutura aberta da internet, como a liberdade de expressão e a autonomia dos usuários (CNIL, 2022), podendo ser extremamente prejudicial àqueles que dependem de um grau adequado de anonimização online, como jornalistas, advogados e defensores de direitos humanos (European Digital Rights (EDRi), 2023). Ademais, também cria riscos de vazamento de dados, roubo de identidade e utilização dos dados para outros fins.

Ao menos em teoria, já existem métodos que buscam solucionar alguns dos problemas identificados acima, como os baseados em "*zero-knowledge proof*". Neste modelo, é possível que indivíduos provem a acurácia de certa informação (que possuem certa idade, por exemplo, sem revelá-la ou revelar sua identidade. Isso é idealmente feito através de um **sistema independente fornecido por terceiros**. Esse modelo ideal já foi, por exemplo, discutido pela autoridade francesa de proteção de dados em 2022 (CNIL, 2022).

Ademais, algo parecido tem sido implementado na União Europeia (2024) através da atualização da eIDAS Regulation. No novo modelo, cada Estado Membro tornará disponível uma carteira digital gratuita e voluntária que possibilita o compartilhamento seletivo de certos atributos (como a idade), sem revelar a identidade do usuário. Quando feito pelo setor público, como no caso da União Europeia, isso certamente gera outros desafios como a aceitação social e confiança do modelo, especialmente para situações mais sensíveis como o acesso a conteúdo adulto. Ademais, o problema de exclusão digital e de pessoas sem documentação permaneceria.

O exposto acima demonstra que **ainda não há ainda uma solução perfeita e universal para o problema**. Todavia, já é possível argumentar que certos modelos são extremamente invasivos e não acurados, devendo ser rechaçados. Esse é o caso por exemplo, de métodos de estimação de idade. Ademais, **métodos tradicionais de verificação através de documentos oficiais devem ser utilizados apenas quando extremamente necessários**, devido ao grande risco imposto a todos os usuários.

A declaração de idade continua sendo o método menos invasivo e os seus desafios podem ser contornados, em certos casos, através de verificação em duas etapas. Ademais, é preciso recordar que o princípio do melhor interesse demanda uma atitude proativa para evitar a necessidade de utilização desses métodos através da **mitigação dos riscos desde o início**. Isso significa que, em determinadas situações, é possível **implementar medidas de proteção de *design* para todos os usuários por padrão**, fazendo com que todos estejam protegidos, não apenas crianças e adolescentes (5Rights Foundation, 2021a).

Isso se aplica, por exemplo, a práticas intrusivas e padrões de *design* problemáticos relativos aos principais modelos de negócio existentes hoje. Assim, nos casos em que não é possível assegurar a implementação do método de verificação com risco proporcional aos direitos fundamentais de crianças e adolescentes, é preciso adotar um padrão universal de proteção (o que é chamado pela autoridade irlandesa de proteção de dados como *floor of protection* — cf. DPC, 2021). O recente caso da parceria entre a Google e a Meta para o direcionamento de marketing para crianças e adolescentes (Morris &

Murphy, 2024) é um grande exemplo de prática que poderia ser evitada ao se regular o modelo de negócio por *design* e se aplicar o princípio do melhor interesse.

Por fim, é preciso incentivar o desenvolvimento de métodos seguros e protetivos à proteção de dados pessoais baseados em *zero knowledge proof*, algo que no Brasil poderia ser feito, por exemplo, através da parceria da ANPD com o sistema gov.br.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

O art. 6º, III, da LGPD, determina que o tratamento de dados pessoais deve ser restringido ao mínimo necessário, relevante, proporcional e não excessivo para alcançar os fins especificados pelo controlados. No entanto, além de reforçar esse princípio, é possível argumentar que o art. 14, §4º, vai além ao utilizar a expressão "estritamente necessário **para a atividade**" (grifo nosso).

De maneira geral, princípio da necessidade disposto no art. 6º está intrinsicamente relacionado ao princípio da finalidade e não existe por si só. Isto é, **o que é considerado necessário sempre dependerá da finalidade para o tratamento de dados pessoais** (que, como discutido acima, deve estar alinhada ao melhor interesse da criança e do adolescente para ser legítima). Assim, caso a finalidade seja legítima e o controlador tenha uma base legal para tratar os dados necessários para essa finalidade, basta que a anuncie em sua política de privacidade e esteja em conformidade com o restante da LGPD.

Todavia, o art. 14, §4º, LGPD, apresenta regra mais restritiva para o tratamento de dados de crianças (titulares de que se trata o §1º do art. 14). Este dispositivo dispõe que os controladores não deverão condicionar a sua participação em jogos, aplicações de internet ou outras atividades ao fornecimento de informações para além das **estritamente necessárias à *atividade***. O legislador cita **jogos e aplicações de internet como exemplos de atividades** (tendo em vista os ter inserido logo antes da expressão "ou outras atividades").

Assim, entende-se que não se trata de dados necessários a determinada finalidade de tratamento de dados, mas sim de **dados necessários para a aplicação prática ou funcional específica, para o serviço ou produto mais amplo que requer o tratamento de dado pessoal**. Embora essa atividade possa envolver diversas finalidades de tratamento, os dados coletados, observados ou inferidos devem ter uma relação direta com a atividade em questão.

Nesse sentido, apenas mencionar outras finalidades nos termos de serviço não é suficiente para coletar dados além dos **principais objetivos da aplicação**. Pode-se pensar, por exemplo, na situação de tratamento de dados pessoais em uma aplicação com fins educacionais. O tratamento de dados deve ser reservado estritamente para possibilitar o funcionamento básico da aplicação para os fins educacionais, não sendo possível tratar dados, por exemplo, para direcionamento de publicidade, melhoramento de outros serviços ou treinamento de sistemas de inteligência artificial, seja por parte do controlador, seja de terceiros. Isso deve ocorrer **mesmo que a finalidade seja legítima**, pois a análise da conformidade com os diferentes princípios deve ocorrer de forma separada.

Esta é uma regra extremamente importante no âmbito da LGPD, que **protege os dados das crianças desde o momento da coleta** e impede que sejam acumulados em larga escala para fins não relacionados ao propósito principal da aplicação ou jogo em que a criança está envolvida. Portanto, os dados pessoais coletados devem aderir estritamente ao que é indispensável e justificável (Zanatta et al., 2021), o que também está **alinhado ao princípio da boa-fé**.

Destaca-se que essa interpretação mais restritiva em relação aos princípios da finalidade e necessidade é uma tendência mundial. Já em seu comentário sobre o princípio da finalidade em 2013, o Article 29 Data Protection Working Party (WP29), antecessor do European Data Protection Board, já afirmava que quanto mais sensível o dado (e, no documento, isso é estendido para dados de crianças e adolescentes), mais restrita deve ser a interpretação destes princípios, inclusive para a análise de finalidades compatíveis quando do uso secundário de dados (WP29, 2013, p. 25) — **o que, destaca-se poderia também ser objeto de regulação por parte da ANPD, tendo em vista a falta de parâmetros claros para uso secundário de dados na LGPD**.

No âmbito dos Estados Unidos da América (EUA), a Federal Trade Commission (FTC), responsável pela aplicação do COPPA, publicou uma *Notice of Proposed Rulemaking* (NPRM) a fim de propor mudanças à legislação. De acordo com a FTC Chair, Lina M. Khan, **crianças devem poder brincar e aprender no ambiente digital sem serem rastreadas por empresas que procuram rentabilizar os seus dados pessoais**. A proposta impõe obrigações diretas aos prestadores de serviços, incluindo a proibição do uso comercial de dados de crianças — inclusive para o desenvolvimento de serviços; **a proibição de condicionar a participação de uma criança em um serviço digital à coleta de informações pessoais** (o que está bastante alinhado ao art. 14, §4º, da LGPD), e limites para incentivar crianças a permanecerem online (Federal Trade Commission (FTC), 2023).

Por fim, especificamente no que se concerne ao perfilamento, é preciso destacar que este pode ocorrer para diversas finalidades. De forma mais óbvia, como já defendido acima, ele não seria compatível com o melhor interesse de crianças e adolescentes quando é realizado para fins comerciais. Todavia, ele pode ocorrer para outras finalidades, como no caso de tecnologias de educação que buscam aplicar metodologias de ensino personalizado. Neste caso, é essencial que o agente de tratamento demonstre que este **perfilamento de crianças é indispensável para alcançar uma finalidade consistente com o seu melhor interesse**. Ademais, essa indispensabilidade deve ser **baseada em evidências científicas claras e no princípio da precaução** (o que, como defendido em outra instância, não é o caso de tecnologias de ensino personalizado — cf. Fernandes, 2024).

Isso, pois o perfilamento em si, independentemente da finalidade de tratamento, pode afetar diretamente diversos direitos fundamentais de crianças. Riscos dessa automaticidade vão desde o vazamento de dados e roubo de identidade, até a limitação de oportunidades devido a erros e vieses (Van Der Hof et al., 2020). Nesse sentido, em seu Comentário Geral Nº 25, o Comitê sobre os Direitos da Criança (2021, parag. 42) defende que Estados Membros proíbam o uso de perfilamento de crianças e adolescentes para finalidades comerciais, incluindo dados coletivos ou de grupos (proibição que já é reconhecida no DSA da União Europeia, como destacado acima).

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

O controle parental pode ser entendido como qualquer medida utilizadas por pais ou responsáveis legais para adaptar a experiência online de crianças e adolescentes. Isso pode ser feito, por exemplo, através de mecanismos de imposição de limites de uso, como temporizadores e bloqueios de determinados sites, ou então do controle de acesso a informações da criança ou adolescente por determinado website. Esta é uma **forma extremamente importante de incluir pais e responsáveis na proteção de direitos de crianças e adolescentes online**, assim como demandado pelo art. 227, da CRFB. Todavia, **é preciso reconhecer, também, os seus limites**.

O primeiro limite a ser reconhecido diz respeito à relação estabelecida entre as partes envolvidas. **Crianças e adolescentes também precisam de um espaço de privacidade em relação aos seus pais ou responsáveis** para que possam desenvolver sua identidade de maneira saudável. Portanto, qualquer medida adotada nesse sentido deve ser sempre **necessária e proporcional**, levando em consideração o princípio do melhor interesse. Essas medidas devem ser **transparentes**, de modo que crianças e adolescentes estejam cientes de que suas experiências estão sendo monitoradas ou moldadas de alguma forma. A comunicação sobre essas medidas também deve ser adequada à idade e às capacidades da criança ou adolescente, respeitando sua autonomia progressiva.

O segundo limite refere-se à própria **função do controle parental**. A existência de controles parentais ou a possibilidade de ajuste das configurações de privacidade por pais ou responsáveis não deve servir como justificativa para padrões de *design* que não estejam alinhados com o melhor interesse da criança, **nem para transferir aos pais a responsabilidade de decidir sobre questões complexas de tratamento de dados**. Assim, as decisões tomadas por pais ou responsáveis devem ser sempre secundárias a *designs* que protejam, por padrão, os interesses da criança e do adolescente.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

A disponibilização de informações de maneira clara e acessível para crianças e adolescentes sobre o tratamento de seus dados pessoais desempenha um papel crucial no **reconhecimento desse grupo como sujeitos de direitos**, que, desde o início, foi o principal objetivo da Convenção. Embora esses direitos muitas vezes sejam exercidos com a representação ou assistência de pais ou responsáveis legais, eles continuam a pertencer, em essência, às crianças e adolescentes.

Adaptar a comunicação sobre o tratamento de dados pessoais é o **primeiro passo para empoderar esses indivíduos no ambiente digita**l, auxiliando-os a desenvolver a literacia digital, a compreender o impacto negativo e positivo do tratamento de dados em seus direitos e, em última análise, a exercê-los de forma consciente. De toda forma, porém, é preciso enxergar essa realização do princípio da transparência como a base mínima para a proteção dessas pessoas no ambiente digital, sem que isso signifique transferir de forma completa a responsabilidade pela proteção de dados para as crianças ou seus pais e responsáveis.

Diversas instituições ao redor do mundo já se debruçaram sobre o tema e a ANPD pode se beneficiar de trabalhos que buscaram estudar a compreensão de crianças e adolescentes sobre informações acerca do tratamento de seus dados pessoais. Isso não quer dizer, porém, que os resultados dessas análises possam ser aplicados, diretamente, à realidade brasileira, o que **demandaria, por parte da autoridade, estudos empíricos específicos com crianças do país para confirmar a eficácia destes métodos**. De toda forma, acredita-se que muitos dos princípios básicos possam ser aproveitados.

Tendo em vista a complexidade do tema e a falta de espaço adequado para a discussão de todas as suas nuances, indica-se como ponto de partida o trabalho recente realizado por Sas, Denoo e Mühlberg (2023), que **mapearam as diversas estratégias de comunicação apropriada à idade sugeridas por autoridades de proteção de dados, organizações de proteção à criança e adolescente, assim como a literatura científica**. Essas estratégias são classificadas em sete categorias que fazem parte de uma matriz de avaliação: linguagem, tamanho, formato de comunicação, acessibilidade, técnicas de *nudge*, momento e envolvimento parental. Apesar de nem todas as estratégias serem específicas para crianças, estas podem se beneficiar enormemente de sua implementação.

Por fim, é essencial lembrar que todas essas estratégias devem levar em conta a diversidade dentro do grupo de crianças e adolescentes, reconhecendo que diferentes faixas etárias possuem entendimentos e necessidades distintas. Assim, **a comunicação deve ser adaptada de acordo com o público-alvo**. Por exemplo, crianças de até cinco anos têm um nível de compreensão e necessidades específicas, dependendo muito mais de seus pais ou responsáveis do que adolescentes de 15 anos, que já possuem maior autonomia e capacidade de lidar com questões relacionadas à própria vida. Portanto, é crucial que a abordagem seja ajustada para **atender adequadamente às diferentes etapas de desenvolvimento**, garantindo que todos recebam a informação de maneira eficaz e apropriada.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

Para além das questões já discutidas acima, indica-se uma atenção especial à regulação dos seguintes temas:

- O exercício dos direitos de titulares por crianças;
- A realização do RIPD e a sua relação com o CRIA;
- A regulação de bases legais específicas, como a interpretação do que significa tratar dados para a proteção da criança, conforme art. 14, §3º, LGPD;
- A regulação do uso de bases legais do art. 7º, LGPD, como execução de contrato ou proteção ao crédito;
- O tratamento de dados em situações específicas, como no âmbito da educação (incluindo regras sobre a inclusão de medidas de proteção de crianças por *design* em processos licitatórios);
- Medidas especiais de cyber segurança para a proteção de dados de crianças e adolescentes;
- Medidas de educação digital para pais e responsáveis para a sua conscientização dos problemas relacionados à divulgação excessiva de dados e da imagem de crianças e adolescentes (*over-sharenting*).

==========

REFERÊNCIAS

5Rights Foundation. (2021a). *But how do they know it is a child? Age Assurance in the Digital World*. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

5Rights Foundation. (2021b). *Pathways: How digital design puts children at risk*. https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

Agencia Española de Protección de Datos. (2023). *Frequently Asked Questions (FAQ) about the Proofs of Concept (PoCs) of systems for age verification and protection of minors from inappropriate content*. https://www.aepd.es/guides/faq-proof-of-concept-age-verification-systems.pdf

ANPD. (2022a). *Estudo Preliminar: Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf

ANPD. (2022b). *Nota Técnica Nº 46/2022/CGF/ANPD*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000730_2022_53-nt-46.pdf

ANPD. (2022c). Portaria ANPD Nº 35, de 4 de Novembro de 2022. Torna Pública a Agenda Regulatória para o biênio 2023-2024, Pub. L. No. 35, Diário Oficial da União. https://in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885

ANPD. (2023a). *ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes*. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes

ANPD. (2023b). *Nota Técnica nº 6/2023/CGF/ANPD*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica.pdf

ANPD. (2023c). *Nota Técnica nº 12/2023/CGF/ANPD*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-12-2023-cgf-anpd-inep.pdf

ANPD. (2023d). Resolução CD/ANPD Nº 11, de 27 de Dezembro de 2023. Altera a Agenda Regulatória para o biênio 2023-2024, Diário Oficial da União (2023). https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/resolucao_cd_anpd_11_2023-27122023.pdf

ANPD. (2024a). *Guia Orientativo. Hipóteses legais de tratamento de dados pessoais: Legítimo Interesse*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

ANPD. (2024b). *ANPD abre Tomada de Subsídios para projeto regulatório sobre crianças e adolescentes*. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-para-projeto-regulatorio-sobre-criancas-e-adolescentes

Australian eSafety Commissioner. (2024). *Safety by Design*. https://www.esafety.gov.au/industry/safety-by-design

Brasil. (2017). Supremo Tribunal Federal. Suspensão de Liminar nº 1103. Requerente: Instituto Brasileiro de Geografia e Estatística - IBGE. Requerido: Tribunal Regional Federal da 3ª Região. Interessado: Ministério Público Federal. Relator: Ministra Cármen Lúcia. Brasília, 2 de maio de 2017. **Diário Oficial da União**. n. 95.

Brochado Teixeira, A. C., & Rettore, A. C. de C. (2024). O Princípio do Melhor Interesse no Ambiente Digital. In E. Fernandes, C. de Teffé, & S. Branco (Orgs.), *Privacidade e Proteção de Dados de Crianças e Adolescentes* (2º ed). Instituto de Tecnologia e Sociedade do Rio.

Commissão Europeia. (2022). Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52022PC0209

Committee on the Rights of the Child. (2009). *General Comment No. 12 (2009). The right of the child to be heard. CRC/C/GC/12*. https://www.refworld.org/legal/general/crc/2009/en/70207

Committee on the Rights of the Child. (2013). *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14*. https://www.refworld.org/legal/general/crc/2013/en/95780

Committee on the Right of the Child. (2016). *General comment No. 20 (2016) on the implementation of the rights of the child during adolescence. CRC/C/GC/20*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/404/44/PDF/G1640444.pdf?OpenElement

Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25*. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

CNIL. (2021). *CNIL publishes 8 recommendations to enhance the protection of children online*. https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online

CNIL. (2022, setembro 22). *Online age verification: balancing privacy and the protection of minors*. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

D4CR Association. (2024). *Designing for Children's Rights*. http://designingforchildrensrights.org/

Digital Futures Commission. (2021, fevereiro 22). *The best interests of children in the digital world*. https://digitalfuturescommission.org.uk/blog/the-best-interests-of-children-in-the-digital-world/

Digital Futures Commission. (2023). *Child Rights by Design*. https://childrightsbydesign.digitalfuturescommission.org.uk

DPC. (2021). *Children front and centre: Fundamentals for a child-oriented approach to data processing*. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

EDPB. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EDPB & EDPS. (2022). Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

European Commission, Directorate-General for Communications Networks, Content and Technology, Raiz Shaffique, M., & van der Hof, S. (2024). *Research Report: Mapping age assurance typologies and requirements*. https://data.europa.eu/doi/10.2759/455338

European Digital Rights (EDRi). (2023). *Position paper - Online age verification and children's rights*. https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf

Federal Trade Commission (FTC). (2023). *FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data*. https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens

Fernandes, E. (2024). Ensino personalizado: desafios à proteção de dados de crianças e adolescentes. In E. Fernandes, C. S. de Teffé, & S. Branco (Orgs.), *Privacidade e Proteção de Dados de Crianças e Adolescentes* (2º ed). Instituto de Tecnologia e Sociedade do Rio (ITS-Rio).

Fernandes, E., & Medon, F. (2021). Proteção de crianças e adolescentes na LGPD: desafios interpretativos. *Revista Eletrônica da PGE-RJ*, *4*(2), 1–24. https://doi.org/10.46818/pge.v4i2.232

Global Privacy Assembly. (2021). *Adopted Resolution on children's digital rights*. https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf

Hof, S. van der, & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. *Communications Law: The Journal of Computer, Media and Telecommunications Law*, *23*(1), 33–43. https://infolawcentre.blogs.sas.ac.uk/files/2018/03/Comms_Law_23.1.pdf

ICO. (2020). *Age appropriate design: a code of practice for online services*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

IEEE. (2021). *IEEE publishes new standard to address age appropriate design for children's digital services*. https://standards.ieee.org/news/ieee-2089/

Information Commissioner's Office (ICO). (2024). *The full best interests framework and UNCRC*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/best-interests-framework/the-full-best-interests-framework-and-uncrc/

International Telecommunication Union. (2020). *Guidelines for industry on Child Online Protection*. https://www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf

Kidron, B., & Rudkin, A. (2017). *Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment*. https://5rightsfoundation.com/static/Digital_Childhood_report_-_EMBARGOED.pdf

Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024). *The best interests of the child in the digital environment*. https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf

Lundy, L., & Byrne, B. (2017). The four general principles of the United Nations Convention on the Rights of the Child: the potential value of the approach in other areas of human rights law. In E. Brems, Desmet Ellen, & W. Vandenhole (Orgs.), *Children's Rights Law in the Global Human Rights Landscape: Isolation, Inspiration, Integration?* (p. 52–70). Routledge.

Ministerie van Binnenlandse Zaken en Koninkrijsrelaties, Universiteit Leiden, & waag technology & society. (2021). *Code voor Kinderrechten*. https://codevoorkinderrechten.nl/

Morris, S., & Murphy, H. (2024, agosto 8). Google and Meta struck secret ads deal to target teenagers. *Financial Times*. https://www.ft.com/content/b3bb80f4-4e01-4ce6-8358-f4f8638790f8?countryCode=BEL

Mukherjee, S., Pothong, K., & Livingstone, S. (2021). *Child Rights Impact Assessment: A Tool to Realise Children's Rights in the Digital Environment*. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf

Nordic Data Protection Authorities. (2024). *Principles on Children & Online Gaming*. https://www.datatilsynet.no/contentassets/97e47a7795b34267a17021253dfe284e/principles-on-children-and-online-gaming.pdf

Payne, L. (2019). Child rights impact assessment as a policy improvement tool. *International Journal of Human Rights*, *23*(3), 408–424. https://doi.org/10.1080/13642987.2018.1558989

Perrino, J. (2022, julho 26). Using 'safety by design' to address online harms. *Brookings*. https://www.brookings.edu/articles/using-safety-by-design-to-address-online-harms/

Pôle d'Expertise de la Régulation Numérique (PEReN). (2022). *Online underage users detection: can we reconcile efficiency, convenience and anonymity?* https://www.peren.gouv.fr/rapports/2022-06-23%20-%20Eclairage-sur-detection-mineurs_EN.pdf

União Europeia. (2022). Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais), OJ L 277, 27.10.2022, p. 1-102. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R2065

União Europeia. (2024). Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho de 11 de abril de 2024 que altera o Regulamento (UE) n.o 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital, OJ L 257, 28.8.2014, p. 73–114. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202401183

Ruggiero, R. (2022). Article 3: The Best Interest of the Child. In Z. Vaghri, J. Zermatten, G. Lansdown, & R. Ruggiero (Orgs.), *Monitoring State Compliance with the UN Convention on the Rights of the Child: An Analysis of Attributes* (p. 21–29). Springer.

Sas, M., Denoo, M., & Mühlberg, J. T. (2023). Informing Children about Privacy: A Review and Assessment of Age-Appropriate Information Designs in Kids-Oriented F2P Video Games. *Proceedings of the ACM on Human-Computer Interaction*, *7*. https://doi.org/10.1145/3611036

Sas, M., & Mühlberg, J. T. (2024). *Trustworthy Age Assurance? A risk-based evaluation of available und upcoming age assurance technologies from a fundamental rights perspective*. https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf

Teffé, C. S. de, & Fernandes, E. (2022). Contratação em redes sociais e proteção de dados de crianças e adolescentes. In A. V. Roque & M. D. Oliva (Orgs.), *Direito na era digital: aspectos negociais, processuais e registrais* (p. 97–122). Editora Jus Podivm.

Termo de Ajustamento de Conduta - Autocomposição (2018). https://www.mpf.mp.br/sp/sala-de-imprensa/docs/tac-ibge.pdf

UNICEF, & Danish Institute for Human Rights. (2013). *Children's Rights in Impact Assessments. A guide for integrating children's rights into impact assessments and taking action for children*. https://sites.unicef.org/csr/css/Children_s_Rights_in_Impact_Assessments_Web_161213.pdf

Van Der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The Child's Right to Protection against Economic Exploitation in the Digital World. *International Journal of Children's Rights*, *28*(4), 833–859. https://doi.org/10.1163/15718182-28040003

Verdoodt, V. (2020). *Children's rights and commercial communication in the digital era: Towards an empowering regulatory framework for commercial communication*. Intersentia.

WP29. (2013). *Opinion 03/2013 on purpose limitation*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Zanatta, R., Valente, J., & Mendonça, J. (2024). Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. In E. Fernandes, C. de Teffé, & S. Branco (Orgs.), *Privacidade e Proteção de Dados de Crianças e Adolescentes* (2º ed). Instituto de Tecnologia e Sociedade do Rio.

Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (Ibrac) - Grupo de Trabalho de Proteção de Dados do Comitê de Regulação

Contribuição do IBRAC à Tomada de Subsídios sobre o Tratamento de Dados Pessoais de Crianças e Adolescentes da ANPD

Em 18/06/2024, a Autoridade Nacional de Proteção de Dados brasileira (ANPD) abriu uma Tomada de Subsídios para colher contribuições que possam apoiar a Análise de Impacto Regulatório e a posterior implementação de ações de normatização/regulatórias relacionadas ao tratamento de dados pessoais de crianças e adolescentes.

Cumpre notar que a ANPD também realizou, em 08/08/2024, um Webinário para ouvir a opinião de especialistas sobre os pontos relacionados ao tratamento de dados pessoais de crianças e adolescentes, colher subsídios para a análise e escolha das opções disponíveis para a regulamentação e levar o conhecimento e debate à população.

Ademais, de acordo com a Agenda Regulatória da ANPD para o biênio 2023-2024, o tratamento de dados pessoais de crianças e adolescentes teve seu processo regulatório iniciado durante a vigência da Agenda Regulatória para o biênio 2021-2022, tendo prevalência sobre os demais itens constantes da Agenda Regulatória.

Levando em consideração o contexto supracitado, visando auxiliar a ANPD em seu processo regulatório e na construção de um ambiente jurídico seguro de proteção de dados pessoais, o Grupo de Trabalho de Proteção de Dados Pessoais do Comitê de Regulação do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (Ibrac) vem, através do presente documento, apresentar suas contribuições à Tomada de Subsídios sobre o Tratamento de Dados Pessoais de Crianças e Adolescentes.

Tomada de Subsídios ANPD – Tratamento de Dados Pessoais de Crianças e Adolescentes

I - Princípio do melhor interesse

De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança, [1] no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU [2] e no Comentário Geral n° 25, de 2021, do Comitê dos Direitos da Criança. [3] Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz.

[1] FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). Convenção sobre os Direitos da Criança. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em 12 jun 2024.

[2] UNITED NATIONS. General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em 12 jun 2024.

[3] 8 UNITED NATIONS. General comment No. 25 (2021) on children's rights in relation to the digital environment. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em 12 jun 2024.

Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, questiona-se:

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD? [4200 caracteres]

A ANPD ressaltou a importância de adotar o princípio do melhor interesse nas discussões sobre a proteção de crianças e adolescentes, mas não definiu

claramente o escopo desse princípio. Embora tenha se baseado em diretrizes da OCDE e da ONU para delinear o 'melhor interesse' de crianças e adolescentes, essas orientações ainda não oferecem segurança suficiente para que os controladores de dados atuem com confiança no contexto da proteção de dados pessoais, conforme o Guia do Legítimo Interesse. Portanto, é crucial que a autoridade aproveite a oportunidade para esclarecer o que constitui o melhor interesse de crianças e adolescentes no âmbito da proteção de dados, especialmente considerando as particularidades da interpretação deste princípio nesta seara. Por exemplo, ao avaliar mecanismos de verificação de idade, que muitas vezes requerem maior coleta de dados para maior precisão, surge a questão: o que deve prevalecer como o melhor interesse da criança e do adolescente? Mecanismos mais precisos ou a adesão rigorosa ao princípio da minimização de dados?

O Comentário Geral n.º 25 da Convenção sobre os Direitos da Criança da ONU destaca a importância de considerar as particularidades de cada contexto específico nessa definição. Diante das diversas realidades e desigualdades socioeconômicas que afetam o acesso de crianças e adolescentes aos meios de comunicação, bem como os diferentes contextos e modelos de negócios, é fundamental que a ANPD dê maior concretude ao conceito de melhor interesse. Isso poderia ser feito por meio de exemplos práticos e situações hipotéticas, elucidando os critérios que serão aplicados na proteção de dados de crianças e adolescentes no ambiente digital.

Sugere-se que a ANPD continue a fornecer orientações claras sobre o que constitui o melhor interesse da criança e do adolescente em situações específicas, especialmente por meio de guias e documentos com eficácia geral. Esses documentos, alinhados com o conceito de crianças e adolescentes estabelecido pelo ECA, ofereceriam maior segurança jurídica, permitindo que os agentes ajustem suas práticas de acordo com parâmetros estabelecidos.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas. [4200 caracteres]

Considerando os diferentes contextos socioeconômicos não apenas de crianças e adolescentes, mas também de seus pais e responsáveis, é fundamental que a Autoridade dê especial atenção ao definir o melhor interesse em situações concretas. A diversidade dessas realidades traz consigo múltiplas possibilidades de garantir, ou não, a observância desse princípio, o que, dada a sensibilidade do tema, requer uma abordagem cuidadosa. Em certos cenários, o princípio do melhor interesse precisa ser equilibrado com outros princípios da LGPD — como a tensão entre acurácia e minimização de dados, por exemplo. Esses são os casos que exigem um esforço adicional de esclarecimento por parte da Autoridade.

Além disso, dado que a cultura de proteção de dados pessoais no Brasil ainda está em processo de consolidação, é natural que haja dificuldades em compreender e aplicar os parâmetros que a ANPD usará em situações práticas. Por isso, é de suma importância que sejam estabelecidas diretrizes claras para orientar os agentes na tomada de decisões em diferentes contextos. Isso inclui, por exemplo, orientações específicas sobre as regras que as redes sociais devem seguir na coleta e armazenamento de informações, sobre mecanismos de verificação e identificação de idade, e nas particularidades do uso de dados pessoais de crianças e adolescentes para fins de direcionamento de conteúdo. Nesse contexto, é crucial distinguir a personalização do conteúdo exibido da publicidade direcionada, visto que, nesse caso, a personalização visa, em muitos casos, proteger as crianças e adolescentes.

II - Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais? [4200 caracteres]

Vale destacar que o consentimento nem sempre será a base legal mais adequada para o tratamento de dados pessoais de crianças e adolescentes, conforme indicado pela ANPD em documentos como o Enunciado nº 01/2023 e o Guia de Legítimo Interesse. No entanto, quando o consentimento parental é necessário, ele deve ser adequado ao contexto específico entre o titular, o responsável legal e o agente de tratamento. Isso implica que diferentes situações demandam abordagens personalizadas. Por exemplo, em interações que ocorrem exclusivamente offline, não faria sentido exigir um consentimento digital "específico e em destaque", assim como o inverso.

Além disso, é importante notar que os termos "específico e em destaque" não têm o mesmo significado que "livre, informado e inequívoco" na LGPD. Por isso, a ANPD precisa esclarecer a que se refere a especificidade — se está relacionada às finalidades do tratamento, ao titular em particular, ou ao conjunto de dados.

No que tange ao "destaque", isso geralmente significa que a informação deve ser destacada em relação a outras. Contudo, seria útil que a ANPD detalhasse se isso envolve a utilização de elementos visuais específicos, como cores e fontes que garantam uma diferenciação clara. Exemplos de boas práticas poderiam incluir o uso de pop-ups, banners destacados, animações ou ícones chamativos, alertas com cores contrastantes, entre outros, para assegurar que o consentimento seja claramente visível.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança? [4200 caracteres]

Quando o consentimento é adotado como base legal, especialmente no tratamento de dados pessoais de crianças e adolescentes, é fundamental que sua obtenção seja a menos invasiva possível em termos de privacidade, conforme reconhecido por autoridades internacionais. A Children's Online Privacy Protection Rule (COPPA), sob a administração da FTC, apesar de estabelecer o consentimento dos pais ou responsáveis como regra, também prevê exceções claras e objetivas.

A ANPD deve levar em consideração os esforços razoáveis empreendidos pelos controladores para obter e verificar o consentimento parental, utilizando métodos acessíveis e proporcionais ao contexto específico. Por exemplo, no setor financeiro, onde a validação biométrica já é amplamente utilizada, a documentoscopia — que consiste na análise de documentos para comprovar a identidade — pode ser uma solução viável. Este método, recomendado pelo COPPA, envolve a verificação de uma foto de uma identificação oficial enviada pelo pai ou responsável, comparada com uma segunda foto utilizando tecnologia de reconhecimento facial.

Além disso, é crucial que a autoridade reconheça que não existem mecanismos infalíveis, e todos estão sujeitos a algum nível de vulnerabilidade. O IBRAC destaca a importância de considerar este aspecto ao determinar a responsabilidade dos agentes de tratamento em casos de falhas nos mecanismos de consentimento.

Imposições desproporcionais e onerosas aos agentes de tratamento podem comprometer a eficácia dos processos e serem ignoradas pelos usuários, contrariando os objetivos da LGPD. Considerando que a cultura de proteção de dados no Brasil ainda está em desenvolvimento, é prudente que a autoridade evite estabelecer parâmetros excessivamente rígidos, cuja conformidade possa ser inviável, sem prejuízo de revisões futuras.

A obtenção do consentimento dos pais ou responsáveis deve observar os princípios de razoabilidade, proporcionalidade e minimização, garantindo que o esforço exigido para obtê-lo não seja excessivo ou desnecessário. É essencial oferecer uma variedade de mecanismos para que o controlador possa escolher o que melhor se adapta à sua realidade específica, sem causar impacto negativo significativo em suas operações. Assim, o processo de consentimento pode ser ajustado às necessidades operacionais do controlador, assegurando, ao mesmo tempo, a proteção e os direitos dos menores envolvidos

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais? [4200 caracteres]

Embora a obtenção do consentimento seja uma base legal importante para o tratamento de dados pessoais de crianças e adolescentes, nem sempre será a mais apropriada, dependendo do caso concreto. Compreender esse elemento como o único possível pode levar a restrições excessivas, mesmo quando o tratamento é realizado no melhor interesse da criança.

Um exemplo dessa necessidade de ponderação é o posicionamento da ANPD no Enunciado nº 1/2023. Esse enunciado estabelece que é possível utilizar as hipóteses legais previstas no art. 7º da LGPD, incluindo o legítimo interesse, para o tratamento de dados pessoais de crianças e adolescentes, além das disposições do art. 11 da mesma lei, sempre observando o princípio do melhor interesse da criança ou adolescente. Tal posicionamento é reforçado no Guia de Legítimo Interesse, que oferece orientações para controladores sobre a interpretação e a aplicação prática dessa hipótese legal, precedida da realização de um teste de balanceamento.

No entanto, se o consentimento for a base legal escolhida para o tratamento de dados de crianças e adolescentes, é crucial que a autoridade reguladora considere alguns aspectos.

Primeiro, a legislação brasileira apresenta diferentes definições e capacidades legais para crianças e adolescentes, o que pode causar ambiguidades na aplicação do consentimento como base legal. O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) define "criança" como a pessoa até 12 anos e "adolescente" como aquela entre 12 e 18 anos. O Código Civil Brasileiro estabelece que menores de 16 anos são absolutamente incapazes de exercer pessoalmente os atos da vida civil e aqueles com mais de 16 e menos de 18 anos são relativamente capazes, podendo praticar atos da vida civil desde que assistidos. A definição exata de "atos da vida civil" não é clara, criando uma zona cinzenta que pode complicar a aplicação do consentimento como base legal, especialmente em situações que exigem um entendimento preciso das capacidades legais desses menores.

Segundo, o melhor interesse deve refletir a autonomia progressiva e o desenvolvimento desses indivíduos, podendo tornar desnecessária a representação ou assistência pelos pais ou responsáveis legais. Conforme reconhecido pelo Estatuto da Criança e do Adolescente (ECA), a autonomia progressiva estabelece que crianças e adolescentes devem ter sua capacidade de decisão respeitada e ampliada à medida que crescem e amadurecem. Isso cria um cenário complexo, em que as disposições do Código Civil, ao tratar

menores de 16 anos como uma massa homogênea incapaz, podem obstruir o melhor interesse da criança e do adolescente. Em contraste, outras jurisdições, como o Reino Unido, permitem que crianças a partir dos 13 anos forneçam seu próprio consentimento para o processamento de dados no contexto de serviços online, conforme definido no Age Appropriate Design Code (Best interests of the child; Annex B). Além disso, o GDPR permite que os Estados Membros da União Europeia estipulem, por lei, uma idade inferior a 16 anos para o tratamento de dados pessoais de menores sem autorização do responsável legal, desde que essa idade não seja inferior a 13 anos. Portanto, em alinhamento com os padrões internacionais de obtenção de consentimento como base legal e em respeito à autonomia progressiva dos menores, é importante que o posicionamento da ANPD reflita adequadamente o desenvolvimento individual e as capacidades crescentes de decisão dos jovens.

Ademais, se a obtenção de consentimento seguir as disposições do direito civil sobre representação e assistência de pais ou responsáveis dos adolescentes, é crucial que a autoridade reguladora esclareça alguns requisitos. Por exemplo, não há uma disposição específica no ordenamento jurídico brasileiro sobre como deve ser obtida a representação ou assistência e se, de fato, é necessária a obtenção de autorização explícita dos pais ou responsáveis por menores. Assim, é importante que a ANPD esclareça em quais situações o consentimento dos pais ou responsáveis é indispensável.

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações “estritamente necessárias à atividade”.

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar “as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança”.

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de design, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os

mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas? [4200 caracteres]

A ANPD deve fornecer orientações claras aos controladores sobre como equilibrar a minimização de dados com o melhor interesse de crianças e adolescentes, estabelecendo parâmetros precisos para a coleta adequada de informações e as medidas de segurança necessárias para protegê-las. Isso inclui diretrizes sobre o uso de técnicas como pseudonimização e criptografia, bem como a importância de realizar avaliações de impacto à proteção de dados para identificar e mitigar riscos.

Além disso, é fundamental que a ANPD ofereça diretrizes de boas práticas às plataformas digitais sobre como comunicar de forma clara e acessível a menores e seus responsáveis quais dados estão sendo coletados, a finalidade dessa coleta e como esses dados serão utilizados e protegidos. Nesse contexto, é relevante mencionar a Resolução nº 245 de 2024, do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA), que estabelece como as plataformas devem incorporar os direitos de crianças e adolescentes ao longo de todo o ciclo de vida de seus produtos. Entre os princípios orientadores estão a não discriminação, a primazia dos direitos da criança e do adolescente, o respeito à liberdade de expressão e consciência, o acesso à informação, a autonomia progressiva, e o desenvolvimento da personalidade, dignidade, honra e imagem.

Na implementação das medidas de privacy by design e privacy by default, é crucial que a autoridade reguladora oriente os agentes de tratamento sobre como equilibrar essas medidas com o respeito ao direito à autonomia progressiva das crianças e adolescentes. Um exemplo a ser considerado é o Age Appropriate Design Code do Reino Unido, que recomenda configurações padrão de "alta privacidade", a menos que haja uma justificativa forte para o contrário, sempre levando em conta o melhor interesse da criança. A ANPD deveria avaliar a viabilidade de adotar medidas mais protetivas como padrão, ao mesmo tempo oferecendo flexibilidade aos usuários para ajustá-las conforme necessário.

Em alinhamento com o melhor interesse da criança, a ANPD poderia também sugerir medidas que permitam supervisão parental adequada, garantindo que os pais desempenhem um papel ativo na proteção dos dados dos menores, especialmente em ambientes digitais. Por fim, a autoridade deve orientar sobre a implementação de canais eficazes para o recebimento de denúncias relacionadas ao uso indevido de contas de crianças, além de mecanismos ágeis para a remoção dessas contas e a proteção dos dados envolvidos.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais? [4200 caracteres]

É essencial reconhecer que as técnicas disponíveis no mercado para verificação de idade são variadas, assim como os modelos de negócios e setores onde são aplicadas. Elas diferem em termos de eficácia, invasão à privacidade e segurança dos dados dos titulares, e esses fatores devem ser cuidadosamente avaliados em sua implementação, considerando os trade-offs envolvidos.

Por exemplo, a autodeclaração, onde o próprio titular informa sua idade sem verificação externa, pode comprometer a acurácia. Outras técnicas, que buscam determinar a idade por meio de inferências, utilizando questionários, históricos de navegação ou análise do comportamento online, embora mais precisas, podem apresentar riscos de discriminação ao associar faixas etárias com habilidades como leitura, compreensão, proficiência linguística e referências culturais.

A verificação de idade através de cartão de pagamento tem a vantagem de utilizar uma infraestrutura já existente e confiável. O sistema valida o cartão sem necessariamente processar um pagamento, embora alguns verificadores possam realizar um micropagamento que é imediatamente cancelado. Esse método pode ser utilizado até mesmo em sites gratuitos para restringir o acesso de menores. No entanto, como os sistemas de pagamento não foram concebidos para verificar atributos como a idade do titular, sua eficácia é limitada. Ainda assim, é uma barreira útil, pois, conforme a legislação brasileira, menores de idade não podem ser titulares de cartões de crédito, o que reduz a probabilidade de uso indevido por crianças e adolescentes. Contudo, essa abordagem apresenta limitações, especialmente devido à penetração desigual do uso de cartões de crédito no Brasil, o que poderia restringir o acesso a plataformas para populações sem acesso a esse meio de pagamento.

Independentemente da técnica utilizada, é importante destacar que nenhum mecanismo de verificação de idade é infalível, especialmente considerando a capacidade de menores de idade de contornar essas barreiras, muitas vezes com a ajuda, consciente ou não, de pais e tutores. Portanto, ao invés de estabelecer regras rígidas, é crucial promover boas práticas que considerem as vantagens e limitações de cada sistema. Por fim, é fundamental que uma política prioritária seja a educação de pais e responsáveis sobre os riscos de segurança e privacidade enfrentados por crianças e adolescentes no uso de plataformas digitais.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos,

a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais? [4200 caracteres]

Ao tratar os dados de crianças e adolescentes, é fundamental que as informações sobre o tratamento sejam comunicadas de maneira clara e adaptada ao público-alvo, utilizando uma apresentação, design e linguagem que facilitem a compreensão do uso dos dados, especialmente na criação de perfis comportamentais. Vale destacar que essa prática pode atender ao melhor interesse dos menores ao direcionar conteúdos apropriados para sua idade. Por exemplo, no setor financeiro, a personalização de perfis pode ser utilizada para adaptar programas educativos ao nível de entendimento e interesse dos jovens, tornando o aprendizado mais eficaz. Além disso, perfis comportamentais podem identificar padrões incomuns ou riscos de fraude, protegendo os menores contra atividades financeiras prejudiciais.

É importante lembrar que a LGPD não impõe restrições automáticas ao tratamento de dados de menores, desde que as bases legais sejam respeitadas e medidas de segurança adequadas sejam implementadas. Nesse contexto, a coleta de dados de crianças e adolescentes não deve ser limitada por padrão, exceto quando necessário para proteger seus melhores interesses. Em setores como o financeiro, a coleta de dados, incluindo a formação de perfis comportamentais, pode trazer benefícios significativos ao proporcionar segurança e ajudar os menores a desenvolver habilidades financeiras de forma segura e informada.

O IBRAC destaca que o tratamento de dados deve ser analisado caso a caso, levando em consideração os riscos específicos associados à natureza dos dados e ao modelo de negócio envolvido.

Por fim, é essencial que essas práticas sejam implementadas de maneira responsável e transparente, equilibrando a proteção dos dados pessoais com a promoção da autonomia e do desenvolvimento dos menores. O objetivo é garantir que o tratamento de dados, longe de ser prejudicial, possa contribuir positivamente para o bem-estar e a segurança de crianças e adolescentes, sempre respeitando os princípios da LGPD e o melhor interesse desses titulares.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital? [4200 caracteres]

A autonomia progressiva, conforme prevista no Estatuto da Criança e do Adolescente (ECA), exige que a capacidade de decisão das crianças e adolescentes seja respeitada e ampliada conforme seu crescimento e amadurecimento. Nesse contexto, é fundamental que a ANPD reconheça as especificidades desse setor e promova soluções que permitam a participação gradual e supervisionada dos jovens, transformando o controle parental em uma supervisão responsável, até que esses jovens alcancem a maioridade com uma autonomia financeira consolidada.

As medidas de proteção à privacidade para menores devem ser adaptáveis aos diferentes níveis de maturidade e autonomia de cada usuário, respeitando o princípio da autonomia progressiva. Em vez de configurações de privacidade excessivamente rígidas, é crucial que essas medidas sejam flexíveis, permitindo ajustes que considerem o conteúdo apropriado para a idade, o estágio de desenvolvimento do usuário e o modelo de negócio em questão. Essa abordagem reconhece que diferentes idades e níveis de compreensão demandam graus variados de proteção e interação, sempre em conformidade com o melhor interesse da criança e do adolescente, conforme a legislação brasileira.

A ampliação do controle por parte dos pais e responsáveis deve ser vista como uma assunção de maiores responsabilidades no uso de jogos e aplicativos de internet, considerando aspectos psicológicos e sociológicos. O controle parental deve ser entendido como uma medida voltada à segurança, e não como um estado constante de vigilância.

O controle parental deve ser transparente. Recomenda-se que as crianças e adolescentes sejam informados de maneira clara sobre a existência e os limites desse controle, como, por exemplo, esclarecendo que os pais ou responsáveis não teriam acesso a mensagens privadas trocadas com terceiros. O respeito à privacidade dos menores é essencial para garantir seu livre desenvolvimento, especialmente no caso de membros da comunidade LGBTQIAP+, conforme mencionado por alguns adolescentes no podcast Hard Fork, discutindo o livro de Jonathan Haidt.

Por fim, é altamente recomendável disponibilizar controles parentais de fácil compreensão e utilização, que permitam aos pais monitorar o uso de aplicativos e jogos, independentemente da marca ou do sistema operacional dos dispositivos usados por seus filhos.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes? [4200 caracteres]

A transparência no tratamento de dados pessoais de crianças e adolescentes é essencial para garantir que pais, responsáveis e os próprios titulares compreendam como seus dados são coletados, utilizados e protegidos. O Artigo 12 do General Data Protection Regulation (GDPR) da União Europeia exemplifica essa necessidade, exigindo que as informações fornecidas às crianças sejam acessíveis e compreensíveis. Esse artigo especifica que o controlador deve usar uma linguagem clara e simples, apresentando as informações de maneira concisa, transparente e de fácil acesso, seja por escrito, por meios eletrônicos ou, se solicitado, oralmente, desde que a identidade do solicitante seja confirmada.

Essas informações devem estar presentes na Política de Privacidade dos agentes de tratamento e devem ser disponibilizadas em locais de fácil acesso. Para

promover uma transparência adequada, é recomendável que os agentes de tratamento ofereçam portais e outros meios específicos que facilitem a compreensão das informações por crianças e adolescentes. Por exemplo, o Age Appropriate Design Code sugere o uso de explicações em pequenos pedaços, ou "bite-size", para ajudar os menores a entenderem como seus dados pessoais são utilizados.

Além disso, para garantir o melhor interesse das crianças e adolescentes, é igualmente importante fornecer suporte e transparência apropriada aos pais e responsáveis legais. Eles devem ter acesso a informações claras sobre as práticas de tratamento de dados pessoais e os recursos de supervisão parental disponíveis. As plataformas devem manter pais e filhos informados sobre quaisquer mudanças nas práticas de tratamento de dados, comunicando claramente atualizações nas políticas de privacidade e termos de serviço. Oferecer canais de suporte e feedback para que os usuários possam esclarecer dúvidas ou expressar preocupações sobre privacidade e tratamento de dados é uma prática recomendada.

Entretanto, é crucial que a ANPD considere os limites técnicos e a necessidade de proteger segredos comerciais e industriais dos agentes de tratamento ao exigir transparência. A divulgação excessiva de informações sobre as ferramentas de tratamento de dados de menores pode comprometer a segurança, facilitando a ação de agentes mal-intencionados. Assim, a transparência deve ser equilibrada, garantindo que as medidas de proteção dos dados das crianças e adolescentes permaneçam eficazes e seguras.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional? [4200 caracteres]

É crucial que a autoridade reguladora forneça orientações mais claras sobre as medidas de "privacy by default" que devem ser adotadas pelos agentes de tratamento ao processarem dados de crianças e adolescentes. Embora a legislação atual não imponha restrições específicas sobre o tratamento de certos tipos de dados pessoais, como geolocalização, perfilamento e publicidade direcionada, é importante que os controladores recebam diretrizes sobre quando esses tratamentos devem estar sujeitos a configurações de privacidade padrão.

Além disso, é necessário integrar melhor esse tema com os requisitos para a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e a identificação de tratamentos de dados pessoais de alto risco. A presença de dados de crianças e adolescentes deve ser um critério relevante para determinar a necessidade de um RIPD, juntamente com outros fatores, como o uso de tecnologias inovadoras, perfilamento em larga escala, dados biométricos e rastreamento online.

A regulamentação do tratamento de dados para fins de publicidade direcionada a crianças e adolescentes também é um aspecto fundamental. É essencial que esse tratamento seja disciplinado por critérios claros, garantindo que a

publicidade seja apropriada para o público-alvo, além de assegurar transparência e o consentimento informado dos pais ou responsáveis.

Por fim, é importante considerar o impacto das tecnologias emergentes, como a inteligência artificial, no tratamento de dados de crianças e adolescentes. Pode ser necessário estabelecer regulamentações adicionais para enfrentar os desafios específicos que essas tecnologias apresentam, garantindo que seu uso seja adequado e que os direitos das crianças e adolescentes sejam protegidos de maneira eficaz.

ITI Promoting Innovation Worldwide

Comentários do ITI à Tomada de Subsídios da ANPD sobre Tratamento de Dados Pessoais de Crianças e Adolescentes

Agosto 2024

O *Information Technology Industry Council* (ITI) é a principal voz, defensor e líder de pensamento da indústria global de tecnologia de informação e comunicação. Nossos membros incluem as principais empresas de inovação do mundo, com sedes e cadeias de valor distribuídas ao redor do globo. A privacidade e a confiança são fundamentais para os negócios e operações globais dos nossos membros. Juntamente com os nossos membros, o ITI trabalha com governos, reguladores e partes interessadas em todo o mundo para fortalecer e alinhar abordagens em matéria de proteção de dados e privacidade que salvaguardem os direitos individuais e promovam a inovação.

O ITI agradece a oportunidade de comentar a Tomada de Subsídios da Autoridade Nacional de Proteção de Dados (ANPD) sobre Tratamento de Dados Pessoais de Crianças e Adolescentes. Promover um ambiente online seguro para crianças e adolescentes é uma das prioridades dos nossos associados e apoiamos o objetivo da ANPD de desenvolver uma abordagem clara e interoperável que esteja alinhada com os padrões globais de proteção de dados e possibilite a inovação.

À medida que mais países introduzem leis de proteção de dados, são necessárias regras flexíveis e interoperáveis para garantir que as empresas tenham acesso a diferentes mecanismos para tratar dados pessoais de forma segura, proporcionando valor para os titulares dos dados e segurança para os negócios. O ITI apoia fortemente propostas que acompanhem os desenvolvimentos tecnológicos, mantendo ao mesmo tempo uma abordagem clara e previsível que seja consistente com as melhores práticas da indústria para a proteção dos dados das crianças.

O ITI submete os seguintes comentários às perguntas com considerações adicionais e permanece disponível para discutir cada um dos nossos comentários com mais detalhes.

I - Princípio do melhor interesse

1. **Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais**

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Seria fundamental que a ANPD destacasse que o melhor interesse das crianças e dos adolescentes não podem ser concebidos de forma abstrata e a priori, sendo necessária uma análise concreta para definir quais seriam os melhores interesses das crianças e dos adolescentes em uma determinada circunstância.

Como se sabe, o melhor interesse exige necessariamente um olhar dinâmico, voltado para o caso concreto e para as características do indivíduo ou do grupo de indivíduos afetados. Nesse sentido, cabe referenciar o Comentário Geral nº 14 do Comitê dos Direitos da Criança da Organização das Nações Unidas (ONU) [1]: "[...] o conceito de melhor interesse da criança é flexível e adaptável. Deve ser ajustado e definido de forma individual, com base na situação concreta da criança ou crianças afetadas, tendo em vista o contexto e as necessidades pessoais. No que diz respeito às decisões particulares, deve ser analisado e determinado o interesse superior da criança em função das circunstâncias específicas de cada criança em concreto".

Nesse sentido, o Comentário Geral nº 14 não prescreve quais seriam os melhores interesses da criança, preferindo fornecer uma estrutura para que os agentes públicos e privados possam avaliar e determinar os melhores interesses de forma concreta. Esta escolha baseia-se precisamente na natureza dinâmica do conceito de melhor interesse, que engloba diversas questões em constante evolução e que podem afetar um menor e/ou um grupo de menores com características e realidades diferentes. Neste sentido, a Convenção das Nações Unidas sobre os Direitos da Criança destaca a complexidade e a mutabilidade do conceito de melhor interesse, salientando que deve haver a devida consideração ao contexto pessoal, bem como à situação e às necessidades específicas do menor ou grupo de menores envolvidos. Ainda no Comentário Geral nº 14, destaca-se que a flexibilidade do conceito de melhor interesse permite que este seja responsivo à situação de cada menor e que haja progresso no conhecimento sobre o desenvolvimento dos menores. Por outro lado, a flexibilidade, o dinamismo e o foco no caso específico permitem-nos abordar a interação do melhor interesse com os diversos direitos que podem estar envolvidos em situações concretas que envolvem um menor e/ou um grupo de menores. Neste sentido, a Convenção das Nações Unidas sobre os Direitos da Criança destaca a interação do conceito com vários direitos, incluindo: o direito à não discriminação; direito à vida, sobrevivência e desenvolvimento; e direito de ser ouvido.

[1] United Nations. General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1) https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf

Da mesma forma, o Comentário Geral n.º 25[2] da Convenção das Nações Unidas sobre os Direitos da Criança, que visa abordar a aplicação dos direitos dos menores no ambiente digital, prevê que: "O melhor interesse da criança é um conceito dinâmico que exige uma avaliação apropriada ao contexto específico". Da mesma forma, a legislação nacional entende que o melhor interesse deve ser determinado de forma concreta, destacando o risco de o legislador definir o melhor interesse de forma genérica e, no caso específico, demonstrar que o melhor caminho seria diferente daquele geralmente previsto. Diante disso, o ITI gostaria de esclarecer que entende que, para definir o melhor interesse de uma determinada criança ou adolescente ou de um determinado grupo de crianças e adolescentes, é necessário olhar para o caso específico, que considera as circunstâncias específicas desse contexto, bem como as características e a situação em que se encontra essa criança ou adolescente ou esse grupo de crianças e adolescentes.

Diante disso, o ITI ressalta que a ANPD deve evitar perspectivas a priori e genéricas sobre o melhor interesse de crianças e adolescentes no que diz respeito ao tratamento de seus dados pessoais. Entendemos que, para avaliar o melhor interesse das crianças e adolescentes, é necessário olhar para o caso específico, que considera as circunstâncias específicas do tratamento dos dados pessoais em questão, tais como: (a) características gerais dos titulares dos dados; (b) quais dados são tratados; (c) qual é a finalidade do tratamento; e (d) possíveis benefícios e malefícios decorrentes do tratamento de dados. Da mesma forma, é necessário dar ao controlador a oportunidade de fazer ajustes (por exemplo, adotar certas salvaguardas, promover maior transparência, etc.) para que o tratamento não afete o melhor interesse das crianças e adolescentes.

2. **Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.**

O ITI entende que seria relevante que a ANPD esclarecesse que a utilização da base legal do interesse legítimo para o tratamento de dados pessoais de crianças e adolescentes não é, a princípio, contrária ao seu melhor interesse.

Nesse sentido, é importante destacar que, apesar do entendimento estabelecido no Enunciado nº 1/2022, onde a ANPD reconhece que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas bases legais

[2] United Nations. General comment No. 25 (2021) on children's rights in relation to the digital environment https://www.unicef.org/bulgaria/en/media/10596/file

previstas tanto no artigo 7º e art. 11 da LGPD, o Guia sobre o Legítimo Interesse trouxe uma perspectiva preocupante sobre o tratamento de dados pessoais de crianças e adolescentes. Gostaríamos de citar algumas afirmações do Guia que geraram preocupação, tais como: (i) "o tratamento de dados pessoais de crianças e adolescentes com base na hipótese do legítimo interesse tende a ser mais apropriado em situações nas quais há uma relação prévia e direta do controlador com os titulares e quando o tratamento visa a assegurar a proteção de seus direitos e interesses ou viabilizar a prestação de serviços que os beneficiem"[3]; e (ii) "o tratamento de dados pessoais de crianças e adolescentes com base na hipótese legal do legítimo interesse pressupõe que o controlador leve em consideração, de forma prioritária, o melhor interesse da criança ou do adolescente. Além disso, deve prevalecer a interpretação que atenda ao melhor interesse da criança e do adolescente de forma mais eficaz, inclusive, se for o caso, com a não realização do tratamento com base no legítimo interesse, em particular se o teste de balanceamento não for conclusivo ou se não forem identificadas medidas de segurança e de mitigação de risco adequadas à hipótese. Assim, se o resultado do teste de balanceamento for inconclusivo, ou se não forem identificadas medidas de segurança e de mitigação de risco adequadas à hipótese, deverá ser adotada outra base legal"[4].

Apesar dessa afirmativa, o Estudo Preliminar que embasou o Enunciado nº 1/2022 da ANPD concluiu que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base em todas as bases legais previstas na LGPD, desde que observado e prevalente o seu melhor interesse, a ser avaliado no caso concreto. Para chegar a esta conclusão, diversos argumentos foram considerados:

a) a flexibilidade propiciada pela possibilidade do uso de bases legais distintas, desde que o tratamento respeite o melhor interesse da criança e do adolescente;
b) a possibilidade de estender a aplicação do melhor interesse da criança e do adolescente para todas as bases legais;
c) a ausência de proibições jurídicas abstratas em relação a certas hipóteses legais e a necessidade de analisar as situações de forma concreta; e
d) o tratamento não diferenciado entre as hipóteses legais, mantendo-se a ausência de hierarquia entre elas, como previsto pela LGPD.

[3] ANPD. Hipóteses legais de tratamento de dados pessoais legítimo interesse. Página 11: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

[4] ANPD. Hipóteses legais de tratamento de dados pessoais legítimo interesse.Página 10-11: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

Dito isso, o ITI solicita respeitosamente à ANPD que não descarte, a priori, a utilização de qualquer base legal, inclusive legítimo interesse, para o tratamento de dados pessoais de crianças e adolescentes.

II – Consentimento

1. **Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?**

2. **Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?**

Em primeiro lugar, é necessário esclarecer que o § 5º do artigo 14, que estabelece que o controlador deve envidar todos os esforços razoáveis para verificar se o consentimento foi dado pelo responsável pela criança, diz respeito ao § 1º do mesmo artigo. Ou seja, trata-se do consentimento prestado por pelo menos um dos pais ou responsável legal para o tratamento de dados pessoais de crianças. Nesse sentido, esta resposta visa discutir a verificação do consentimento e não a verificação da idade, tema que será devidamente abordado na questão 2 do item III.

Sobre os mecanismos de verificação de consentimento parental em si, é importante salientar que o European Data Protection Board ("EDPB") [5] advoga pela proporcionalidade e destaca que o que é considerado razoável para verificar se o consentimento foi de fato fornecido pelos pais ou responsáveis legais dependerá dos riscos ligados ao tratamento, bem como das tecnologias disponíveis. O EDPB pontua que, em casos de baixo risco, a verificação via e-mail seria suficiente, enquanto em casos de alto risco, poderia ser apropriado solicitar mais provas. No mesmo sentido, o Information Commissioner's Office[6] entende que a análise da adequabilidade dos esforços razoáveis dependerá dos riscos ensejados pelo tratamento e da tecnologia

[5] EDPB. Guidelines 05/2020 on consent under Regulation 2016/679 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[6] ICO. What are the rules about an ISS and consent?. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/

disponível. A Data Protection Commission[7] também endossa a posição do EDPB e realiza apontamentos relevantes: (i) em vista do princípio da minimização, é preciso cautela para não realizar uma coleta excessiva de dados ao realizar o procedimento de verificação do consentimento; (ii) em última análise, cabe às organizações (como controladoras) decidir quais métodos de verificação são mais apropriados e proporcionais; e (iii) não há um padrão de referência quanto ao que constitui "esforços razoáveis", o que pode ser considerado um esforço razoável para uma organização pode não ser razoável para outra.

Ao dispor sobre a Children's Online Privacy Protection Rule ("COPPA"), a Federal Trade Commission ("FTC") [8] também salienta que cabe à organização determinar qual mecanismo utilizará para obter o consentimento parental, listando uma série de mecanismos que considera aceitáveis. São eles: (i) assinar um formulário de consentimento e enviá-lo de volta; (ii) usar um cartão de crédito, cartão de débito ou outro sistema de pagamento online que forneça notificação de cada transação separada ao titular da conta; (iii) ligar para um número gratuito atendido por pessoal treinado; (iv) conectar-se a pessoal treinado por meio de videoconferência; (v) fornecer uma cópia de um documento de identidade; (vi) responder a uma série de perguntas de desafio baseadas em conhecimento que seriam difíceis de responder para alguém que não seja o pai ou responsável; e (vii) verificar uma foto de uma carteira de motorista ou outro documento de identidade com foto enviado pelo pai ou responsável e depois comparar essa foto com uma segunda foto enviada pelo pai ou responsável, usando tecnologia de reconhecimento facial.

Portanto, o ITI entende que caberá a cada organização determinar, de acordo com os riscos do tratamento e as tecnologias disponíveis, qual seria o mecanismo mais adequado para verificar o consentimento. Deve-se notar que não existe um padrão fixo para o que seriam esforços razoáveis e que isso irá variar de acordo com as organizações. Por fim, é importante ressaltar que não existe um método único ou solução definitiva para esta verificação; Existem múltiplos métodos, cada um com os seus prós e contras, que devem ser cuidadosamente avaliados por cada organização à luz dos riscos que o tratamento realizado representa.

Para definir parâmetros de adoção para permitir e verificar se o consentimento foi fornecido pelos pais/responsáveis, a ANPD deve levar em consideração esforços razoáveis com base na tecnologia disponível, recursos, nível de risco, natureza e finalidades dos serviços e produtos. A autoridade não deve estabelecer medidas rígidas, mas sim orientações flexíveis que sejam, em particular, adequadas à forma

[7] DPC. Children Front and Centre - FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

[8] FCC. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business

como o titular dos dados e o agente de tratamento interagem. Além disso, deve esclarecer parâmetros para que esse consentimento possa ser obtido de forma que respeite a privacidade, garantindo que os métodos sejam práticos e adequados.
De qualquer forma, vale ressaltar que garantir um ambiente online saudável e seguro para as crianças é do interesse das empresas, dos governos e da sociedade em geral. Sobre esta questão, vale destacar o papel fundamental desempenhado pela colaboração e presença dos pais ou responsáveis legais de forma responsável na vida das crianças e adolescentes, especialmente nas suas interações com o ecossistema digital.

Empresas de tecnologia e internet têm oferecido diversas soluções para permitir que os pais monitorem e aprovem as interações de crianças e adolescentes na Internet. Por exemplo, ao configurar inicialmente um dispositivo, os pais já podem indicar que o utilizador é menor de idade, e ativar o controle parental, associando os seus dados de contato, como número de telefone e email, como meio de notificação e meio de dar consentimento parental para baixar aplicativos ou fazer compras on-line.

Dessa forma, os pais poderão supervisionar e aprovar a atividade online de seus adolescentes de forma prática, segura e objetiva. Este modelo traz vários benefícios, pois evita que os pais tenham que passar por diferentes métodos para se inscrever, fornecer informações de identificação (de pais e filhos) a aplicações com práticas inconsistentes de segurança e privacidade e repetir este processo várias vezes. Além disso, contribui para a privacidade e a minimização da coleta de dados pessoais ao nível de múltiplas aplicações: os fornecedores de aplicações só precisam da idade recolhida ao nível da loja de aplicações para garantir a verificação de idade e experiências adequadas à idade, oferecendo mecanismos de controle e supervisão ao nível da aplicação.

3. **No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?**

O ITI destaca a necessidade de uma separação clara e precisa das obrigações e direitos relativos às crianças daqueles relativos aos adolescentes e alerta para a necessidade de cautela no debate, relativamente ao consentimento, para não criar

confusão entre os institutos da capacidade civil e as disposições da Lei Geral de Proteção de Dados, que serão mais exploradas ao longo do texto.

O Estatuto da Criança e do Adolescente faz diferenciação clara, em seu artigo 2º, entre a criança (pessoa de até 12 anos incompletos) e o adolescente (pessoas entre 12 a 18 anos), e estabelece, em seu artigo 6º, o dever de interpretação de suas normas considerando a condição peculiar de desenvolvimento desses sujeitos. A abordagem diferenciada para crianças e adolescentes exige considerar os diferentes estágios de desenvolvimento e autonomia desses titulares, gerando a desnecessidade de representação ou assistência pelos pais ou responsáveis legais no caso dos adolescentes, em respeito ao princípio da condição peculiar de pessoa em desenvolvimento, em consonância com o princípio do melhor interesse da criança e do adolescente.

Neste contexto, a Lei Geral de Proteção de Dados Pessoais, em seu artigo 14, dispõe especificamente sobre o tratamento de dados pessoais de crianças e adolescentes, que deve ser feito visando o melhor interesse do menor e respeitando a legislação pertinente. Observa-se que, ao não mencionar a necessidade de consentimento por pelo menos um dos pais ou pelo responsável legal no §1º do artigo 14, a LGPD pretende reconhecer a validade do consentimento manifestado pelo próprio adolescente para tratamento de seus dados, atribuindo maior liberdade para o adolescente progressivamente exercer sua personalidade de forma autônoma, o que deve levar, naturalmente, a uma redução gradual da interferência parental, respeitando a crescente capacidade dos adolescentes de exercerem seus direitos de forma independente.

É preciso ter cautela e não confundir o instituto da capacidade civil com o disposto na LGPD, ou seja, não confundir consentimento parental com fiscalização parental. Embora a LGPD permita que os adolescentes consintam no tratamento de seus dados, ela não autoriza a formação de negócios jurídicos pelo adolescente, esta matéria é amplamente regulamentada pelo Código Civil. A LGPD visa dar maior liberdade ao adolescente para o exercício de sua personalidade, permitindo que seja válida a manifestação de sua vontade quanto ao tratamento de seus dados, de forma autônoma. Portanto, não há necessidade de falar em confusão ou sobreposição entre a LGPD, uma lei específica, e as disposições do direito civil relativas às capacidades civis.

III - Jogos e aplicações de internet

1. **Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar**

o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Em relação aos princípios, é importante considerar que o ordenamento jurídico já os estabelece. Nesse sentido, no artigo 6º, a Lei Geral de Proteção de Dados Pessoais lista uma série de princípios que devem ser considerados para salvaguardar o direito à proteção de dados. Complementarmente, o artigo 14 estabelece que o princípio do melhor interesse deve ser um balizador no tratamento de dados pessoais de crianças e adolescentes. De igual modo, o direito internacional, a Constituição Federal e o Estatuto da Criança e do Adolescente trazem uma série de princípios aplicáveis a crianças e adolescentes, incluindo o princípio da condição peculiar de pessoa em desenvolvimento.

Especificamente no que tange a este princípio, o ITI gostaria de destacar a importância de considerá-lo no tratamento de dados de crianças e adolescentes. Isso porque, é preciso que haja equilíbrio entre o desejo de proteger as crianças e os adolescentes no ambiente digital com a necessidade de respeitar o desenvolvimento de capacidades e o alcance paulatino de discernimento. Além disso, é preciso evitar perspectivas excessivas que podem afetar o gozo de diversos direitos, como: liberdade, dignidade como pessoa em processo de desenvolvimento, convivência comunitária, educação, cultura, lazer, etc. Nesse sentido, ao estabelecer orientação sobre como respeitar e proteger os direitos das crianças e dos adolescentes no ambiente digital, para além dos direitos à privacidade, proteção e segurança, o Conselho da Europa[9] destaca que outros direitos que merecem igualmente proteção, são eles: acesso ao ambiente digital, liberdade de expressão e informação, educação e participação.

No mesmo sentido, a Organização para a Cooperação e Desenvolvimento Econômico ("OCDE") [10] entende que atores desempenham um papel ativo na definição de políticas e práticas ou prestação de serviços para crianças e adolescentes no ambiente digital devem considerar suas diferentes necessidades em vista da idade e da maturidade. No mesmo documento, a OCDE destaca que as medidas adotadas por tais atores devem: (i) ser proporcionais aos riscos, baseadas em evidências, eficazes, equilibradas e formuladas com uma visão de maximizar as oportunidades e benefícios para as crianças e adolescentes no ambiente digital; e (ii) promover a liberdade de expressão das crianças e dos adolescentes e não prejudicar outros direitos humanos e liberdades fundamentais.

[9] COE. Building a Europe for and with children. https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[10] OECD. Recommendation of the Council on Children in the Digital Environment https://legalinstruments.oecd.org/public/doc/272/272.en.pdf

Assim, entende-se que a condição peculiar de pessoa em desenvolvimento deve ser considerada não só como um princípio, mas também como um parâmetro que a guie não só a atuação das organizações como também da própria ANPD. O Age Appropriate Design Code do ICO[11], por exemplo, trabalha com cinco estágios de desenvolvimento, são eles pré-alfabetizados e alfabetizados (de zero a cinco anos de idade); anos básicos do ensino fundamental (de seis a nove anos de idade); anos de transição (de dez a doze anos de idade); início da adolescência (de treze a quinze anos de idade); e aproximando-se da idade adulta (de doze a dezessete anos). Além disso, o escritório do Reino Unido fornece um anexo[12] visando trazer clareza sobre os principais aspectos a serem considerados em cada fase.

Outros elemento que pode ser considerado como um parâmetro não só pelas organizações mas pela própria a ANPD é a proporcionalidade, a fim de equilibrar o desejo de proteger crianças e adolescentes online com a necessidade de salvaguardar seus diversos direitos e liberdades, dentre eles o acesso ao ambiente digital, a liberdade de expressão, o acesso à informação e à educação. Uma abordagem baseada em risco, adaptável a diferentes produtos e serviços, que pondere a disponibilidade tecnológica, natureza e propósito é mais um parâmetro que deve ser considerado e que pode ser um grande aliado em uma abordagem guiada pela proporcionalidade. Essa abordagem é um reflexo da própria LGPD, mas também pode ser encontrada em diversos documentos elaborados por autoridades internacionais sobre a temática da proteção de crianças e adolescentes online, dentre elas: ICO[13], Ministério do Interior e das Relações do Reino da Holanda[14], Commission Nationale Informatique & Libertés ("CNIL") [15] e DPC[16].

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as

[11] ICO. Age appropriate application. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/

[12] ICO. Age appropriate design: a code of practice for online services https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[13] ICO. Age appropriate design: a code of practice for online services https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[14] Code Voor Kinderrechten. Code for Children's Rights. https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf

[15] CNIL. Digital rights of children. https://www.cnil.fr/en/digital-rights-children

[16] DPC. Children Front and Centre. Fundamentals for a Child-Oriented Approach to Data Processing https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

Como aspecto preliminar, o ITI gostaria de destacar que o termo "verificação de idade" abrange uma gama restrita de mecanismos que visam certificar a idade de um indivíduo. Nesse sentido, conforme documento elaborado pelo Future of Privacy Forum[17], a expressão "age assurance" é utilizada para englobar uma variedade mais ampla de mecanismos de certificação de idade: declaração, estimativa e verificação. A declaração incluiria mecanismos nos quais o usuário indica sua data de nascimento, ou nos quais o responsável declara a idade da criança ou adolescente. Já a estimativa abrangeria métodos que vão desde a estimativa da idade com base em imagens faciais até métodos que utilizam outros meios (voz, histórico de navegação, etc.). Por fim, a verificação englobaria mecanismos como aqueles que avaliam um escaneamento de documento em relação a uma foto ou vídeo, utilizando reconhecimento facial e aqueles que se utilizam de identidades digitais.

Em relação à temática de certificação de idade, é preciso que essa Autoridade considere que não há uma solução única e/ou perfeita. Nesse sentido, a DPC destaca que: (i) a área tecnológica de mecanismos e ferramentas de certificação de idade ainda está em desenvolvimento; e (ii) não existe uma solução única para a questão da certificação de idade, mecanismos apropriados provavelmente variarão, dependendo, por exemplo, de fatores como o serviço sendo oferecido e a sensibilidade dos dados pessoais sendo tratados. A CNIL salienta que todas as soluções atualmente propostas podem ser, em alguma medida, burladas. Além disso, ao analisar várias soluções existentes para certificação de idade, a autoridade francesa pontuou que nenhuma delas atenderia satisfatoriamente os seguintes requisitos: verificação suficientemente confiável, cobertura completa da população e respeito à proteção dos dados e privacidade dos indivíduos, bem como sua segurança.

3. **Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?**

Inicialmente, é preciso esclarecer o recorte do artigo 14, §4º da LGPD, que dispõe que os controladores não deverão condicionar a participação de crianças em jogos,

[17] FPF. Unpacking Age Assurance: Technologies and Tradeoffs. https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf

aplicações de internet e outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. O parágrafo faz remissão clara às disposições do parágrafo 1º, sobre tratamento de dados pessoais de crianças, e não de adolescentes, qualquer interpretação extensiva na tentativa de equiparar crianças e adolescentes poderia gerar violação ao princípio da condição peculiar de pessoa em desenvolvimento, presente nas mais diversas normas protetivas, como na Constituição Federal, no Estatuto da Criança e do Adolescente na Convenção sobre os Direitos da Criança, promulgada pelo Decreto nº 99.710/1990 e com a Doutrina.
Como destacado em outros momentos desta contribuição, é importante considerar o princípio do melhor interesse e a condição peculiar da pessoa em desenvolvimento no tratamento de dados de crianças e adolescentes. É preciso evitar perspectivas excessivas que podem afetar o gozo de diversos direitos, como: liberdade, dignidade como pessoa em processo de desenvolvimento, convivência comunitária, educação, cultura, lazer, et, para que haja equilíbrio entre o desejo de proteger as crianças e os adolescentes no ambiente digital com a necessidade de respeitar o desenvolvimento de capacidades e o alcance paulatino de discernimento. Qualquer restrição automáticas ou pré-definidas para a coleta de dados pessoais de crianças e adolescentes para além das já explícitas na legislação, pode resultar em maior insegurança para os menores e agentes de tratamento. Além disso, a LGPD não estabelece restrições específicas ao tratamento de dados de crianças e adolescentes, inclusive dados pessoais sensíveis, desde que o agente de tratamento justifique com base legal adequada, implementem medidas necessárias para cumprimento das obrigações estabelecidas pela LGPD e que este tratamento seja alinhado com o melhor interesse dos menores.

Em relação à formação de perfis comportamentais, embora exista uma tendência de enxergar a prática com preocupação, estes não devem ser associados automaticamente a práticas prejudiciais. O uso destas tecnologias representa diversos benefícios, principalmente quanto ao tratamento de dados de crianças e adolescentes. Por vezes, é necessário realizar o perfilamento para cumprimento de obrigações legais, regulatórias e até mesmo para indicar conteúdos adequados à idade do usuário e restringir o conteúdo inadequado. A formação de perfis comportamentais também pode ser usada no combate de ilícitos, para melhorar a precisão da estimativa de idade, além de permitir personalização de serviços para oferecer experiências relevantes e seguras para crianças e adolescentes, dentre outras várias situações nas quais as técnicas de perfilamento são utilizadas, justamente, no melhor interesse da criança e do adolescente.

4. **Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?**

Como afirmamos acima, garantir um ambiente online saudável e seguro para as crianças é do interesse das empresas, dos governos e da sociedade em geral. Sobre esta questão, vale destacar o papel fundamental desempenhado pela colaboração e presença dos pais ou responsáveis legais de forma responsável na vida das crianças e adolescentes, especialmente nas suas interações com o ecossistema digital.

5. **Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?**

6. **Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?**

ITI Promoting Innovation Worldwide

ITI Comments to ANPD Open Call for Initial Input on Processing of Personal Data of Children and Adolescents

August 2024

The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader for the global information and communication technology industry. Our members include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. Privacy and trust are central to our members' businesses and global operations. Together with our members, ITI works with governments, regulators, and stakeholders around the world to strengthen and align approaches towards data protection and privacy that safeguard individual rights and promote innovation.

ITI welcomes the opportunity to comment on the National Data Protection Authority (ANPD) Open Call for Initial Input on Processing of Personal Data of Children and Adolescents. Promoting a safe online environment for children and adolescents is one of the priorities of our members and we support ANPD's aim of developing a clear and interoperable approach that is aligned with global data protection standards and enables innovation.

As more countries introduce national data protection frameworks, flexible and interoperable rules are required to ensure that companies have access to different mechanisms to process personal data securely, providing value for data subjects and certainty for business. ITI strongly supports proposals that will keep pace with technological developments while maintaining a clear and predictable approach that is consistent with industry best-practices for the protection of children's data.

ITI submits the following comments to questions with further considerations and remains available to discuss each of our comments in greater detail.

I - Principle of best interest

1. **In addition to the aspects addressed in CD/ANPD Statement no. 01/2022 and in the Guidance on the legal basis of legitimate interest, what issues related to the principle of best interest require specific guidance or regulation by the ANPD?**

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

It would be essential for the ANPD to highlight that the best interests of children and adolescents cannot be conceived in an abstract and a priori way, requiring a concrete analysis to define what would be the best interests of children and adolescents in a given circumstance.
As we know, the best interests of children and adolescents necessarily require a dynamic approach, focused on the specific case and the characteristics of the individual or group of individuals affected. In this sense, it is worth referring to UN General Comment No. 14[1]: "The concept of the child's best interests is complex and its content must be determined on a case-by-case basis. [...] The concept of the child's best interests is flexible and adaptable. It should be adjusted and defined on an individual basis, according to the specific situation of the child or children concerned, taking into consideration their personal context, situation and needs. For individual decisions, the child's best interests must be assessed and determined in light of the specific circumstances of the particular child".

In this sense, General Comment No. 14 does not prescribe what the best interests of the child would be, preferring to provide a structure so that public and private agents can evaluate and determine the best interests in a concrete way. This choice is based precisely on the dynamic nature of the concept of best interests, which encompasses several issues that are constantly evolving and that can affect a minor and/or a group of minors who have different characteristics and realities. In this sense, the UN Convention on the Rights of the Child highlights the complexity and mutability of the concept of best interests, pointing out that there must be due consideration to the personal context, as well as the situation and specific needs of the minor or group of minors involved.

Still in General Comment No. 14, it is highlighted that the flexibility of the concept of best interests allows it to be responsive to the situation of each minor and for there to be progress in knowledge about the development of minors. On another point, flexibility, dynamism and a focus on the specific case allow us to address the interaction of best interests with the various rights that may be involved in concrete situations involving a minor and/or a group of minors. In this sense, the UN Convention on the Rights of the Child highlights the interaction of the concept with various rights, including: the right to non-discrimination; right to life, survival and development; and right to be heard.

Likewise, General Comment No. 25[2] of the UN Convention on the Rights of the Child, which aims to address the application of the rights of minors in the digital environment, provides that: "The best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context". Likewise, national legislation understands that the best interest must be determined in a concrete way,

[1] United Nations. General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1) https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf

[2] United Nations. General comment No. 25 (2021) on children's rights in relation to the digital environment https://www.unicef.org/bulgaria/en/media/10596/file

highlighting the risk of the legislator defining the best interest in a generic way and, in the specific case, demonstrating that the best path would be different from that generally foreseen. In view of this, ITI would like to clarify that it understands that, in order to define the best interests of a given child or adolescent or a certain group of children and adolescents, it is necessary to look at the specific case, which considers the specific circumstances of that context, as well as such as the characteristics and situation in which that child or adolescent or that group of children and adolescents finds themselves.

In view of this, ITI would like to point out that the ANPD must avoid a priori and generic perspectives on the best interests of children and adolescents with regard to the processing of their personal data. We understand that, to assess the best interests of children and adolescents, it is necessary to look at the specific case, which considers the specific circumstances of the processing of personal data in question, such as: (a) general characteristics of data subjects; (b) what data is processed; (c) what is the purpose of the processing; and (d) possible benefits and harms arising from data processing. Likewise, it is necessary to give the controller the opportunity to make adjustments (e.g., adopting certain safeguards, promoting greater transparency, etc.) so that the processing does not affect the best interests of children and adolescents.

2. **Are there specific situations or contexts in the processing of children and adolescents personal data that require greater attention and detail regarding the best interests principle? If so, indicate the situations or contexts identified and the main issues to be addressed.**

ITI understands that it would be relevant for ANPD to clarify that the use of the legal basis of legitimate interest for the processing of personal data of children and adolescents is not, at first, contrary to their best interests.

In this sense, it is important to highlight that, despite the understanding established in Statement No. 1/2022, where ANPD recognizes that the processing of personal data of children and adolescents may be carried out based on the legal bases provided for in both article 7 and art. 11 of the LGPD, the Guidance on the Legitimate Interest brought a worrying perspective on the processing of personal data of children and adolescents. We would like to cite some statements in the Guidance that generated concern, such as: (i) “the use of legitimate interest tends to be more appropriate in situations in which there is a prior and direct relationship between the controller and the data subjects and when the processing aims to ensure the protection of their rights and interests or enable the provision of services that benefit them”[3]; and (ii) “the processing of personal data of children and adolescents based on legitimate interest presupposes that the controller takes into account, as a priority,

[3] ANPD. Hipóteses legais de tratamento de dados pessoais legítimo interesse. Página 11: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

the best interests of the child or adolescent. Furthermore, the interpretation that meets the best interests of the child and adolescent in the most effective way must prevail, including, if applicable, not carrying out processing based on legitimate interests, in particular if the balancing test is not conclusive or if security and risk mitigation measures appropriate to the hypothesis are not identified. Therefore, if the result of the balancing test is inconclusive, or if security and risk mitigation measures appropriate to the hypothesis are not identified, another legal basis must be adopted"[4].

Despite these statements of the Guidance on the Legitimate Interest, the Preliminary Study that supported ANPD Statement No. 1/2022 concluded that the processing of personal data of children and adolescents may be carried out based on the legal bases provided for in the LGPD, as long as their best interests are observed and prevailed, to be assessed in the specific case. Several arguments were considered to reach this conclusion:

a) The flexibility provided by the possibility of using different legal bases, as long as the processing respects the best interests of the child and adolescent;
b) The possibility of extending the application of the best interests of children and adolescents to all legal bases;
c) The absence of abstract legal prohibitions in relation to certain legal hypotheses and the need to analyze situations in a concrete way; and
d) Non-differentiated treatment between legal hypotheses, maintaining the absence of hierarchy between them, as provided for by the LGPD.

That being said, ITI respectfully urges the ANPD to not rule out, a priori, the use of any legal basis, including legitimate interest, for the processing of personal data of children and adolescents.

II – Consent

1. **What criteria or parameters must be observed in order to obtain "specific and prominent" consent from parents or legal guardians?**

2. **Considering good practices, available technologies and the principles of the LGPD, especially the principles of purpose, necessity and adequacy, as well as the legal requirement to adopt "all reasonable efforts", what measures and mechanisms should controllers adopt, especially in the digital environment, to enable and verify that consent has been provided by the child's parents or legal guardians?**

[4] ANPD. Hipóteses legais de tratamento de dados pessoais legítimo interesse.Página 10-11: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf

Firstly, it is necessary to clarify that Paragraph 5 of article 14, which establishes that the controller must make all reasonable efforts to verify that consent was given by the person responsible for the child, concerns Paragraph 1 of the same article. That is, it deals with the consent provided by at least one parent or legal guardian for the processing of children's personal data. In this sense, this response aims to discuss the verification of consent and not the verification of age, a topic that will be duly addressed in question 2 of item III.

Regarding the topic, it is important to highlight that the European Data Protection Board ("EDPB")[5] advocates proportionality and highlights that what is considered reasonable to verify whether consent was in fact provided by parents or legal guardians will depend on the risks linked to the processing, as well as available technologies. The EDPB points out that, in low-risk cases, verification via email would be sufficient, while in high-risk cases, it could be appropriate to request further evidence. In the same sense, the UK Information Commissioner's Office (ICO)[6] understands that the analysis of the adequacy of reasonable efforts will depend on the risks posed by the processing and the available technology. The Data Protection Commission[7] also endorses the EDPB's position and makes relevant notes: (i) in view of the principle of minimization, care must be taken not to collect excessive data when carrying out the consent verification procedure; (ii) ultimately it is up to organizations (as controllers) to decide which verification methods are most appropriate and proportionate; and (iii) there is no standard of reference as to what constitutes "reasonable efforts", what may be considered a reasonable effort for one organization may not be reasonable for another.

When providing for the Children's Online Privacy Protection Rule ("COPPA"), the US Federal Trade Commission ("FTC")[8] also emphasizes that it is up to the organization to determine which mechanism it will use to obtain parental consent, listing a series of mechanisms that it considers acceptable. They are: (i) sign a consent form and send it back; (ii) use a credit card, debit card or other online payment system that provides notification of each separate transaction to the account holder; (iii) call a toll-free number staffed by trained personnel; (iv) connect with trained personnel via video conferencing; (v) provide a copy of an identity document; (vi) answer a series of knowledge-based challenge questions that would be difficult for someone other than

[5] EDPB. Guidelines 05/2020 on consent under Regulation 2016/679 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[6] ICO. What are the rules about an ISS and consent?. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/

[7] DPC. Children Front and Centre - FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

[8] FCC. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business

the parent or guardian to answer; and (vii) verify a photo of a driver's license or other photo ID submitted by the parent or guardian and then compare that photo to a second photo submitted by the parent or guardian using facial recognition technology. Therefore, ITI understands that it will be up to each organization to determine, according to the risks of the processing and the available technologies, which would be the most appropriate mechanism to verify consent. It should be noted that there is no fixed standard for what would be reasonable efforts and that this will vary according to organizations. Finally, it is important to point out that there is no single method or definitive solution for this verification; There are multiple methods, each with its pros and cons, which must be carefully evaluated by each organization in light of the risks posed by the processing carried out.

To define adoption parameters to enable and verify that consent was provided by parents/guardians, the ANPD must take into account reasonable efforts based on available technology, resources, level of risk, nature and purposes of services and products. The authority should not establish rigid measures, but flexible guidelines that are, in particular, appropriate to the way in which the data subject and the processing agent interact. Furthermore, it must clarify parameters so that this consent can be obtained in a way that respects privacy, ensuring that the methods are practical and appropriate.

In any case, it is worth mentioning that ensuring a healthy and safe online environment for children is in the interests of companies, governments and society in general. On this issue, it is worth highlighting the fundamental role played by the collaboration and presence of parents or legal guardians in a responsible manner in the lives of children and adolescents, especially in their interactions with the digital ecosystem.

Technology and internet companies have offered several solutions to enable parents to monitor and approve interactions of children and adolescents on the Internet. For example, when initially configuring a device, the parent can already indicate that the user is a minor, and activate parental control, associating their contact details, such as phone number and email, as means of notification and means to give parental consent to download applications or make online purchases.

This way, parents can supervise and approve their adolescents' online activity in a practical, safe and objective way. This model brings several benefits, as it prevents parents from having to go through different methods to sign up, provide identifying information (of parents and children) to applications with inconsistent security and privacy practices, and repeat this process several times. Furthermore, it contributes to privacy and the minimization of personal data collection at the multiple app level: App providers only need age captured at the app store level to ensure age assurance and age-appropriate experiences by offering control and oversight mechanisms at the app level.

3. **In the case of adolescents, should obtaining consent, especially in the digital environment, comply with the provisions of civil law regarding legal capacity, following the general rule of representation and assistance from parents or guardians? Or is it possible to consider, in line with the of best interest principle, the progressive autonomy of these data subjects to, in certain contexts and situations, provide consent to the processing of their personal data without the need for representation or assistance from parents and legal guardians?**

ITI highlights the need for a clear and precise separation of obligations and rights related to children from those relating to adolescents and warns about the need for caution in the debate, regarding consent, so as not to create confusion between the institutes of civilian capacity and the provisions of the Law General Data Protection, which will be further explored throughout the text.

The Child and Adolescent Statute clearly differentiates, in its article 2, the child (person up to 12 years old) and the adolescent (people between 12 and 18 years old), establishing, in its article 6, the duty of interpretation standards considering the peculiar development conditions of these subjects. The differentiated approach for children and adolescents allows considering the different stages of development, respecting the principle of the peculiar condition of a developing person, in line with the principle of the best interests of the child and adolescent.

In this context, the General Data Protection Law, in its article 14, specifically provides for the processing of personal data of children and adolescents, which must be done with the best interests of the minor and the relevant legislation in mind. It is observed that, by not mentioning the need for specific consent for the adolescent in Paragraph 1 of article 14, the LGPD intends to recognize the validity of the consent expressed by the adolescent themselves for the processing of their data, giving greater freedom to the adolescent to exercise their personality autonomously.

It is necessary to be careful and not confuse the institute of civil capacity with the provisions of the LGPD, that is, not to confuse parental consent with parental monitoring. Although the LGPD allows adolescents to consent to the processing of their data, it does not authorize the formation of legal transactions by the adolescent, this matter is largely regulated by the Civil Code. The LGPD aims to give adolescents greater freedom to exercise their personality, allowing the expression of their will regarding the processing of their data, autonomously, to be valid. Therefore, there is no need to talk about confusion or overlap between the LGPD, a specific law, and the provisions of civil law regarding civil capacities.

III - Games and Internet applications

1. **What principles, parameters and safeguards, including design measures, should be observed in the processing of personal data of children and adolescents by digital platforms, in order to ensure respect for their best interests, promote and ensure high levels of privacy and protection of personal data and mitigate the risks arising from the use of these platforms?**

Regarding principles, it is important to consider that the legal system already establishes them. In this sense, in its article 6, the LGPD lists a series of principles that must be considered in order to safeguard the right to data protection. In addition, article 14 establishes that the principle of best interests must be a guide in the processing of personal data of children and adolescents. In the same sense, international law, the Federal Constitution and the Child and Adolescent Statute ("ECA") bring a series of principles that must be considered in relation to children and adolescents, among them the peculiar condition of a developing person.

Specifically regarding this principle, ITI would like to highlight the importance of considering it when processing data from children and adolescents. This is because there needs to be a balance between the desire to protect children and adolescents in the digital environment with the need to respect the development of capabilities and the gradual reach of discernment. Furthermore, it is necessary to avoid excessive perspectives that could affect the enjoyment of various rights, such as: freedom, dignity as a person in the process of development, community coexistence, education, culture, leisure, etc. In this sense, when establishing guidance on how to respect and protect the rights of children and adolescents in the digital environment, in addition to the rights to privacy, protection and security, the Council of Europe[9] highlights that other rights that equally deserve protection are: access to the digital environment, freedom of expression and information, education and participation.

In the same sense, the Organization for Economic Cooperation and Development ("OECD")[10] understands that actors playing an active role in defining policies and practices or providing services for children and adolescents in the digital environment must consider their different needs in view of their age and maturity. In the same document, the OECD highlights that the measures adopted by such actors must: (i) be proportionate to the risks, based on evidence, effective, balanced and formulated with a vision of maximizing opportunities and benefits for children and adolescents in the digital environment ; and (ii) promote freedom of expression for children and adolescents and not harm other human rights and fundamental freedoms.

[9] COE. Building a Europe for and with children. https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[10] OECD. Recommendation of the Council on Children in the Digital Environment https://legalinstruments.oecd.org/public/doc/272/272.en.pdf

Thus, it is understood that the peculiar condition of a developing person must be considered not only as a principle, but also as a parameter that guides not only the actions of organizations but also of the ANPD itself. The ICO's Age Appropriate Design Code[11], for example, works with five stages of development, they are pre-literate and literate (from zero to five years of age); basic years of elementary school (from six to nine years of age); transition years (from ten to twelve years of age); early adolescence (thirteen to fifteen years of age); and approaching adulthood (ages ten to seventeen). In addition, the UK office provides an annex[12] to provide clarity on the main aspects to be considered at each stage.

Another element that can be considered as a parameter not only by organizations but by the ANPD itself is proportionality, in order to balance the desire to protect children and adolescents online with the need to safeguard their various rights and freedoms, including access to digital environment, freedom of expression, access to information and education. A risk-based approach is another parameter that must be considered and can be a great ally in an approach guided by proportionality. This approach is a reflection of the LGPD itself, but can also be found in several documents prepared by international authorities on the topic of protecting children and adolescents online, among them: ICO[13], Ministry of the Interior and Relations of the Kingdom of the Netherlands[14], Commission Nationale Informatique & Libertés ("CNIL")[15] and DPC[16].

2. **Considering that the processing of personal data must be limited to that which is strictly necessary for its intended purpose, what are the best practices and available techniques for verifying the age of users of digital platforms?**

[11]ICO. Age appropriate application. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/

[12]ICO. Age appropriate design: a code of practice for online services https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[13] ICO. Age appropriate design: a code of practice for online services https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[14] Code Voor Kinderrechten. Code for Children's Rights. https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf

[15] CNIL. Digital rights of children. https://www.cnil.fr/en/digital-rights-children

[16] DPC. Children Front and Centre. Fundamentals for a Child-Oriented Approach to Data Processing https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

As a preliminary aspect, ITI would like to highlight that the term "age verification" covers a restricted range of mechanisms that aim to certify an individual's age. In this sense, according to a document prepared by the Future of Privacy Forum[17], the expression "age assurance" is used to encompass a wider variety of age certification mechanisms: declaration, estimation and verification. The declaration would include mechanisms in which the user indicates their date of birth, or in which the guardian declares the age of the child or adolescent. Estimation would cover methods ranging from age estimation based on facial images to methods that use other means (voice, browsing history, etc.). Finally, verification would encompass mechanisms such as those that evaluate a document scan against a photo or video, using facial recognition and those that use digital identities.

Regarding the issue of age certification, ANPD should consider that there is no single and/or perfect solution. In this sense, the DPC highlights that: (i) the technological area of age certification mechanisms and tools is still under development; and (ii) there is no single solution to the issue of age certification, appropriate mechanisms are likely to vary depending, for example, on factors such as the service being offered and the sensitivity of the personal data being processed. The CNIL emphasizes that all currently proposed solutions can be, to some extent, circumvented. Furthermore, when analyzing several existing solutions for age certification, the French authority noted that none of them would satisfactorily meet the following requirements: sufficiently reliable verification, complete coverage of the population and respect for the protection of individuals' data and privacy, as well as their security.

3. **What specific limitations should be observed in the collection of personal data of children and adolescents by digital platforms, considering the provisions of article 14, § 4, of the LGPD and, among other aspects, the nature of the data collected and the purpose of the processing, such as the development of behavioral profiles?**

Initially, it is necessary to clarify the section of article 14, Paragraph 4 of the LGPD, which states that controllers should not condition the participation of children in games, internet applications and other activities on the provision of personal information beyond that strictly necessary for the activity. The paragraph makes a clear reference to the provisions of paragraph 1, on the processing of personal data of children, and not of adolescents, any extensive interpretation in an attempt to equate children and adolescents could generate a violation of the principle of the peculiar condition of a developing person, present in the most various protective norms, such as in the Federal Constitution, and in the Child and Adolescent Statute.

[17] FPF. Unpacking Age Assurance: Technologies and Tradeoffs. https://fpf.org/wp-content/uploads/2023/06/FPF_Age-Assurance_final_6.23.pdf

As highlighted by ITI elsewhere in this contribution, it is important to consider the principle of best interests and the peculiar condition of the developing person when processing data from children and adolescents. So that there is a balance between the desire to protect children and adolescents in the digital environment with the need to respect the development of capabilities and the gradual reach of discernment. It is necessary to avoid excessive perspectives that could affect the enjoyment of various rights, such as: freedom, dignity as a person in the process of development, community coexistence, education, culture, leisure, etc.

Although there is a tendency to view behavioral profiling with concern, these should not be automatically associated with harmful practices. Sometimes, it is necessary to carry out profiling to comply with legal and regulatory obligations and even to know whether it is in fact a child, teenager or even an adult. It is necessary to look at the benefits of using this technology, especially regarding the processing of data from children and adolescents, considering that they can be used to combat illicit activities, improve the accuracy of age estimation; allow personalization of services to offer relevant and safe experiences for children and adolescents, among other situations in which profiling techniques are used, precisely, in the best interests of the child and adolescent.

4. **What mechanisms and best practices can be adopted to increase parents' and guardians' control over the processing of children's and adolescents' personal data in the digital environment?**

As we stated above, ensuring a healthy and safe online environment for children is in the interests of companies, governments and society in general. On this issue, it is worth highlighting the fundamental role played by the collaboration and presence of parents or legal guardians in a responsible manner in the lives of children and adolescents, especially in their interactions with the digital ecosystem.

5. **What good practices related to transparency and the provision of information in a simple, clear and accessible manner can be observed by digital platforms when processing the personal data of children and adolescents?**

6. **Are there any other issues related to the processing of children's and adolescents' personal data that deserve clarification or additional regulation?**

São Paulo, 16 de agosto de 2024

À
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação Geral de Normatização – CGN/ANPD

Ref.: Tomada de Subsídios | Estudo Preliminar: Tratamento de Dados Pessoais de Crianças e Adolescentes

Prezado Sr. Coordenador Geral de Normatização,

A B3 S. A. – Brasil, Bolsa, Balcão ("B3") submete a esta Autoridade de Proteção de Dados Pessoais ("ANPD") seus comentários à Tomada de Subsídios acerca do Tratamento de Dados Pessoais de Crianças e Adolescentes ("Tomada de Subsídios").

No âmbito da Tomada de Subsídios, a ANPD solicita contribuições sobre o tema a partir de 11 perguntas, que se dividem em 03 blocos: (i) Princípio do Melhor Interesse, (ii) Consentimento e (iii) Jogos e Aplicações de *Internet*.

Nesse sentido, para adequada entrega de nossas contribuições, trazemos abaixo os questionamentos direcionados por esta Autoridade na Tomada de Subsídios, e as respectivas respostas da B3 a cada uma delas. Observamos que a participação da B3 será restrita aos blocos mencionados nos itens (i) e (ii).

I) Princípio do Melhor Interesse

Pergunta ANPD n.º 1: Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Resposta B3: O Princípio do Melhor Interesse da Criança e do Adolescente envolve um conjunto amplo de mecanismos jurídicos voltados à tutela da criança e do adolescente e está previsto, expressamente, no inciso IV do parágrafo único do art. 100 do Estatuto da Criança e Adolescente - ECA[1], como um dos princípios que devem ser observados para

[1] Art. 100. Na aplicação das medidas levar-se-ão em conta as necessidades pedagógicas, preferindo-se aquelas que visem ao fortalecimento dos vínculos familiares e comunitários. Parágrafo único. São também princípios que regem a aplicação das medidas: I - condição da criança e do adolescente como sujeitos de direitos: crianças e adolescentes são os titulares dos direitos previstos nesta e em outras Leis, bem como na Constituição Federal; II - proteção integral e prioritária: a interpretação e aplicação de toda e qualquer norma contida nesta Lei deve ser voltada à proteção integral e prioritária dos direitos de que crianças e adolescentes são titulares; III - responsabilidade primária e solidária do poder público: a plena efetivação dos direitos assegurados a crianças e a adolescentes por esta Lei e pela Constituição Federal, salvo nos casos por esta expressamente ressalvados, é de

aplicar as respectivas medidas constantes do Capítulo II e garantir a proteção integral do menor.

Nesse sentido, a ANPD deveria regulamentar a aplicação prática do princípio do melhor interesse de forma objetiva, trazendo exemplos de sua aplicação, inclusive, e considerando o disposto no inciso IV referido acima, de que essa aplicação deve ocorrer "sem prejuízo da consideração que for devida a outros interesses legítimos no âmbito da pluralidade dos interesses presentes no caso concreto". Deve-se observar que essa orientação converge com o entendimento da ANPD sobre a utilização das demais hipóteses legais presentes nos arts. 7 e 11 da LGPD[2] para o tratamento dos dados de crianças e adolescentes, e não apenas o consentimento.

Nesse sentido, para além de regulamentar de forma prática a aplicação do princípio do melhor interesse conforme indicado acima, é importante que a Autoridade também defina, expressamente, se a aplicação dos princípios da LGPD e dos requisitos presentes da norma (medidas técnicas e de segurança, finalidade legítima, base legal válida, anonimização, minimização dos dados etc.,) já serão capazes de atender ao que a autoridade tem como expectativa quando o tratamento envolver dados pessoais de crianças e adolescentes.

---

responsabilidade primária e solidária das 3 (três) esferas de governo, sem prejuízo da municipalização do atendimento e da possibilidade da execução de programas por entidades não governamentais; IV - interesse superior da criança e do adolescente: a intervenção deve atender prioritariamente aos interesses e direitos da criança e do adolescente, sem prejuízo da consideração que for devida a outros interesses legítimos no âmbito da pluralidade dos interesses presentes no caso concreto; V - privacidade: a promoção dos direitos e proteção da criança e do adolescente deve ser efetuada no respeito pela intimidade, direito à imagem e reserva da sua vida privada; VI - intervenção precoce: a intervenção das autoridades competentes deve ser efetuada logo que a situação de perigo seja conhecida; VII - intervenção mínima: a intervenção deve ser exercida exclusivamente pelas autoridades e instituições cuja ação seja indispensável à efetiva promoção dos direitos e à proteção da criança e do adolescente; VIII - proporcionalidade e atualidade: a intervenção deve ser a necessária e adequada à situação de perigo em que a criança ou o adolescente se encontram no momento em que a decisão é tomada; IX - responsabilidade parental: a intervenção deve ser efetuada de modo que os pais assumam os seus deveres para com a criança e o adolescente; X - prevalência da família: na promoção de direitos e na proteção da criança e do adolescente deve ser dada prevalência às medidas que os mantenham ou reintegrem na sua família natural ou extensa ou, se isso não for possível, que promovam a sua integração em família adotiva; XI - obrigatoriedade da informação: a criança e o adolescente, respeitado seu estágio de desenvolvimento e capacidade de compreensão, seus pais ou responsável devem ser informados dos seus direitos, dos motivos que determinaram a intervenção e da forma como esta se processa; XII - oitiva obrigatória e participação: a criança e o adolescente, em separado ou na companhia dos pais, de responsável ou de pessoa por si indicada, bem como os seus pais ou responsável, têm direito a ser ouvidos e a participar nos atos e na definição da medida de promoção dos direitos e de proteção, sendo sua opinião devidamente considerada pela autoridade judiciária competente, observado o disposto nos §§ 1 o e 2 o do art. 28 desta Lei. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/L8069compilado.htm

2 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Pergunta ANPD n.º 2: Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

Resposta B3: O Enunciado nº 1/2023 da ANPD fixou a interpretação de que é possível utilizar as hipóteses legais previstas no art. 7º, entre as quais está a do legítimo interesse, para o tratamento de dados pessoais de crianças e adolescentes, bem como as previstas no art. 11 da LGPD. Por outro lado, também enfatizou que, nessas situações, o tratamento deve sempre atender a um requisito adicional: a observância e a prevalência do princípio do melhor interesse da criança ou adolescente, conforme determina o art. 14 da LGPD. Assim, o Guia Orientativo sobre a hipótese legal do legítimo interesse já aborda que, quando houver a utilização de dados pessoais de crianças e de adolescentes, o controlador deverá elaborar relatório de impacto à proteção de dados pessoais.

Dessa forma, entendemos que o tema já está adequadamente tratado.

II) Bloco sobre Consentimento

Pergunta ANPD n.º 1: Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

Resposta B3: Para a adequada obtenção do consentimento, devem ser observados os seguintes critérios e parâmetros:

a) Finalidade: o consentimento deve ser solicitado para finalidades específicas e claramente definidas. Os pais ou responsáveis devem ser informados de forma transparente e exata sobre quais dados serão tratados, quais tratamentos serão realizados e para quais finalidades.
b) Visibilidade da solicitação do consentimento: o pedido de consentimento deve ser apresentado de forma destacada. Isso pode incluir o uso de fontes maiores, cores contrastantes, ou caixas de diálogo separadas do restante do conteúdo apresentado.
c) Transparência: todas as informações necessárias devem ser fornecidas de forma clara e acessível, incluindo a identidade do controlador, os direitos dos titulares dos dados, e as formas de contato para esclarecimento de dúvidas. Além disso, a linguagem deverá ser acessível e simples, evitando-se o uso de jargões técnicos ou legais que possam dificultar a compreensão.
d) Revogação simplificada do consentimento: o consentimento deve ser facilmente revogável a qualquer momento. Os pais ou responsáveis devem ser informados sobre como podem revogar o consentimento e as consequências dessa revogação.

e) Verificação de Identidade: devem ser implementados mecanismos para verificar se o consentimento está sendo fornecido por um dos pais ou pelo responsável legal da criança, especialmente em ambientes digitais. Pode ser utilizado, por exemplo, assinatura digital e conferência na base da Receita Federal.

Pergunta ANPD n.º 2: Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

Resposta B3: Sugerimos a adoção das seguintes medidas e mecanismos:

a) Autenticação e verificação de identidade: implementar processos que exijam a apresentação de documentos de identidade dos pais ou responsáveis para verificar sua autenticidade, como por exemplo, a utilização de assinatura digital e conferência na base da Receita Federal.
b) Autenticação multifator: utilizar autenticação multifator (MFA) para garantir que a pessoa que está fornecendo o consentimento é realmente um dos pais ou o responsável legal.
c) Tecnologias de reconhecimento: implementar tecnologias de reconhecimento facial ou biometria, quando apropriado e seguro, para verificar a identidade dos responsáveis.
d) Manutenção de registros: manter registros detalhados do consentimento obtido, incluindo data, hora, método de verificação e as informações fornecidas.
e) Rotinas de revisão e atualização: criar métodos para revisar periodicamente o consentimento para garantir que ele continue relevante e adequado às finalidades do tratamento de dados.
f) Notificações de alterações: informar os pais ou responsáveis sobre qualquer mudança significativa nas práticas de tratamento de dados e obter novo consentimento, se necessário.
g) Segurança e proteção de dados: fazer uso de criptografia para proteger os dados pessoais durante a transmissão e o armazenamento.

Pergunta ANPD n.º 3: No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer

consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

Resposta B3: Segundo o Enunciado 692 da IX Jornada de Direito Civil[3], a LGPD, ao dispensar o consentimento de pelo menos um dos pais ou do responsável legal para que haja o tratamento de dados pessoais de adolescentes, reconhece a redução gradual da autoridade parental face ao amadurecimento do menor. O dispositivo trazido acolhe a realidade fática de inserção digital precoce e reconhece a gradativa construção da personalidade do adolescente no meio digital. Assim, a LGPD já relativiza o regime das incapacidades do Código Civil, ao passo que faz prevalecer o entendimento de que à medida do crescimento, o adolescente adquire paulatinamente a capacidade de discernir e decidir, devendo ser respeitada a dimensão da responsabilidade consequente do ato a ser praticado. No entanto, no contexto da autonomia progressiva, é necessário que a ANPD identifique os cenários em que essa autonomia pode ser exercida, como em plataformas educacionais e redes sociais, onde a privacidade e a confidencialidade são cruciais para o bem-estar do adolescente.

A B3 agradece a oportunidade de contribuir com esta Tomada de Subsídios e se coloca à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

B3 S. A. – BRASIL, BOLSA, BALCÃO

3 Disponível em https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf/view.

TOMADA DE SUBSÍDIOS: TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

I - Princípio do melhor interesse

De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse.

Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança,[1] no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU[2] e no Comentário Geral n° 25, de 2021, do Comitê dos Direitos da Criança.[3] Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz.

1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?

Em seu Guia Orientativo sobre a base legal do legítimo interesse, a ANPD dispõe, brevemente, sobre o melhor interesse da criança, reconhecendo se tratar de um conceito

---

[1] FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). **Convenção sobre os Direitos da Criança.** Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em 14.08.2024.

[2] UNITED NATIONS. **General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration**. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em 14.08.2024.

[3] 8 UNITED NATIONS. **General comment No. 25 (2021) on children's rights in relation to the digital environment.** Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em 14.08.2024.

plurívoco e cuja observância deve ser prioritária em todas as operações de tratamento de dados pessoais de crianças e adolescentes. Dada a centralidade do conceito para a efetiva garantia dos direitos de crianças e adolescentes, seria interessante que a ANPD produzisse material que detalhe e sistematize as orientações já dadas aos controladores de dados pessoais no referido Guia, buscando conferir-lhes amplitude suficiente para que se apliquem plenamente a qualquer operação de tratamento de dados pessoais de crianças e adolescentes e não apenas àquelas que tenham por base legal o legítimo interesse do controlador.

Nesse material, a ANPD poderia aprofundar o que deve ser entendido por tratar os dados de crianças e adolescentes em seu melhor interesse, como dispõe o art. 14, caput da LGPD, usando o Comentário Geral N. 14 como fio norteador e esclarecendo que o conceito abrange, no mínimo i) a priorização, em absoluto, da proteção dessas pessoas nas operações de tratamento de dados pessoais, devendo o controlador avaliar previamente se, na prática, poderá realizar o tratamento de dados pessoais de crianças e adolescentes e adotar medidas procedimentais para o resguardo dos seus direitos (como a elaboração de RIPD), implementar medidas de mitigação de riscos, adaptar os seus produtos e serviços para que incorporem os direitos das crianças e adolescentes em seu design e a monitorar a efetividade dessas medidas, prestando contas à sociedade; e ii) o respeito e a promoção dos direitos garantidos a essas pessoas à luz de suas circunstâncias concretas, levando em conta as suas opiniões e os insumos fornecidos por especialistas, especialmente nas situações em que houver possíveis conflitos de direitos. Destaca-se que a ANPD, no Guia relativo à base legal do legítimo interesse, determina que os controladores devem demonstrar "o que foi considerado como sendo o melhor interesse da criança ou do adolescente", orientação que, apesar de absolutamente pertinente, poderia ser mais explorada, a partir de parâmetros nacionais e internacionais.

Em termos sucintos, é preciso que a ANPD detalhe a aplicação da garantia do melhor interesse, que se desdobra tanto em deveres de conduta para os controladores quanto na aferição das medidas que melhor atenderão à efetivação e proteção plena dos direitos das crianças e dos adolescentes a partir da consideração de suas circunstâncias concretas. O Instituto Alana, na contribuição apresentada à Coordenadoria Geral de fiscalização desta Autoridade no processo fiscalizatório nº 00261.000297/2021-75, detalha a forma como o

melhor interesse deve ser compreendido, ficando à disposição desta Coordenadoria para apresentar insumos mais aprofundados sobre outros pontos não detalhados naquela ocasião, como a aferição do melhor interesse em casos concretos.

Além disso, é preciso que a Autoridade forneça parâmetros que esclareçam quais controladores deverão adotar diligências para respeitar o melhor interesse de crianças e adolescentes. Não basta, nesse sentido, que se vinculem a essas obrigações somente os controladores que afirmem tratar dados desse grupo de pessoas; aqueles que, na prática, realizam ou possam realizar operações de tratamento que afetem crianças e adolescentes, ainda que não intencionalmente, devem estar adstritos à avaliação dos impactos da operação e ao dever de cuidado para com as crianças e os adolescentes, que tanto deverá ser maior quanto maiores os potenciais riscos aos direitos de titulares oferecidos pelo tratamento.

Por fim, é imprescindível que a ANPD busque fornecer orientações concretas sobre situações nas quais a forma de melhor atender ao melhor interesse de crianças e adolescentes não é clara ou envolve o balanceamento de diferentes direitos. Como exemplos, citam-se as discussões sobre a verificação etária e as relacionadas à criptografia, conforme será explorado mais detalhadamente na resposta ao item 3.3.

2. Existem <u>situações ou contextos específicos</u> de tratamento de dados pessoais de crianças e adolescentes que <u>demandam maior atenção e detalhamento</u> sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

Sim. A seguir, são enumerados contextos e situações que demandam maior atenção à luz das principais questões envolvidas e falta de regulamentação específica, conforme demonstrado abaixo:

- Dados Estudantis: no âmbito educacional, o tratamento de dados desses indivíduos é particularmente sensível. A ANPD deve estabelecer diretrizes para garantir que as informações dos estudantes sejam tratadas com rigor, respeitando a privacidade e os direitos dos mesmos. Nesse sentido, Organizações. Educacionais têm como obrigação

informar aos responsáveis sobre como os dados são coletados, armazenados e utilizados, incluindo: (i) a participação da comunidade escolar (ii) a garantia real do consentimento pelos responsáveis; (iii) por respeito ao princípio da transparência[4], quais os dados serão usados e as suas finalidades; e (iv) quais medidas de segurança são necessárias para a proteção dos dados dos estudantes.

- Reconhecimento facial em escolas: a implementação desses sistemas em escolas para controle de acesso e segurança, sem a devida regulamentação, pode resultar em violação. Em escolas do Paraná[5], isso gerou preocupações quanto à violação de direitos e a conformidade com a legislação. Pesquisa realizada pelo APP-Sindicato e o Instituto IPO destaca várias falhas e riscos associados a essas tecnologias: (i) falta de consulta pública; (ii) desconsideração à LGPD e ECA; (iii) ausência de avaliação de impactos na coleta de dados; (iv) política de consentimento inadequada; (v) custos de implementação totalmente questionáveis; (vi) limitações técnicas e preocupações quanto à proteção de dados sensíveis, como etnia e gênero, resultando em discriminação e exclusão de grupos vulneráveis.
- Reconhecimento Facial na Segurança Pública: o uso de tecnologias de reconhecimento facial na segurança pública traz preocupações graves quanto à violação da privacidade e de outros direitos individuais. Como exemplo, cita-se a ação civil pública ajuizada contra o Metrô de São Paulo em razão da implementação de sistemas de reconhecimento facial na linha vermelha[6], na qual destacam-se os riscos associados a essa tecnologia e as implicações legais de seu uso, como: (i) violação da privacidade em espaços públicos; (ii) discriminação devido às altas taxas de erro de etnia e gênero e afetando

---

[4] Observação: *O princípio da transparência, previsto na LGPD, exige que os titulares de dados pessoais sejam informados de maneira clara, precisa e acessível sobre o tratamento de seus dados, incluindo quais dados serão coletados, a finalidade do uso desses dados, e outras informações relevantes que garantam a compreensão plena do processo de tratamento de dados. No caso de crianças e adolescentes, esse dever de transparência é ainda mais rigoroso devido à sua condição de pessoas em desenvolvimento, conforme estabelecido no art. 14, §2º (dever de prestação de contas qualificado), art. 14, §§3º e 4º (dever de minimização da coleta de dados qualificado), e art. 14, §6º (dever de transparência qualificado) da LGPD*.

[5] APP SINDICATO. **Reconhecimento facial nas escolas do Paraná viola direitos das crianças e promove controle social, aponta estudo**. Disponível em: https://appsindicato.org.br/reconhecimento-facial-nas-escolas-do-parana-viola-direitos-das-criancas-e-promove-controle-social-aponta-estudo/#:~:text=Reconhecimento%20facial%20nas%20escolas%20do,promove%20controle%20social%2C%20aponta%20estudo. Acesso em 14.08.2024.

[6] G1. **Justiça de SP determina que Metrô interrompa implantação de sistema de reconhecimento facial.** Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/03/22/justica-de-sp-determina-que-metro-interrompa-implantacao-de-sistema-de-reconhecimento-facial.ghtml. Acesso em 14.08.2024

desproporcionalmente crianças e adolescentes de comunidades vulneráveis; (iii) inibição na liberdade de expressão e a participação em manifestações públicas; (iv) ausência da transparência e clareza da coleta de dados e (v) riscos de abusos por autoridades.

- Casos de exposição de dados em aborto legal[7]: Casos em que crianças e adolescentes tiveram seus dados expostos na Internet por realizarem abortos legais, que resultaram em danos irreparáveis, tendo, como exemplo, o caso ocorrido após uma publicação que divulgou ilegalmente o nome da criança e o hospital onde o procedimento iria ser realizado.
- Perfilamento comercial[8]: o perfilamento comercial de crianças e adolescentes é prática que colide com o seu melhor interesse, na medida em que se volta à manipulação de comportamentos e indução abusiva ao consumo. Sendo prática corrente nos modelos de negócios de grandes empresas atuantes no ambiente digital, como fornecedoras de redes sociais e jogos online, necessário que a ANPD publique enunciado reconhecendo expressamente a ilegalidade e abusividade da prática, em linha com a normatização vigente em outras jurisdições.
- Redes sociais e jogos online: nas redes sociais, a exposição a conteúdos inadequados, assédio e bullying são riscos que se relacionam ao tratamento de dados pessoais dos usuários e que demandam mecanismos eficazes para a proteção integral, incluindo uma noção de supervisão parental que apoie a autonomia progressiva ao mesmo tempo que proteja crianças e adolescentes do risco de violências intrafamiliares. Em jogos online, a coleta de dados para monetização e a proteção contra dependência e interações prejudiciais são questões críticas, que precisam ser reguladas com urgência.

II - Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o

[7] MPMT. **Brasil registra 6 abortos por dia em meninas entre 10 e 14 anos estupradas**. Disponível em: https://www.mpmt.mp.br/conteudo/733/89778/brasil-registra-6-abortos-por-dia-em-meninas-entre-10-e-14-anos-estupradas. Acesso em 14.08.2024.

[8] Criança e Consumo. **O MELHOR INTERESSE DE CRIANÇAS E ADOLESCENTES E AS BASES LEGAIS APLICÁVEIS AO TRATAMENTO DE SEUS DADOS PESSOAIS**. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2023/03/O-MELHOR-INTERESSE-DE-CRIANCAS-E-ADOLESCENTES-E-AS-BASES-LEGAIS-APLICAVEIS-AO-TRATAMENTO-DE-SEUS-DADOS-PESSOAIS.pdf. Acesso em 14.08.2024.

ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

Para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais, conforme exigido pelo §5º do Art. 14 da Lei Geral de Proteção de Dados Pessoais (LGPD), é essencial observar uma **análise dos deveres de conduta de proteção, informação e lealdade qualificados pelo art. 6º, *caput* e art. 14 e §§, em especial, 1º, 2º e 6º.** Tratando-se de atividade de impacto a direitos de crianças e adolescentes, a LGPD exige **esforços qualificados de garantia de informação e demais direitos dos responsáveis legais** (art. 14, §6º LGPD) e **de toda a sociedade no exercício de sua responsabilidade compartilhada constitucionalmente** (art. 14, §2º, LGPD; art. 227, CF/88).

- O art. 14, §2º, exige informações públicas e detalhadas sobre: **i) dados coletados de criança e adolescentes, ii) forma de uso** e **iii) procedimentos para exercício de direitos de titulares.**
- O art. 14, §6º exige, do controlador, a adoção de medidas procedimentais, como consideração das características das **crianças, adolescentes e responsáveis** para conseguir prover **informações simples, claras e acessíveis às suas necessidades.** Indica também o **uso de recursos audiovisuais** para garantia da compreensão.

O que tem-se é a **qualificação de deveres anexos dos controladores visando à plena compreensão do tratamento de dados pessoais que afetam os direitos e melhor interesse de crianças e adolescentes pelos responsáveis legais e a sociedade**, inclusive no estabelecimento de compreensão para legitimidade da base legal do **consentimento.**

A Autoridade Nacional de Proteção de Dados (ANPD) tem um papel fundamental em promover e consolidar um ambiente normativo e regulatório que valorize a acessibilidade, o uso de linguagem simples, e a consideração das necessidades específicas de pessoas com deficiência como orientações centrais para a construção de uma Internet inclusiva, criativa e justa.

É primordial orientar controladores na garantia de:

1. **Linguagem Simples, Recursos Audiovisuais e Facilitação da Compreensão:** Devem ser utilizados recursos audiovisuais que facilitem a compreensão das informações, especialmente para públicos que possam ter dificuldades de leitura ou entendimento. Esses recursos podem incluir vídeos, áudios, infográficos e outras formas de comunicação visual e a priorização de orientações sobre técnicas de hierarquia da informação e padrões de acessibilidade em prol da devida compreensão de todos, sem discriminação.
2. **Transparência "On-Time" no digital e fora das telas:** As informações devem ser fornecidas no momento certo, coibindo que sejam relegadas a termos complexos, extensos e fictícios.
3. **Coibição, em absoluto, de táticas manipulativas de design[9] na interface de plataformas.** Práticas como o mascaramento de informações, redações enganosas, obstruções e indução de escolhas de compartilhamento de dados pessoais com o uso de cores atrativas exploram e manipulam a vulnerabilidade das pessoas (crianças, adolescentes e famílias) e causam um falso sentimento de escolha informada quando,

[9] "(...) um conjunto de técnicas de design que visam manipular o comportamento dos usuários para desempenharem ações que eles não desejariam em outra ocasião, como, por exemplo, entregar mais dados pessoais ou comprar um produto. Para crianças e adolescentes, dependendo da faixa etária e da maturidade, há uma falta de discernimento para compreender a manipulação em serviços e plataformas digitais os colocam em grande risco.". IP.REC. **Relatório Termômetro do Acesso Adequado à Idade**: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais. 2024. p. 48. Disponível em: https://ip.rec.br/wp-content/uploads/2024/07/Termometro-do-Acesso-Adequado-a-Idade-enderecando-o-acesso-apropriado-para-criancas-e-adolescentes-em-plataformas-digitais.pdf. Acesso em 16.08.2024.

na prática, as estratégias ampliam a assimetria informacional e de poder entre titulares e agentes de tratamento de dados e ferem a autodeterminação informacional[10].

4. **Exigibilidade proporcional ao risco do tratamento e à capacidade econômica do controlador.** Quanto maior o potencial de impacto negativo aos direitos de crianças e adolescentes, maior a capacidade econômica do controlador e maior a sua capacidade tecnológica, mais exigíveis e rigorosos devem ser os esforços para assegurar que o consentimento seja devidamente qualificado e baseado em uma compreensão mútua. Não é aceitável, ainda, que grandes empresas de análise de dados e distribuição de fluxo de informações cumpram suas obrigações de forma a mascarar realidades, entregar informações desorganizadas ou dificultar a compreensão de riscos e atividades de tratamento por toda a sociedade.

5. **Ônus da Prova para os Controladores.** As empresas têm a responsabilidade de demonstrar que o consentimento obtido atende a todos os requisitos legais e éticos. A verificação deve ser transparente e auditável, garantindo que a ANPD e outros órgãos possam assegurar o cumprimento dos direitos dos titulares de dados. Os esforços de obtenção de consentimento devem ser documentados à luz da obrigação do art. 14, §5º da LGPD, demonstrando **consideração apropriada de tecnologias disponíveis no contexto concreto da avaliação dos impactos e riscos a direitos de crianças e adolescentes e consideração dos direitos dos responsáveis afetados,** garantindo a proteção também de seus dados**.**tratamento de dados sejam claras, acessíveis e compreensíveis para os responsáveis legais e garantindo a devida informação também a todos atores da sociedade, co-obrigados na responsabilidade compartilhada pela proteção integral.

2. **Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?**

[10] DECEPTIVE PATTERNS. **Types of deceptive pattern.** [s.d.]. Disponível em: https://www.deceptive.design/types. Acesso em 17.07.2024.

1. **Comprovação da Responsabilidade Legal:** Os controladores devem implementar mecanismos que comprovem que a pessoa que fornece o consentimento é, de fato, o responsável legal pela criança. No artigo "*How do They Know It's a Child?*", a organização *5rights* mapeia contextos de uso e pontos de atenção à privacidade e proteção de dados pessoais para autenticação de identidade.

2. Para contribuir com o importante debate, o Instituto Alana preparou um quadro anexo que mapeia métodos de garantia etária, incluindo verificação, estimativa e autenticação, elaborado a partir do documento.

3. Destaca-se a necessidade de garantir **medidas procedimentais na garantia de direitos no tratamento de dados pessoais da pessoa responsável e da criança e do adolescente que possa vir a ser efeito de procedimento adotado de autenticação para garantia de consentimento.**

Indica-se, nesse sentido:

4. **Adoção de "Todos os Esforços Razoáveis"**: A aplicação desse conceito implica em um conjunto de práticas e medidas que vão além do mínimo exigido, considerando as melhores práticas do mercado e as tecnologias disponíveis em prol do desenvolvimento integral. Isso inclui a revisão periódica dos processos de verificação, a atualização contínua das ferramentas de segurança e a adaptação dos métodos de verificação para acompanhar as evoluções tecnológicas e as mudanças regulatórias. Também exige investimentos para coibir riscos inerentes ao modelo de negócios e colaborar no desenvolvimento de soluções técnicas que reforcem a proteção de dados de crianças e adolescentes.
5. **Múltiplos Meios de Verificação**: Considerando a diversidade tecnológica e social, os controladores devem oferecer meios alternativos para a autenticação, adaptados ao público-alvo e ao contexto de tratamento. Tal forma coíbe o risco de que medida exclusiva de autenticação implique exclusão de oportunidade no ambiente digital e a análise deve ser amparada com lastro de avaliação do melhor interesse no caso concreto.

6. **Coibição da Geração de Perfis Comportamentais familiares com dados de garantia etária:** Ao conectar dados de contas de adultos com contas de crianças, cria-se o risco de perfilamento comportamental, o que vulnerabiliza ambas as partes. Dados usados para verificação de consentimento devem ser restritos a essa finalidade, coletados no mínimo escopo necessário.
7. **Prevenção, Segurança e Proteção**: Para proteger as informações durante a verificação de identidade e idade, devem ser empregadas técnicas robustas de segurança, como criptografia de ponta a ponta, assegurando a proteção dos dados na coleta, transmissão e armazenamento.[11].
8. **Retenção e minimização:** Os dados coletados para verificação de consentimento devem ser retidos apenas pelo tempo necessário para comprovar a validade e conformidade com as exigências legais. É recomendada a priorização de tecnologias que garantam a eliminação dos dados, mas que permitam a certificação da validade do procedimento. Além disso, deve-se documentar todo o processo para garantir auditabilidade e transparência perante órgãos reguladores e os titulares de dados.
9. **Responsabilidade por autenticação que dependa de serviço de terceiros.** Em caso de violações decorrentes de falhas no serviço de autenticação fornecido por terceiros, o controlador continua responsável perante os titulares e a ANPD. É fundamental que o controlador mantenha mecanismos rigorosos de controle e supervisão sobre as diligências de parceiros comerciais e públicos, documentando riscos e benefícios ao escolher serviços de terceiros.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

[11] LIGUORI, Carlos. **Direito e Criptografia - Direitos Fundamentais, Segurança da Informação e os limites da regulação jurídica na tecnologia.** São Paulo: SaraivaJur, 2022, Cap. 1 e 2.

A possibilidade de flexibilização do regime de capacidades do Código Civil para a obtenção do consentimento de adolescentes para o tratamento de seus dados pessoais é debate que contrapõe a autonomia progressiva dessas pessoas à sua segurança, ou, ainda, a proteção de sua privacidade interpessoal à proteção de sua privacidade comercial. Havendo possíveis interpretações distintas da legislação que podem afetar, de maneiras diversas, a esfera de direitos dessas pessoas, imprescindível que o exercício hermenêutico seja pautado pela garantia do melhor interesse, buscando-se a interpretação legal que garanta a proteção e efetivação dos direitos dos adolescentes na maior extensão possível.

Dada a complexidade da questão, o Instituto Alana entende serem necessários debates mais profundos a nível nacional entre todos os stakeholders para que a interpretação da lei que melhor atende aos direitos e interesses de crianças e adolescentes seja consagrada pela ANPD. Sugere-se, assim, que sejam realizadas consultas públicas e tomadas de subsídio especificamente sobre este tema, priorizando a participação e escuta de crianças e adolescentes.

De partida, contudo, parece possível afirmar que admitir uma flexibilização absoluta das normas do Código Civil, para que, em toda e qualquer situação, o consentimento dos adolescentes possa ser dado sem a representação ou assistência parental, não atende ao seu melhor interesse e pode colocar a proteção de seus direitos em xeque, além de não ser congruente com a legislação vigente no Brasil. Conforme explicam Bruno Miragem e Cláudia Lima Marques em parecer concedido ao Instituto Alana sobre o tema, se a regra geral posta pelo Código Civil é pela necessidade de representação ou assistência parental, admitir que ela não se aplique às operações de tratamento de dados pessoais seria admitir que essas operações geram efeitos jurídicos menos relevantes às esferas de direitos dos adolescentes do que outros negócios jurídicos "tradicionais". Essa leitura, contudo, é incongruente com a LGPD, que, justamente reconhecendo os possíveis impactos agravados do tratamento de dados pessoais de crianças e adolescentes sobre os direitos dos titulares, cria tutela específica e protetiva para eles em seu art. 14.

Por outro lado, não se ignora a necessidade de que determinadas operações de tratamento de dados pessoais de adolescentes se deem desacompanhadas da representação ou assistência parental, sob pena de ferir-se a autonomia dessas pessoas em situações nas quais o

acompanhamento dos pais sobre as atividades on-line não necessariamente atende ao seu melhor interesse. Assim, para que se chegue a um ponto de equilíbrio e que se pensem em exceções à regra geral do Código Civil de maneira razoável e que privilegie a proteção integral dos direitos e melhor interesse de crianças e adolescentes, sugerem-se o aprofundamento dos debates e a realização de esforço regulatório específico para este tema.

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital, bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações "estritamente necessárias à atividade".

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada

no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de design, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

Diversos documentos, de caráter normativo ou não, nacionais e internacionais, fornecem orientações sobre as medidas a serem implementadas por plataformas digitais cujo acesso por crianças e adolescentes é provável, no sentido de garantir a proteção de seus dados pessoais. Citam-se, como exemplos, i) O Comentário Geral N. 25 sobre os direitos da criança em relação ao ambiente digital, do Comitê dos Direitos da Criança da ONU, em especial seus parágrafos 67 a 78; ii) O Age Appropriate Design Code desenvolvido pelo ICO, autoridade regulatória do

Reino Unido[12]; iii) O Kids Online Safety Act (KOSA), dos Estados Unidos; iv) o Digital Services Act, da União Europeia; v) o IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, do IEEE[13]; e vi) o Termômetro do Acesso Apropriado à Idade, do IP.Rec[14].

A partir desses parâmetros e de elementos relevantes à realidade brasileira, a ANPD pode desenvolver material voltado para controladores que realizem o tratamento de dados pessoais de crianças e adolescentes, no qual, além de fornecer detalhes acerca da aplicação da garantia do melhor interesse (vide resposta ao item 1.1), pode apresentar parâmetros e salvaguardas a serem implementados para assegurar elevados níveis de privacidade e mitigar os riscos relativos à utilização dessas plataformas, no espírito de construir um Código de Design aplicável aos produtos e serviços digitais disponíveis no Brasil. Como exemplos desses parâmetros, citam-se, tomando-se como referência os documentos mencionados:

- Elaboração de relatório de impacto à proteção de dados (RIPD) sempre que o tratamento de dados de crianças e adolescentes contiver elementos que ofereçam riscos aos seus direitos fundamentais;
- Monitoramento periódico dos impactos e riscos oferecidos pelo produto ou serviço e transparência na divulgação dos resultados;
- Vedação do perfilamento de crianças e adolescentes para fins atentatórios ao seu melhor interesse, sobretudo para o direcionamento de publicidade comportamental;
- Vedação de técnicas de "nudge" que induzam crianças e adolescentes a comportamentos prejudiciais a seus próprios direitos e interesses;
- Configurações padrão (por "default"), as mais protetivas possíveis, para a privacidade quando o usuário for, ou tiver chances consideráveis de ser, uma criança ou um adolescente;

[12] ICO. **Age appropriate design: a code of practice for online services**. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em 14.08.2024.

[13] IEEE XPLORE. I**EEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children**. Disponível em: https://ieeexplore.ieee.org/document/9627644. Acesso em: 14.08.2024.

[14] IP REC. **Termômetro do Acesso Adequado à Idade: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais.** Disponível em: https://ip.rec.br/publicacoes/termometro-do-acesso-adequado-a-idade-enderecando-o-acesso-apropriado-para-criancas-e-adolescentes-em-plataformas-digitais/. Acesso em: 14.08.2024.

- Redução da coleta de dados pessoais ao mínimo necessário para oferecimento do produto ou serviço e proteção dos direitos dos titulares e anonimização dos dados;
- Adequação de interfaces ao estágio de desenvolvimento progressivo de crianças e adolescentes, com o fornecimento de informações adequadas à sua compreensão e à de suas famílias;
- Rigor quanto às políticas de compartilhamento de dados pessoais de crianças e adolescentes com terceiros, garantindo-se que aqueles que recebem esses dados respeitarão o melhor interesse desses indivíduos;
- Políticas de privacidade que garantam a retenção dos dados pessoais de crianças e adolescentes estritamente apenas pelo tempo necessário para o fornecimento do produto ou serviço ou garantia do melhor interesse, vedando-se o tratamento de dados pessoais coletados durante a infância ou adolescência para fins comerciais na vida adulta dos titulares;
- Garantir que o rastreamento da geolocalização de crianças e adolescentes seja desligado por padrão e que os titulares sejam ostensivamente informados caso estejam sendo rastreados, o que só deve ocorrer em seu melhor interesse;
- Implementar ferramentas que facilitem o exercício dos direitos do titular por crianças, adolescentes e suas famílias;
- Disponibilizar ferramentas de acompanhamento e mediação parental de maneira equilibrada com a autonomia da criança ou do adolescente e respeitosa ao seu desenvolvimento progressivo;
- Implementar mecanismos de garantia etária e controle de acesso razoáveis e proporcionais aos riscos oferecidos pelo produto ou serviço aos direitos de crianças e adolescentes.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

- A **garantia etária** é um termo guarda-chuva que inclui soluções de **verificação etária e estimativa de idade.** A palavra garantia remete a diferentes níveis de certeza que

soluções estabelecem ao propor estabelecer uma idade de certo usuário de plataforma digital ou estimar sua faixa etária.

- A **verificação etária** é um processo que depende de identificadores rígidos e/ou outras fontes verificadas de identificação, que proporcionam alto grau de certeza na determinação exata da idade de um usuário.
- **A estimativa de idade** é um processo que estabelece que um usuário: tem uma certa idade, está dentro de uma faixa etária ou está acima ou abaixo de uma certa idade.
- No documento 5Rights - How do They Know It's a Child, alguns métodos mapeados, oferecidos de forma sistematizada em quadro anexo são:
    - **Autodeclaração (Estimativa)**. Utilizada em plataformas como TikTok e Instagram, onde os usuários inserem suas datas de nascimento. Embora medidas técnicas sejam adotadas para desencorajar declarações falsas (como bloqueio de acesso), esse método é facilmente burlável e pode responsabilizar indevidamente crianças e adolescentes. A percepção de risco é baixa, e a eficácia é limitada.
    - **Uso de identificadores duros (Verificação Etária ou Identificação).** Uso de documentos como RG, CPF ou cartão de crédito, cruzados com bases de dados certificadas. É eficaz para identificar maiores de 18 anos, mas menos útil para determinar faixas etárias específicas, especialmente para menores de 18 anos. Um ex.: é o YouTube na Europa, que exige RG ou cartão de crédito para acessar conteúdo 18+.
    - **Biometria (identificação/verificação etária)**, a ex.: de análises de métricas e dados corporais e biológicos. O método do reconhecimento facial, em especial, tem sido identificado como ineficiente para crianças e adolescentes, não sendo apropriado para distinguir pessoas **entre idades próximas**. A sensibilidade dos dados tratados e os notórios casos de impacto a direitos fundamentais fazem questionar tratar-se de método adequado. Qualquer uso deve ser atrelado a padrões altos de prestação de contas, garantia de auditorias independentes e fortes requisitos de transparência. A má utilização de dados pode ensejar em usos absolutamente ilegítimos, a exemplo de análise emocional da criança e do adolescente. O método, entretanto, é usado para operações de segurança no combate ao abuso e exploração sexual, a ex.: de softwares que rastreiam faces de

crianças em exibição em sites de pornografia a fim de identificar caso de possível abuso e exploração sexual.

- **Teste de capacidade (estimativa)**, Inclui quizzes ou testes de linguagem e matemática. Deve ser usado com cautela, pois capacidade e idade não são sinônimos, e o método é facilmente fraudável. É recomendado como complemento a outras estratégias, mas não pode determinar a idade exata.
- **Autenticação entre contas (single sign on):** Permite que um novo serviço acesse dados do usuário de outra plataforma via API. Depende da qualidade de autenticação da plataforma original. No caso de uso deste método, a **transferência de dados deve ater-se à minimização e vinculação estrita à legitimidade de verificação etária**, coibindo práticas que criam perfis de monitoramento compartilhados de crianças e adolescentes entre diferentes redes.
- **Provedor de garantia de idade terceirizado:** Em que pese ser solução que depende de padrões de segurança para garantia da integridade do terceiro autenticador, políticas de *tokens* de idade e de validação etária por provedores de certificados podem apoiar uma minimização na medida em que não é necessário transmitir outras informações além da confirmação de *query* de idade.
- **Controles de dispositivo/sistema operacional** (estimação/verificação)**:** Permite que sistemas operacionais definam a experiência adequada para crianças e adolescentes, com base na estimativa etária. Pode haver conflitos em ambientes onde o uso de dispositivos é compartilhado. Seu uso deve ser modulado para garantir uma abordagem de supervisão parental à luz da noção de parentalidade positiva e respeito à autonomia progressiva, evitando que a implementação de filtros e controles impactam direitos à informação, privacidade e outros aspectos da criança e do adolescente.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

O Comentário Geral n° 25 reconhece os impactos negativos dos sistemas de recomendação algorítmica sobre os direitos de crianças e adolescentes. No parágrafo 62, alerta que esses sistemas podem inferir o estado emocional das crianças, sendo necessário que os Estados garantam que não sejam usados para influenciar seu comportamento ou limitar suas oportunidades e desenvolvimento. A interpretação da ANPD sobre perfilamento comportamental deve reafirmar as disposições da Convenção sobre os Direitos da Criança, com base nos parágrafos 42, 53 e 62 do Comentário Geral n° 25, que estabelece parâmetros claros para a formação de perfis e práticas de tratamento de dados.

1. **Interesse Prioritário e Justificado**: O perfilamento de crianças e adolescentes deve ser conduzido com foco na garantia do melhor interesse desse público. Qualquer atividade de perfilamento deve ser rigorosamente avaliada para assegurar que não prejudique, mas promova seu bem-estar e direitos fundamentais em sua maior extensão possível.
2. **Proibição de Perfilamento para Publicidade**: Todas as práticas de tratamento de dados que visem ao perfilamento comportamental para direcionamento de publicidade são ilegais desde a coleta, devido à hipervulnerabilidade das crianças. Isso inclui a análise emocional, neuromarketing e uso de dados para criar perfis destinados ao direcionamento de comunicação mercadológica. A proibição abrange tanto perfis individuais quanto grupais e protege a privacidade de crianças e adolescentes quanto à atributos inferidos de sua análise comportamental.
3. **Desativação Padrão de Perfilamento Comportamental**: O perfilamento comportamental para direcionamento de publicidade deve ser desligado por padrão, especialmente quando não há verificação confiável da idade do usuário, de forma a não colocar a criança ou adolescente que acessa ou burla sistema de garantia etária de plataforma em risco de exploração comercial. Nenhuma coleta de dados comportamentais, rastreamento ou monitoramento deve ocorrer automaticamente ou de forma oculta, posto que isto coloca mais em riscos os direitos e melhor interesse de crianças e adolescentes e fomenta cultura de monitoramento e rastreamento. Configurações padrões mais protetivas para adultos são medidas de design a serem

exigidas em casos concretos de evidências notórias de falhas de mecanismos de verificação etária. Caso o controlador não seja capaz de implementar medidas que impeçam a exploração comercial dos dados de crianças e adolescentes neste fim, deve deixar de realizar a atividade.

4. **Promoção do Empoderamento e Autonomia**: O processo de perfilamento deve ser orientado por princípios que promovam o empoderamento, direito à informação, autonomia e liberdade das crianças e adolescentes. Plataformas digitais devem criar ambientes apropriados à idade, respeitando a capacidade e estágio de desenvolvimento do usuário.
5. **Direito de Reset**: Crianças e adolescentes devem ter o direito de redefinir, controlar ou apagar seus perfis e históricos digitais a qualquer momento, com comunicação facilitada e acessível para esse exercício. Esse "direito de reset" assegura a proteção da privacidade e o direito ao esquecimento.
6. **Proibição do Uso de Dados a Longo Prazo**: Dados coletados durante a infância ou adolescência não podem ser utilizados posteriormente para perfilamento comercial. A proteção desses dados deve se estender ao longo da vida, respeitando o contexto em que foram inicialmente coletados.
7. **Sistemas de Recomendação Transparente**: Sistemas de recomendação de conteúdo não devem priorizar conteúdos pagos ou com motivação comercial em detrimento do direito à informação das crianças e adolescentes (CG25, §62).
8. **Reparação de Danos**: Deve ser garantida a devida reparação à criança ou adolescente que sofreu perfilamento que afetou negativamente sua esfera de proteção de direitos.
9. **Restrições à Análise Emocional**: Sistemas de recomendação de conteúdo, mesmo que orgânicos, não devem realizar direcionamento baseado em análise emocional, evitando a exploração de vulnerabilidades e o reforço de padrões negativos repetitivos, conhecidos como "efeito toca de coelho".
10. **Responsabilidade das Plataformas**: Grandes plataformas digitais que lucram com a gestão de informações e anúncios por meio de análises comportamentais devem garantir um plano específico para abordar riscos e danos do perfilamento, levando em consideração as peculiaridades das múltiplas infâncias brasileiras.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

- Parentalidade Positiva (Lei nº 14.826/2024)[15] e Autonomia Progressiva[16]: a Lei mencionada enfatiza a importância da parentalidade positiva e da consideração da autonomia progressiva no desenvolvimento de crianças e adolescentes. Além disso, a lei promove respeito, acolhimento e não violência na educação, garantindo um ambiente seguro a crianças e adolescentes. Esses usuários devem adquirir mais controle sobre seus dados à medida que ficam mais velhos, sempre com orientação e supervisão dos responsáveis, por meio de configurações de privacidade adaptáveis.
- A personalização das plataformas digitais por faixa etária é essencial para ampliar o controle dos responsáveis sobre o tratamento de dados pessoais. Adaptar conteúdo e interações de acordo com a idade dos usuários assegura que as informações e funcionalidades ofertadas sejam adequadas e seguras. De acordo com o *Design Apropriado para a Idade: Código de Práticas para Serviços Online*[17] , do ICO, isso significa aplicar padrões que proporcionem um nível adequado de proteção aos dados das crianças e adolescentes, adaptando as salvaguardas conforme a faixa etária dos usuários, tornando-se uma prática flexível e ajustada às especificidades de cada serviço online
- A privacidade é um direito fundamental[18] para crianças e adolescentes no ambiente digital. As plataformas digitais devem implementar políticas transparentes

[15] LUNETAS. O que diz a lei de parentalidade positiva e direito ao brincar?. Disponível em: https://lunetas.com.br/o-que-diz-a-lei-de-parentalidade-positiva-e-direito-ao-brincar/. Acesso em 14.08.2024.
[16] CRIANÇA E CONSUMO. **Dados e direitos na infância e adolescência no ambiente digital: caminhos para a proteção jurídica no Brasil e Argentina**. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2022/07/dados-e-direitos-na-infancia-e-adolescencia-no-ambiente-digital.pdf. Acesso em 14.08.2024.
[17] ITS RIO. **Design Apropriado para a Idade: Código de Práticas para Serviços On-line**. Disponível em: https://itsrio.org/wp-content/uploads/2021/08/Design-Apropriado-para-a-Idade_-Codigo-de-Praticas-para-Servicos-Online.pdf. Acesso em 14.08.2024.
[18] INTERNET LAB. **O direito das crianças à privacidade**. Disponível em: https://internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em 14.08.2024.

e eficazes que protejam os dados desses usuários, utilizando métodos como anonimização e minimização de dados para evitar exploração comercial e manipulação comportamental. O Instituto Alana enfatiza, por exemplo, a importância de educar e capacitar[19] os pais e responsáveis sobre o uso seguro da tecnologia.

- Mecanismos para o exercício dos direitos dos titulares, como acesso, correção e exclusão de dados, devem ser simplificados. A LGPD exige que o consentimento parental [20]seja específico e destacado, reforçando a necessidade de ferramentas que facilitem esse processo. As plataformas digitais devem alertar sobre os riscos do compartilhamento irresponsável de dados, por meio de avisos, bem como campanhas educativas para os responsáveis.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

Com o aumento do uso de plataformas online por crianças e adolescentes, que são hipervulneráveis e não têm plena consciência dos riscos envolvidos, é essencial que essas plataformas adotem boas práticas que garantam o melhor interesse da criança e do adolescente, especialmente no que diz respeito à transparência no tratamento de seus dados.

Uma das principais diretrizes para garantir essa transparência é a clareza na comunicação. As organizações devem utilizar uma linguagem simples e acessível, evitando jargões técnicos que possam confundir as crianças e seus responsáveis. Além disso, é fundamental adotar múltiplas linguagens além da escrita, como gráficos, vídeos e elementos interativos, para facilitar a compreensão de como os dados são coletados e utilizados. Isso é

[19]INSTITUTO ALANA; MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. **Comentário Geral N° 25 (2021) sobre os direitos das crianças em relação ao ambiente digital - Versão Comentada. 2022**. Disponível em: https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf. Acesso em 14.08.2024.

[20] MAUK, M. **Parenting and the algorithm: a perspective on parental Controls and guilt amidst digital media. In: Works in Progress • Algorithmic Rights and Protections for Children**, 2021.

crucial para que crianças e adolescentes compreendam seus direitos e as implicações do compartilhamento de suas informações pessoais.[21].

O acesso às informações também é crucial[22]. As políticas de privacidade devem ser facilmente acessíveis e redigidas de forma que as crianças possam entender, com seções específicas voltadas para o público infantil. Ferramentas interativas podem ajudar esses usuários a explorar suas informações e direitos de maneira lúdica, aumentando a compreensão e o engajamento com as questões de privacidade[23].

Além disso, é fundamental que as plataformas ofereçam opções de configuração que permitam que esses usuários gerenciem suas preferências de privacidade de maneira adequada à sua faixa etária.

Outro aspecto essencial é o consentimento[24] e a autorização[25]. A obtenção do consentimento dos responsáveis legais deve ser feita de maneira clara e informada, garantindo que os pais compreendam o que está sendo consentido. Também é importante que as plataformas ofereçam opções de configuração que permitam que crianças e adolescentes gerenciem suas preferências de privacidade.

A educação e a conscientização sobre privacidade digital são indispensáveis. Programas educativos que ensinam crianças e adolescentes sobre segurança online e proteção de dados.

---

[21] 5RIGHTSFOUNDATION. **Approaches to children's data protection A comparative international mapping**. Disponível em: Disponível em: https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf. Acesso em 14.08.2024.

[22] FEDERAL TRADE COMMISSION - PROTECTING AMERICA´S CONSUMERS. **A Guide For Business and Parents And Small Entity Compliance Guide.** Disponível em: Disponível em: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions. Acesso em 14.08.2024.

[23] AN COIMISIÚN UM CHOSAINT SONRAÍ - DATA PROTECTION COMMISSION. **Guidance for children on their data protection rights.** Disponível em: https://www.dataprotection.ie/en/dpc-guidance/childrens-data-protection-rights. Acesso em 14.08.2024.

[24] ICO. **Consent**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/. Acesso em 14.08.2024.

[25] ECOVIS PROVENTUSLAW**. European Data Protection Board adopts guidelines on consent under the GDPR**. Disponível em: https://ecovis.lt/european-data-protection-board-adopts-guidelines-on-consent-under-the-gdpr. Acesso em: 14.08.2024.

Campanhas de sensibilização voltadas para responsáveis também são importantes, pois ajudam a criar um ambiente familiar que valoriza a proteção de dados.

Por fim, é imprescindível evitar a publicidade direcionada a crianças, seja ela simples ou por meio de IA[26]. As organizações devem garantir que informações sobre direitos e privacidade não sejam misturadas com conteúdos publicitários, especialmente em plataformas que não são apropriadas para o público infantil. O cumprimento de regulamentações que proíbem essa prática é essencial para proteger esses usuários de influências ilícitas[27].

Exemplos de boas práticas podem ser observados tanto em âmbito nacional quanto internacional: a ANPD fornece orientações sobre o tratamento de dados pessoais, incluindo orientações específicas para crianças e adolescentes, e o ICO recomenda que as plataformas adotem uma abordagem centrada na criança, com informações claras sobre como os dados são usados e a importância do consentimento.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

Por fim, de maneira complementar às demais considerações apresentadas ao longo das respostas a essa tomada de subsídios, o Instituto Alana apresenta algumas linhas de ação que considera importantes para que a ANPD possa cumprir plena e efetivamente com o papel que lhe cabe na proteção dos direitos de crianças e adolescentes:

- **Realização de tomadas de subsídios e "sandboxes" regulatórios para a regulação de temas complexos e recorrentes do ponto de vista da proteção de crianças e adolescentes:** determinados temas relacionados à proteção de dados pessoais de crianças e adolescentes desafiam a proteção integral desses

[26] CONSUMER PROTECTION REVIEW. **CARU Issues Warning About Using AI in Child-Directed Advertising and Data Collection**. Disponível em: https://www.consumerprotectionreview.com/2024/05/caru-issues-warning-about-using-ai-in-child-directed-advertising-and-data-collection/#more-2643. Acesso em: 14.08.2024.

[27] ICO. **Protecting children's privacy online: Our Children's code strategy**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/. Acesso em: 14.08.2024.

indivíduos na medida em que contrapõem e tensionam diferentes direitos fundamentais garantidos a eles. É o que se verifica, por exemplo, nas discussões relativas à verificação etária e à criptografia, que, de maneira geral, apresentam uma tensão (ao menos aparente) entre os direitos de crianças e adolescentes à privacidade e à segurança. Como antes se expôs, a garantia do melhor interesse presta-se, também, a oferecer parâmetros para que, em casos como esses, sejam adotadas soluções que atendam à proteção e promoção dos direitos dessas pessoas na maior extensão possível, à luz de suas circunstâncias concretas, da escuta de suas vozes e dos insumos fornecidos por especialistas. Assim, considerando que essas discussões afetam uma grande quantidade de controladores e titulares de dados pessoais, a ANPD, orientando-se pela garantia do melhor interesse, pode fazer uso dos instrumentos regulatórios à sua disposição, como tomadas de subsídios e sandboxes, para buscar determinar de que forma esses debates podem ser solucionados na realidade brasileira, de modo a concretizar o melhor interesse das crianças e adolescentes residentes em território nacional. Esses instrumentos, evidentemente, devem ser complementados por iniciativas que garantam a participação de crianças e adolescentes nesses processos, como dispõe o C.G. nº 14.

- **Articulação com o Sistema de Garantia de Direitos da Criança e do Adolescente:** a articulação com outros órgãos integrantes do SGCA é imprescindível para que a ANPD possa ampliar o alcance de suas ações e a sua capacidade fiscalizatória. Parcerias com o Ministério da Educação, por exemplo, podem ser firmadas para disseminar informações sobre a proteção de dados pessoais a crianças e adolescentes de maneira mais efetiva. Ministérios Públicos, Defensorias e órgãos do Sistema Nacional de Proteção ao Consumidor podem contribuir com as investigações conduzidas pela ANPD e colaborar com a investigação de ilícitos. Na mesma toada, é particularmente relevante a articulação com o Conanda, que não apenas detém competência para articular as políticas de proteção à criança e ao adolescente em território nacional, como ainda publicou, em maio, a sua Resolução n° 245, que prevê a criação de uma política nacional para a proteção de crianças e adolescentes nos ambientes digitais. É essencial que a ANPD atue em parceria com o Conanda e oriente sua

atuação pelas disposições da referida Resolução, inclusive no que diz respeito à interpretação a ser conferida à LGPD e às bases legais aplicáveis ao tratamento de dados pessoais de pessoas com menos de 18 anos.

- **Articulação com outras Autoridades de Proteção de Dados em nível internacional:** a colaboração direta com outras Autoridades de Proteção de Dados pode fornecer subsídios importantes para a atuação da ANPD. Investigações conduzidas em outras jurisdições podem servir de ponto de partida para a atuação fiscalizatória da ANPD e aumentar a sua capacidade de monitorar efetivamente a atuação de empresas com atuação transnacional. Além disso, o diálogo com outras Autoridades pode servir para evidenciar políticas discriminatórias de empresas contra países do Sul Global, cuja existência já foi evidenciada em estudos conduzidos sobre o tema. Ainda, podem ser fornecidos insumos relevantes para a avaliação concreta do melhor interesse de crianças e adolescentes, especialmente em se tratando da colaboração com autoridades de outros países latino-americanos.
- **Outros:** recomenda-se à ANPD que adote as diretrizes da Resolução nº 245 do Conanda, citada acima, no seu Enunciado nº 1, ou que considere sua inclusão em futuros enunciados. Além disso, é recomendável que a ANPD dialogue com o CNPD para fomentar o debate sobre a construção de um Código de Design com participação multissetorial, incluindo crianças e adolescentes, à luz das obrigações e boas práticas reconhecidas pelo Comentário Geral n° 25 e por outros parâmetros nacionais e internacionais.

REFERÊNCIAS

FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA (UNICEF). **Convenção sobre os Direitos da Criança.** Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em 14.08.2024.

UNITED NATIONS. **General Comment Nº 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration**. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em 14.08.2024.

8 UNITED NATIONS. **General comment Nº 25 (2021) on children's rights in relation to the digital environment.** Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em 14.08.2024.

COMISSÃO NACIONAL DE PROMOÇÃO DOS DIREITOS E PROTEÇÃO DAS CRIANÇAS E JOVENS. **Interesse Superior da Criança**: **Comentário geral n.º 14 (2013) do Comité dos Direitos da Criança sobre o direito da criança a que o seu interesse superior seja tido primacialmente em consideração**. 1. ed. [S. l.]: Editorial do Ministério da Educação e Ciência, 2017. p. 1-36. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/cdc_com_geral_14.pdf. Acesso em: 14.08.2024.

HENRIQUES, Isabella Vieira Machado. **Direitos Fundamentais Da Criança No Ambiente Digital**: O Dever De Garantia Da Absoluta Prioridade. 2022.

LIGUORI, Carlos. **Direito e Criptografia - Direitos Fundamentais, Segurança da Informação e os limites da regulação jurídica na tecnologia. Cap. 1 e 2.** São Paulo: SaraivaJur, 2022, Cap. 1 e 2.

APP SINDICATO. **Reconhecimento facial nas escolas do Paraná viola direitos das crianças e promove controle social, aponta estudo**. Disponível em: https://appsindicato.org.br/reconhecimento-facial-nas-escolas-do-parana-viola-direitos-das-criancas-e-promove-controle-social-aponta-estudo/#:~:text=Reconhecimento%20facial%20nas%20escolas%20do,promove%20controle%20social%2C%20aponta%20estudo. Acesso em: 14.08.2024

G1. **Justiça de SP determina que Metrô interrompa implantação de sistema de reconhecimento facial.** Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/03/22/justica-de-sp-determina-que-metro-interrompa-implantacao-de-sistema-de-reconhecimento-facial.ghtml. Acesso em 14.08.2024.

MPMT. **Brasil registra 6 abortos por dia em meninas entre 10 e 14 anos estupradas**. Disponível em: https://www.mpmt.mp.br/conteudo/733/89778/brasil-registra-6-abortos-por-dia-em-meninas-entre-10-e-14-anos-estupradas. Acesso em 14.08.2024.

Observação: "*O princípio da transparência, previsto na LGPD, exige que os titulares de dados pessoais sejam informados de maneira clara, precisa e acessível sobre o tratamento de seus dados, incluindo quais dados serão coletados, a finalidade do uso desses dados, e outras informações relevantes que garantam a compreensão plena do processo de tratamento de dados. No caso de crianças e adolescentes, esse dever de transparência é ainda mais rigoroso devido à sua condição de pessoas em desenvolvimento, conforme estabelecido no art. 14, §2º (dever de prestação de contas qualificado), art. 14, §§3º e 4º (dever de minimização da coleta de dados qualificado), e art. 14, §6º (dever de transparência qualificado) da LGPD*".

CRIANÇA E CONSUMO. **O MELHOR INTERESSE DE CRIANÇAS E ADOLESCENTES E AS BASES LEGAIS APLICÁVEIS AO TRATAMENTO DE SEUS DADOS PESSOAIS**. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2023/03/O-MELHOR-INTERESSE-DE-

CRIANCAS-E-ADOLESCENTES-E-AS-BASES-LEGAIS-APLICAVEIS-AO-TRATAMENTO-DE-SEUS-DADOS-PESSOAIS.pdf. Acesso em 14.08.2024.

W3C. **Web Content Accessibility Guidelines (WCAG) 2.1**. "*Para construção de material digital acessível"*. Disponível em https://www.w3.org/TR/WCAG21/. Acesso em 16.08.2024.

Para orientações sobre utilização de Linguagem Simples, ver cartilha "Simples Assim": https://www.arca.fiocruz.br/handle/icict/59614. Acesso em 16.08.2024.

Para dicas de acessibilidade para materiais em redes sociais, ver p. 68 do Guia "Somos Plurais": https://somosplurais.com.br/assets/publicacao-somos-plurais-2021.pdf

Para dicas de acessibilidade na construção de materiais de comunicação, ver material com referências organizadas pela Equipe de Comunicação do Instituto Alana.

BRASIL. Código Civil Brasileiro - **Lei nº 10.406/2002**. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 14.08.2024.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD) - **Lei nº 13.709/2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 14.08.2024.

Criança e Consumo. **Comentário Geral N. 25 sobre direitos da criança em relação ao ambiente digital**. Disponível em: https://criancaeconsumo.org.br/biblioteca/comentario-geral-n-25/. Acesso em 14.08.2024.

ICO. **Age appropriate design: a code of practice for online services**. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em 14.08.2024.

IEEE XPLORE. I**EEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children**. Disponível em: https://ieeexplore.ieee.org/document/9627644. Acesso em: 14.08.2024.

IP REC. **Termômetro do Acesso Adequado à Idade: endereçando o acesso apropriado para crianças e adolescentes em plataformas digitais.** Disponível em: https://ip.rec.br/publicacoes/termometro-do-acesso-adequado-a-idade-enderecando-o-acesso-apropriado-para-criancas-e-adolescentes-em-plataformas-digitais/. Acesso em: 14.08.2024.

LUNETAS. **O que diz a lei de parentalidade positiva e direito ao brincar?**. Disponível em: https://lunetas.com.br/o-que-diz-a-lei-de-parentalidade-positiva-e-direito-ao-brincar/. Acesso em 14.08.2024.

CRIANÇA E CONSUMO. **Dados e direitos na infância e adolescência no ambiente digital: caminhos para a proteção jurídica no Brasil e Argentina**. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2022/07/dados-e-direitos-na-infancia-e-adolescencia-no-ambiente-digital.pdf. Acesso em 14.08.2024.

ITS RIO. **Design Apropriado para a Idade: Código de Práticas para Serviços On-line**. Disponível em: https://itsrio.org/wp-content/uploads/2021/08/Design-Apropriado-para-a-Idade_-Codigo-de-Praticas-para-Servicos-Online.pdf. Acesso em 14.08.2024.

INTERNET LAB. **O direito das crianças à privacidade**. Disponível em: https://internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em 14.08.2024.

INSTITUTO ALANA; MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. **Comentário Geral N° 25 (2021) sobre os direitos das crianças em relação ao ambiente digital - Versão Comentada.2022**. Disponível em: https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf. Acesso em 14.08.2024.

MAUK, M. **Parenting and the algorithm: a perspective on parental Controls and guilt amidst digital media. In: Works in Progress • Algorithmic Rights and Protections for Children**, 2021.

5RIGHTSFOUNDATION. **Approaches to children's data protection A comparative international mapping**. Disponível em: Disponível em: https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf. Acesso em 14.08.2024.

FEDERAL TRADE COMMISSION - PROTECTING AMERICA´S CONSUMERS. **A Guide For Business and Parents And Small Entity Compliance Guide.** Disponível em: Disponível em: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions. Acesso em 14.08.2024.

AN COIMISIÚN UM CHOSAINT SONRAÍ - DATA PROTECTION COMMISSION. **Guidance for children on their data protection rights.** Disponível em: https://www.dataprotection.ie/en/dpc-guidance/childrens-data-protection-rights. Acesso em 14.08.2024.

ICO. **Consent**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/. Acesso em 14.08.2024.

ECOVIS PROVENTUSLAW**. European Data Protection Board adopts guidelines on consent under the GDPR**. Disponível em: https://ecovis.lt/european-data-protection-board-adopts-guidelines-on-consent-under-the-gdpr. Acesso em: 14.08.2024.

CONSUMER PROTECTION REVIEW. **CARU Issues Warning About Using AI in Child-Directed Advertising and Data Collection**. Disponível em:

https://www.consumerprotectionreview.com/2024/05/caru-issues-warning-about-using-ai-in-child-directed-advertising-and-data-collection/#more-2643. Acesso em: 14.08.2024.

ICO. **Protecting children's privacy online: Our Children's code strategy**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/. Acesso em: 14.08.2024.

BRASIL. Resolução CONANDA nº 245/2024, de 05 de abril de 2024. Disponível em: https://www.lex.com.br/resolucao-conanda-no-245-de-5-de-abril-de-2024/. Acesso em: 14.08.2024.

Tomada de Subsídios da ANPD: **Tratamento de Dados Pessoais de Crianças e Adolescentes**

A iniciativa da ANPD de realizar uma Tomada de Subsídios e abrir espaço para a participação de diversos setores da sociedade em um diálogo construtivo reflete a preocupação da Autoridade em criar um processo plural e participativo, essencial para embasar a Análise de Impacto Regulatório e a implementação de ações regulatórias subsequentes.

Nossa contribuição busca oferecer orientações práticas baseadas em consultas a especialistas e em princípios de *privacy by design* específicos para ambientes digitais voltados a crianças e adolescentes. Ao destacar considerações-chave e melhores práticas, esperamos contribuir para o desenvolvimento de instrumentos eficazes da ANPD.

A forma como as crianças acessam conteúdos *online* para se conectar e aprender tem evoluído significativamente, levantando questões importantes sobre como construir uma experiência para os jovens que seja segura e de qualidade. Os meios digitais são fundamentais para ajudar as crianças a prepararem-se para o futuro e é essencial que existam salvaguardas eficazes para que crianças e famílias sejam protegidas.

Os comentários aqui compartilhados foram extraídos de nosso arcabouço de políticas públicas para proteção de crianças e adolescentes online, de anos de experiência prática no desenvolvimento de produtos projetados especificamente para crianças, adolescentes e famílias, bem como de nosso trabalho para cumprir as normas internacionais de proteção de dados e requisitos de segurança.

A contribuição a seguir aborda como a ANPD pode proteger efetivamente os dados e a privacidade de crianças e adolescentes e apoiar seus melhores interesses, adotando uma abordagem proporcional e baseada em riscos; fomentar transparência significativa; facilitar o desenvolvimento de produtos e controles adequados à idade que se alinhem com os estágios e necessidades de desenvolvimento de crianças e adolescentes; proibir publicidade personalizada; garantir a viabilidade de conteúdos e experiências diversificados e de alta qualidade; abordar os requisitos de garantia de idade com consciência das vantagens e desvantagens; promover a responsabilização; e colocar as regulamentações

no contexto mais amplo de iniciativas como a educação para a alfabetização digital, que podem ajudar a alcançar os resultados desejados.

Princípios do YouTube

Ao longo dos anos, o YouTube, em parceria com especialistas e pesquisadores, desenvolveu políticas e produtos robustos para garantir a segurança e a adequação por faixa etária em sua plataforma. Acreditamos que esses princípios são relevantes para a atual Tomada de Subsídios da ANPD.

1. **Priorizar proteções especiais online para crianças e adolescentes.** As plataformas de internet devem colocar a segurança e a privacidade de crianças e adolescentes em primeiro lugar. Isso pode ser alcançado por meio de uma abordagem *"safety by design"*, onde as medidas de segurança não são apenas adicionadas posteriormente, mas incorporadas desde o início na própria concepção dos ambientes digitais.

2. **Empoderar os pais e responsáveis no gerenciamento das experiências online de suas famílias:** As plataformas devem fornecer aos pais e responsáveis maneiras de personalizar as experiências online que sejam melhores para suas famílias. Controles parentais, recursos e configurações apropriadas para diferentes faixas etárias são essenciais para equilibrar a supervisão com independência, garantindo ambientes digitais adequados à idade.

3. **Garantir acesso a conteúdo adequado por faixa etária.** Crianças e adolescentes merecem acesso a conteúdo gratuito e de alta qualidade alinhado aos seus estágios de desenvolvimento. As plataformas devem priorizar conteúdo educacional e inspirador em detrimento de publicidade direcionada, protegendo a privacidade dos jovens usuários ao mesmo tempo que promovem o crescimento e o aprendizado.

4. **Considerar as necessidades de desenvolvimento nas experiências online.** Reconhecendo as necessidades únicas de diferentes faixas etárias, as plataformas devem adaptar o conteúdo e os serviços conforme cada uma dessas etapas de crescimento. Ao entender a evolução do ambiente digital para crianças e adolescentes, as plataformas devem explorar mais opções de experiências adequadas à idade que apoiem seu desenvolvimento.

5. **Aliar tecnologias inovadoras a medidas de proteção.** Novas tecnologias têm o potencial de aprimorar as experiências online de crianças e adolescentes. As plataformas devem, portanto, avaliar cuidadosamente os riscos dessas inovações e seus benefícios

potenciais antes de implementá-las, de modo que a segurança e o bem-estar de crianças e adolescentes permaneçam como prioridades. Dessa forma, plataformas podem garantir que a inovação empodere os jovens usuários sem comprometer sua proteção.

Abordagem Proporcional Baseada em Risco

Regulamentações centradas nas crianças e adolescentes devem adotar uma abordagem proporcional e baseada no risco, exigindo que os riscos que advêm do tratamento de dados pessoais sejam avaliados e mitigados, combinando as proteções adequadas aos riscos. Isso significa evitar uma abordagem prescritiva e única que tente estabelecer proibições e obrigações gerais e/ou requisitos estritos de verificação da idade que podem prejudicar os direitos fundamentais das crianças, como a privacidade e o acesso à informação. Existem diferentes opções de proteção para crianças e adolescentes online e qualquer legislação que exija restrições ao tratamento de dados de adolescentes deve refletir as diferenças de maturidade, capacidade e riscos de danos entre crianças e adolescentes.

Além disso, tais regulamentações devem permitir que os serviços proporcionem experiências adequadas à idade, que equilibrem a proteção da privacidade e da segurança com a satisfação da necessidade dos adolescentes de acesso a ferramentas digitais para ajudá-los a aprender e a desenvolver competências sociais, a competir no mercado global economia e conectar-se com amigos e familiares.

Transparência

A legislação deve ter o objetivo de garantir uma transparência significativa para crianças, adolescentes e suas famílias. Isto pode ser alcançado por meio da implementação de uma abordagem baseada em princípios, que tenha em conta a natureza e a sensibilidade dos dados pessoais e incentive soluções novas e inovadoras. Em vez de estabelecer requisitos prescritivos, a legislação poderia exigir que os serviços online fornecessem recursos e ferramentas de transparência que funcionassem para o público mais vasto possível. Isto exigiria que os provedores garantissem textos redigidos em linguagem tão clara e simples quanto possível e que fossem utilizados recursos de comunicação acessíveis.

Controles e recursos adequados à idade

Os serviços online devem oferecer uma gama de configurações de preservação da privacidade que ajudem os pais a atender às necessidades e preferências únicas da sua família. Para crianças com idade inferior à idade de consentimento, estas configurações e ferramentas devem proporcionar aos pais uma capacidade significativa de compreender e controlar a experiência dos seus filhos. Quando apropriado, para crianças menores de idade de consentimento, os serviços online devem ser obrigados a oferecer configurações e ferramentas que incluam opções para os pais ou responsáveis gerenciarem o conteúdo e as configurações da conta, limitarem o tempo de uso e aplicarem proteções de privacidade adicionais.

Para usuários com menos de 18 anos e acima da idade de consentimento, que têm maior maturidade e autonomia, é importante que haja funcionalidades e políticas adicionais, incluindo que os adolescentes fiquem cientes quando estão sendo monitorados, por exemplo por meio de um aviso claro quando o rastreamento preciso de geolocalização está ativado. Esta abordagem respeita os direitos fundamentais dos adolescentes e ajuda-os a tomar decisões informadas sobre a sua presença online e privacidade digital, o que lhes será útil à medida que crescem até à idade adulta.

Princípio do Melhor Interesse

O melhor interesse das crianças e adolescentes deve ser a principal consideração em todas as decisões relacionadas aos seus dados pessoais. Este princípio oferece uma base sólida de proteção online aos jovens usuários.

O Google e o YouTube estão comprometidos em criar plataformas seguras e enriquecedoras para crianças e adolescentes, e nossos esforços para desenvolver conteúdo e recursos apropriados para essas idades estão alinhados com esse princípio.

Especialistas em desenvolvimento infantil concordam que o "melhor interesse" deve ser considerado de forma holística, incluindo fatores como segurança, bem-estar físico e mental, privacidade, autonomia, acesso à informação e liberdade de participação na sociedade. Portanto, no tratamento de dados, este princípio deve ser equilibrado com os outros princípios estabelecidos na LGPD. Há também um consenso de que esses interesses devem ser definidos em alinhamento com a Convenção das Nações Unidas sobre os Direitos da Criança (Artigo 3) e com as melhores práticas globais.

Para implementar efetivamente o princípio do melhor interesse, os serviços online devem adotar uma abordagem centrada na criança. Isso inclui considerar os interesses coletivos das crianças em estágios de desenvolvimento semelhantes, bem como basear-se em pesquisas especializadas e melhores práticas para criar produtos e serviços adequados à cada faixa etária.

Respeito à Autonomia Progressiva e Experiências Adequadas às faixas etárias

O princípio do melhor interesse deve ser equilibrado com a autonomia progressiva de crianças e adolescentes.

A ANPD deve considerar os diferentes tipos de proteção online para crianças e adolescentes em suas futuras regulamentações e ações de fiscalização. As proteções específicas para adolescentes devem refletir sua crescente maturidade, garantindo que essas medidas não limitem desnecessariamente seu acesso aos benefícios no ambiente digital. Essa abordagem reconhece os diferentes estágios de

desenvolvimento e necessidades de crianças e adolescentes, visando proteções mais eficazes e adequadas.

As experiências com produtos e conteúdos devem ser adaptadas às necessidades e interesses de crianças e adolescentes para fomentar a criatividade, a auto expressão, o desenvolvimento de habilidades essenciais e a exploração de interesses e paixões. Adolescentes, com maior capacidade de desenvolvimento e autonomia, devem ter acesso a informações como parte de sua jornada de aprendizado. A interação com a tecnologia varia significativamente entre uma criança do ensino fundamental e um adolescente, o que indica que os requisitos de consentimento para um jovem de 15 anos não devem ser os mesmos que para uma criança de 7 anos.

É possível, seguindo o princípio do melhor interesse, considerar a autonomia progressiva dos adolescentes para fornecer consentimento para o tratamento de seus dados pessoais em contextos específicos sem a assistência de pais ou responsáveis legais. Exigir o consentimento dos pais para que adolescentes acessem serviços online em todos os casos pode levar à exclusão, a menos que os pais tomem medidas proativas, restringindo seu acesso a serviços valiosos e informações adequadas à idade, essenciais para o aprendizado, engajamento cívico e manutenção de conexões sociais.

Portanto, recomendamos a adoção de métodos mais flexíveis e inclusivos que garantam experiências seguras e adequadas para crianças e adolescentes de todas as idades, permitindo que regulamentações sobre o tratamento de dados pessoais e a presença online protejam crianças e adolescentes *na* internet, e não *da* internet.

Opções de Controle Parental Que Respeitem as Habilidades e Autonomia dos Adolescentes

Pais e responsáveis desempenham um papel crucial na definição de regras para as experiências online de suas famílias, especialmente para crianças mais novas. Desta maneira, para permitir que pais e responsáveis usem ferramentas e recursos apropriados, o Google e o YouTube fornecem ferramentas que os ajudam a gerenciar com confiança as experiências de seus filhos na plataforma.

Para atingir este compromisso, implementamos mudanças em nossos produtos com cuidado, envolvendo pais e especialistas em cada etapa do processo de desenvolvimento.

Embora necessários, os controles parentais devem respeitar determinados limites. Por exemplo, os controles parentais devem ser transparentes, deixando claro para crianças e adolescentes quando estão sendo monitorados, e devem evitar rastreamento desnecessário ou geolocalização precisa sem aviso claro. Uma linguagem clara é essencial para que os jovens usuários e seus responsáveis compreendam e exerçam seus direitos de privacidade, evitando designs manipulativos que coletem dados excessivos ou comprometam a privacidade.

Além disso, os serviços online devem oferecer configurações que preservem a privacidade e respeitem a autonomia progressiva dos adolescentes. Para as crianças, os controles devem permitir que os pais gerenciem o conteúdo, o tempo de tela e as configurações de privacidade. Esses mesmos controles podem não ser adequados para adolescentes que estão acima da idade de consentimento e são mais capazes de entender e escolher as configurações que são melhores para eles.

Em vez de usar configurações padrão rígidas, as plataformas devem dar aos usuários mais controle e informações sobre a personalização de conteúdo. Isso atende melhor às necessidades individuais e evita soluções que não consideram as diferenças de idade e capacidade.

Melhores Práticas do YouTube/Google Adotadas para Controle Parental

Uma das perguntas na Tomada de Subsídios diz respeito a quais mecanismos e melhores práticas podem ser adotados para expandir o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital.

O YouTube oferece aos pais uma variedade de controles que lhes permitem decidir o que suas famílias fazem e veem online por meio do YouTube Kids e experiências supervisionadas. Em uma atualização que será lançada ainda este ano, pais e adolescentes poderão vincular suas contas, permitindo que os pais tenham visibilidade sobre as atividades de seus adolescentes no YouTube.

Além disso, sabemos que os pais, com agendas ocupadas, podem achar desafiador gerenciar os controles para seus filhos online. Por isso, desenvolvemos uma solução abrangente e fácil de usar: o Family Link. Com ele, os pais podem:

- Definir limites de tempo de tela e horário de dormir para crianças e seus dispositivos: Isso inclui um novo recurso chamado "Somente Hoje" – para aqueles momentos temporários em que você pode querer permitir mais ou menos tempo online (como durante uma viagem de carro).
- Organizar listas de reprodução no YouTube, YouTube Kids: As listas de reprodução gerenciadas pelos pais permitem que eles criem uma lista de "deve assistir" para as crianças. Basta clicar no filme ou programa, clicar na lista de reprodução e selecionar a lista do perfil da criança.
- Gerenciar os aplicativos com os quais as crianças podem interagir: Com apenas alguns cliques, os pais podem bloquear ou aprovar o uso de aplicativos e sites específicos, definir limites de tela, bloquear automaticamente a tela da criança na hora de dormir, filtrar quais aplicativos são mostrados na loja de aplicativos com base na classificação etária e muito mais.

- Compartilhamento de localização: Na guia Localização, o pai ou responsável pode ver todos os filhos no mesmo mapa com a localização de seus dispositivos. Ele também pode ativar notificações para ser alertado quando seu filho chegar ou sair de um destino específico, como a escola ou a aula de futebol.

Recomendações Personalizadas

Nosso sistema de recomendações desempenha um papel importante em como mantemos uma plataforma responsável e enriquecedora para os usuários mais jovens. Ele ajuda a conectá-los a conteúdos de alta qualidade - baseados em princípios de qualidade desenvolvidos em colaboração com especialistas independentes em desenvolvimento infantil e bem-estar digital - que inspiram curiosidade, imaginação e criatividade. Também minimiza as chances de verem conteúdos de baixa qualidade.

Ao mesmo tempo, o YouTube oferece e continuará oferecendo aos usuários uma gama de ferramentas para otimizar sua experiência na plataforma e decidir quais informações pessoais são usadas para influenciar as recomendações. Por exemplo, usuários logados podem limpar seu histórico de buscas e exibição, remover entradas individuais de busca das sugestões de pesquisa ou pausar o histórico de buscas usando as configurações de histórico do YouTube. Finalmente, os controles na plataforma permitem que os usuários removam conteúdo recomendado de suas páginas iniciais e o próximo vídeo a ser assistido.

Uso de dados pessoais para garantir a segurança e proteção de Crianças e Adolescentes

Informações precisas sobre a idade do usuário permitem que as plataformas forneçam conteúdo e serviços adequados, ao mesmo tempo em que ativam recursos de segurança personalizados, reforçando a segurança online. No entanto, qualquer método para determinar a idade dos usuários apresenta desvantagens, como a intromissão na privacidade, a exigência de maior utilização de dados ou a restrição do acesso de usuários adultos a informações e serviços importantes. Sempre que necessário, essa determinação deve basear-se no risco, preservando-se o acesso do usuário à informação e aos serviços e respeitando a sua privacidade.

Para equilibrar privacidade e segurança, alguns passos e princípios devem ser observados:

- **Foco na minimização de dados:** Coletar apenas os dados essenciais para a determinação da idade, com limitação de finalidade.
- **Empregar verificação em camadas (abordagem baseada em risco):** Implementar métodos menos intrusivos para conteúdo de baixo risco e reservar verificações mais rigorosas para serviços de alto risco, como jogos de azar ou conteúdo adulto. Métodos

mais invasivos, como a verificação com documentos físicos, devem ser limitados a serviços de alto risco ou correção de idade.

- **Incentivar o avanço tecnológico:** Apoiar a inovação em métodos de verificação de idade que aprimorem a privacidade e a experiência do usuário.
- **Fornecer salvaguardas legais:** Proteger os serviços online contra responsabilidades excessivas, incentivando o desenvolvimento e a implementação de soluções de verificação de idade. À medida que as tecnologias de verificação de idade evoluem, os requisitos devem oferecer uma proteção equilibrada contra riscos legais indevidos, permitindo que os serviços inovem e melhorem suas soluções de forma eficaz.

Exigir verificação na criação de contas ou para atividades de menor risco prejudicaria experiências anônimas e poderia dificultar o acesso à informação, especialmente para comunidades vulneráveis que provavelmente serão afetadas de forma desproporcional (por exemplo, pessoas que desejam acessar informações sobre um determinado diagnóstico anonimamente por receio do estigma social)

Publicidade Personalizada

Conteúdo diversificado e de alta qualidade ajuda crianças e adolescentes a aprender, expandir seus interesses e encontrar uma comunidade. A publicidade, quando feita de forma responsável, suporta o custo de criação desse conteúdo, garantindo que esteja disponível para crianças, adolescentes e famílias, bem como para os criadores e para a economia em geral. A manutenção de uma Internet vibrante e apoiada por anúncios permite conteúdos e serviços gratuitos e proporciona uma alternativa de receitas aos modelos por assinatura ou serviços gratuitos limitados.

A publicidade contextual permite que os criadores forneçam às crianças acesso a conteúdo gratuito, incluindo conteúdo educacional ao qual, de outra forma, elas não teriam acesso. Para concretizar estes benefícios, a legislação deve permitir a publicidade contextual que se baseie em sinais como o conteúdo visualizado no momento, a consulta de pesquisa atual, a localização geográfica geral e a hora do dia. A legislação também deve permitir a utilização de dados para veicular e medir publicidade. Outras formas de publicidade que dependem de tratamento adicional de dados, como anúncios personalizados com base na idade, sexo e interesses, podem não ser tão adequadas para indivíduos mais jovens e devem ser proibidas.

Apoiamos também a proibição da troca de informações pessoais de crianças e adolescentes por contrapartida monetária a terceiros, incluindo *data brokers*. Estas proibições limitariam o tratamento de dados pessoais de crianças e adolescentes, reduzindo o potencial de usos prejudiciais, ao mesmo tempo que apoiariam conteúdos gratuitos ou com custos reduzidos para todos os usuários.

Parcerias com Especialistas

Para criar experiências digitais seguras e envolventes para crianças e adolescentes, colaboramos com educadores, especialistas em desenvolvimento infantil, pais, reguladores e ONGs. Essa abordagem orienta o desenvolvimento de produtos personalizados de qualidade que estejam alinhados com as necessidades, interesses e literacia digital de nossos jovens usuários.

Para promover a referida colaboração, o YouTube estabeleceu um Comitê Consultivo em 2018, composto por especialistas independentes em mídia, desenvolvimento infantil, aprendizado digital e cidadania, com diversas experiências clínicas e acadêmicas diversas. Este Comitê aconselha o YouTube sobre as necessidades em evolução dos jovens, aproveitando pesquisas bem fundamentadas e sua própria expertise. Além disso, o Comitê avalia os produtos, as políticas e os serviços que oferecemos a jovens e famílias.

No Brasil, um dos membros do Comitê é Thiago Tavares, fundador e presidente da SaferNet, organização brasileira dedicada à promoção da segurança na internet, com uma história que abrange mais de 18 anos[1].

Harmonização e Interoperabilidade

Reconhecemos as complexidades envolvidas na regulamentação do tratamento de dados pessoais de crianças e adolescentes. As famílias merecem regulamentações claras e consistentes que abordem essas complexidades de forma eficaz. Alinhando-se ao consenso global sobre proteções robustas para jovens usuários, essas salvaguardas também devem garantir o acesso contínuo a serviços que apoiam seu aprendizado e desenvolvimento. A ANPD deve priorizar a consistência e a interoperabilidade regulatória para refletir a natureza global da internet. Essa abordagem aumentará a clareza e a certeza para os usuários, serviços online e formuladores de políticas públicas, levando a experiências mais coesas , previsíveis e juridicamente seguras no ambiente digital.

[1] A SaferNet é a primeira ONG brasileira a implementar uma abordagem multissetorial para proteger crianças e promover os direitos humanos no ambiente digital. Desde 2005, a SaferNet gerencia a linha direta nacional para denúncias de crimes cibernéticos, uma linha de apoio à segurança na internet e o centro brasileiro de conscientização em cidadania digital. Nos últimos 15 anos, Thiago trabalhou extensivamente em segurança infantil, segurança digital e governança da internet, e ministrou palestras em mais de 30 países, incluindo nove edições do Fórum de Governança da Internet (IGF) da ONU.

Zetta

Contribuições para a Tomada de subsídios da ANPD para projeto regulatório sobre crianças e adolescentes

São Paulo, 16 de agosto de 2024.

A Zetta, associação sem fins lucrativos que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, vem, por meio desta manifestação, apresentar contribuições para a tomada de subsídios da Autoridade Nacional de Proteção de Dados ("ANPD") para a elaboração de projeto regulatório sobre crianças e adolescentes, publicada em 18 de junho de 2024.

Em virtude do impacto que as futuras orientações e regulamentações da ANPD podem trazer para a continuidade e o futuro do modelo de negócio de suas empresas e até mesmo para o Sistema Financeiro Nacional, a Zetta apresenta abaixo algumas contribuições para o estudo preliminar.

I - Princípio do melhor interesse
De acordo com o art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Na mesma linha, segundo o Enunciado CD/ANPD nº 01/2022, o tratamento de dados pessoais desses titulares pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse. Por sua vez, o Guia Orientativo sobre a hipótese legal do legítimo interesse menciona que o conceito de melhor interesse abrange três aspectos: um direito, um princípio interpretativo e uma regra processual. Esta definição segue o disposto na Convenção Internacional dos Direitos da Criança,[1] no Comentário Geral nº 14, de 2013, do Comitê dos Direitos da Criança da ONU[2] e no Comentário Geral nº 25, de 2021, do Comitê dos Direitos da Criança.[3] Ainda segundo o Guia, o controlador deve levar em consideração, de forma prioritária, o melhor interesse da criança e do adolescente e adotar a interpretação que atenda a esse interesse de forma mais eficaz. Como se pode observar, o princípio do melhor interesse desempenha um papel central em qualquer tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, questiona-se:
1. Além dos aspectos abordados no Enunciado CD/ANPD nº 01/2022 e no Guia Orientativo sobre a hipótese legal do legítimo interesse, quais questões relacionadas ao princípio do melhor interesse demandam orientação ou regulamentação específicas pela ANPD?
R.: Entendemos que o próprio termo "melhor interesse do menor" requer maior detalhamento por parte da ANPD, a começar pela sua própria definição. Para tanto, consideramos fundamental que a definição de "melhor interesse do menor":

i. seja analisada de forma casuística, tendo em vista o contexto específico no qual ocorrerá o tratamento de dados dos menores;
ii. considere as características específicas do menor cujos dados serão tratados; e
iii. seja equilibrada com outros direitos desses menores.

Exemplo 1: Processos que visam garantir a segurança do menor contra fraudes financeiras, como através de mecanismos de autenticação de identidade, também devem ser contemplados no que se entende por melhor interesse do menor.

Exemplo 2: Contemplar no melhor interesse do menor o envio de comunicações distintas aos menores sobre o tratamento dos seus dados no contexto de abertura de uma conta corrente. Isso porque podemos ter, de um lado, uma criança de 5 anos (que tem suas capacidades e autonomia de certa forma limitadas, para a qual pode ser recomendada uma política de privacidade mais lúdica e acessível), e, de outro, de um adolescente de 16 anos (que já conta com maior independência e gerência sobre os seus atos).

De maneira similar, fazemos referência ao seguinte trecho do Guia Orientativo sobre Legítimo Interesse da ANPD:

> *"A documentação referente ao tratamento poderá, ainda, conter a análise efetuada pelo controlador, em especial o teste de balanceamento, incluindo a indicação sobre a natureza dos dados pessoais tratados, a demonstração da legitimidade do interesse do controlador ou de terceiro, a sua ponderação com os direitos dos titulares e a compatibilidade com as suas legítimas expectativas, e se tratando de dados pessoais de criança ou adolescentes, as evidências da observância e prevalência do seu melhor interesse."*

Com base no trecho acima, ressaltamos também a importância de diferenciar as etapas e requisitos de análise do melhor interesse do menor vs. a análise da base legal do legítimo interesse para tratamento de dados de menores.

2. Existem situações ou contextos específicos de tratamento de dados pessoais de crianças e adolescentes que demandam maior atenção e detalhamento sobre o princípio do melhor interesse? Em caso afirmativo, indicar quais situações ou contextos identificados e as principais questões a serem abordadas.

R.: Sim.

Destacamos casos de publicidade (incluindo publicidade personalizada) que podem fomentar comportamentos positivos em prol do melhor interesse do menor. Embora o envio de publicidade para menores seja visto como negativo por determinados stakeholders, existem casos em que esse envio pode contribuir para atividades que estejam em harmonia com o melhor interesse de crianças e adolescentes. É o caso, por exemplo, do envio de e-mail marketing para menores referente a serviço de investimento voltado a fomentar a educação financeira desse público alvo.

Também ressaltamos os casos de tratamento de dados de menores para fins de desenvolvimento de modelos de riscos relacionados à necessidade de cumprimento de obrigações legais e regulatórias (como AML e fraude).

Outro exemplo importante diz respeito à sobreposição do melhor interesse do menor em relação ao interesse dos próprios pais e responsáveis legais. É o caso, por exemplo, da coleta de dados adicionais de menores a fim de evitar a criação de contas laranjas criadas por responsáveis legais mal intencionados.

II - Consentimento

O consentimento pressupõe uma manifestação livre, informada e inequívoca do titular, por meio da qual este concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Quando utilizada esta hipótese legal, cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na LGPD (art. 8º, § 2º).

Além das regras gerais aplicáveis a qualquer tratamento de dados pessoais, a utilização da hipótese legal do consentimento como amparo para o tratamento de dados pessoais de crianças e adolescentes demanda a observância de cautelas e regras específicas, impondo uma série de desafios adicionais para os controladores.

Nesse sentido, o art. 14, § 1º, da LGPD, estabelece que, no caso de tratamento de dados pessoais de crianças, o consentimento "específico e em destaque" deve ser fornecido por um dos pais ou pelo responsável legal. Para tanto, conforme o § 5º do mesmo artigo, os controladores devem realizar "todos os esforços razoáveis" para verificar que o consentimento foi fornecido pelos pais ou responsáveis legais, "consideradas as tecnologias disponíveis".

Diante do que estabelecem essas disposições normativas, questiona-se:

1. Quais critérios ou parâmetros devem ser observados para a obtenção do consentimento "específico e em destaque" de pais ou responsáveis legais?

R.: Inicialmente, destacamos o entendimento já firmado pelo Enunciado nº 1/2022 da ANPD, conforme o qual foi estabelecido que o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base em qualquer uma das hipóteses de tratamento previstas na LGPD, desde que observado e prevalecente o seu melhor interesse. Além disso, ressaltamos que a LGPD não estabelece qualquer hierarquia entre as hipóteses de tratamento de dados pessoais nela previstas. Por essa razão, e em observância ao tema desta Seção, reafirmamos que o consentimento não necessariamente é a base legal mais adequada, tampouco a única aplicável, para o tratamento de dados pessoais de menores no ordenamento jurídico nacional.

Passando à análise dos critérios para obtenção do consentimento específico e em destaque (conforme previsto pelo art. 14, § 1º da LGPD), seria importante que a ANPD estabelecesse critérios que contemplem aspectos como (i) o uso de linguagem acessível para indicar quais os dados pessoais tratados e qual a finalidade do seu uso, bem como que o menor precisará do consentimento parental para ter os seus dados tratados; (ii) o uso de aspectos visuais que facilitem a obtenção desse consentimento em destaque.

Exemplo: uso de checkbox específico para a coleta do consentimento parental durante o fluxo de onboarding do menor.

2. Considerando as boas práticas, as tecnologias disponíveis e os princípios da LGPD, em especial os princípios da finalidade, da necessidade e da adequação, bem como a exigência legal de adoção de "todos os esforços razoáveis", quais medidas e mecanismos os controladores devem adotar, em especial no ambiente digital, para viabilizar e verificar que o consentimento foi fornecido pelos pais ou responsáveis da criança?

R.: Antes mesmo de definir quais as medidas e mecanismos a serem adotados pelos controladores para verificar que o consentimento para o tratamento de dados de menores foi fornecido pelos seus pais ou responsáveis legais, entendemos que critérios como tecnologia disponível, porte do controlador e criticidade decorrente do tratamento dos dados dos menores devem ser levados em consideração para avaliação da legitimidade desse consentimento. Isso porque a adoção de algumas dessas medidas pode implicar na necessidade de implementação de processos e custos adicionais, que não necessariamente se alinham ao porte da empresa e mesmo ao risco trazido pelo tratamento em pauta.

Para fins ilustrativos, apresentamos algumas das medidas passíveis de serem aplicadas a fim de verificar se o consentimento foi de fato fornecido pelos pais ou representantes legais dos menores: (i) envio de e-mail para os pais/responsáveis legais a fim de confirmar o consentimento supostamente fornecido por eles no app para a criação da conta do menor; (ii) solicitar documento aos pais/responsáveis legais após fornecerem o consentimento para o tratamento do menor, a fim de confirmar a sua identidade.

3. No caso de adolescentes, a obtenção do consentimento, em especial no ambiente digital, deve observar as disposições do direito civil a respeito das capacidades civis, seguindo a regra geral de representação e de assistência de pais ou responsáveis? Ou é possível considerar, em consonância com o princípio do melhor interesse, a autonomia progressiva desses titulares para, em determinados contextos e situações, fornecer consentimento ao tratamento de seus dados pessoais sem a necessidade de representação ou assistência de pais e responsáveis legais?

R.: A obtenção do consentimento de adolescentes deve seguir o ordenamento jurídico estabelecido pelo Código Civil, levando em conta a autonomia progressiva desses titulares. Dessa forma, é possível reconhecer a capacidade evolutiva desses menores, e ao mesmo tempo proteger os seus dados pessoais, e assim assegurar o melhor interesse dos adolescentes.

III - Jogos e aplicações de internet

Os jogos digitais e as aplicações de internet, incluindo as redes sociais, são ambientes em que, sem as devidas salvaguardas, podem ocorrer a coleta excessiva e a divulgação desnecessária de dados pessoais de crianças e adolescentes. Tal situação se agrava ao se considerar a crescente participação de crianças e adolescentes no ambiente digital,

bem como o fato de que parte dessas plataformas digitais não foram especificamente projetadas para este público. De forma diversa, determinadas plataformas digitais foram projetadas para incentivar o seu uso constante e a superexposição de usuários, permitindo a coleta massiva de seus dados pessoais e expondo-os à vigilância de seu comportamento.

Diante desse cenário, é fundamental estabelecer princípios, parâmetros e salvaguardas adequadas para que o tratamento de dados pessoais de crianças e adolescentes no ambiente digital seja realizado em consonância com o seu melhor interesse, de modo a afastar ou mitigar os riscos que decorrem dessas operações.

Nesse contexto, destacam-se os princípios da finalidade, da necessidade e da adequação (art. 6º, I, II e III, LGPD), os quais, em conjunto, limitam o tratamento de dados pessoais ao mínimo necessário para a realização de finalidades específicas, legítimas e informadas aos titulares, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. De forma mais específica, o art. 14, § 4º, da LGPD, veda que o fornecimento de informações pessoais seja imposto como uma condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas aquelas informações "estritamente necessárias à atividade".

Merece destaque, ainda, o princípio da transparência (art. 6º, VI, LGPD), segundo o qual o controlador deve fornecer informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. O art. 14, § 6º, da LGPD, estabelece regra específica a ser observada no tratamento de dados pessoais de crianças e adolescentes. Assim, as medidas de transparência devem considerar "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Também é relevante para a proteção de dados pessoais de crianças e de adolescentes no ambiente digital a adoção de princípios normativos, tecnologias e medidas de design, que promovam e assegurem níveis elevados de privacidade e proteção de dados pessoais. A esse respeito, destacam-se questões como: (i) a definição e a implementação de boas práticas e de padrões técnicos que priorizem a garantia do melhor interesse e a privacidade como padrão; (ii) as técnicas adequadas para a verificação de idade de usuários; (iii) as limitações a serem observadas na coleta de dados pessoais de crianças e adolescentes, em especial para a formação de perfis comportamentais; e (iv) os mecanismos para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes.

Nesse sentido, considerando as disposições da LGPD e a experiência internacional em torno do tema, questiona-se:

1. Quais princípios, parâmetros e salvaguardas, incluindo medidas de design, devem ser observados no tratamento de dados pessoais de crianças e adolescentes por plataformas digitais, de modo a assegurar o respeito ao seu melhor interesse, promover e assegurar níveis elevados de privacidade e proteção de dados pessoais e mitigar os riscos decorrentes do uso dessas plataformas?

R.: Destacamos como recomendação a adoção de experiências com diferentes funcionalidades para diferentes faixas etárias, a fim de mitigar riscos específicos para os menores, como compras excessivas e divulgação de conteúdo inadequado.

Esse tipo de medida está em linha com o California Age-Appropriate Design Code Act, que determina que:

> *"as empresas devem levar em conta as necessidades únicas das diferentes faixas etárias, incluindo os seguintes estágios de desenvolvimento: 0 a 5 anos de idade ou 'pré-alfabetização e alfabetização inicial'; 6 a 9 anos de idade ou 'anos fundamentais do ensino primário'; 10 a 12 anos de idade ou 'anos de transição'; 13 a 15 anos de idade ou 'início da adolescência'; e 16 a 17 anos de idade ou 'aproximando-se da idade adulta'".*

Vale ressaltar que a adoção dos princípios de tratamento de dados trazidos pela LGPD já apresenta uma proteção robusta aos dados pessoais dos menores e ao seu melhor interesse, razão pela qual devem ser respeitados no desenvolvimento de medidas que visem mitigar os riscos decorrentes do tratamento de dados pessoais no contexto de uso de plataformas digitais.

2. Considerando que o tratamento de dados pessoais deve se ater àqueles estritamente necessários à finalidade a que se destina, quais são as boas práticas e as técnicas disponíveis e adequadas para verificação de idade de usuários de plataformas digitais?

R.: Para fins de verificação de idade do menor, idealmente devem ser utilizados fluxos que contemplem tanto o melhor interesse do menor, no sentido de assegurar a sua real idade, quanto a proteção dos seus dados pessoais. Um exemplo é a verificação de dados pessoais de menores junto a fontes oficiais (sejam públicas ou particulares) para confirmar a idade indicada pelo menor.

Destacamos que os critérios que apresentamos na seção referente à verificação do consentimento parental também devem se aplicar para fins de verificação etária, quais sejam: tecnologia disponível, porte do controlador, e criticidade decorrente do tratamento dos dados dos menores.

3. Quais limitações específicas devem ser observadas na coleta de dados pessoais de crianças e adolescentes por plataformas digitais, considerando o disposto no art. 14, § 4º, da LGPD e, entre outros aspectos, a natureza dos dados coletados e a finalidade do tratamento, a exemplo da formação de perfis comportamentais?

R.: A adoção dos princípios de tratamento de dados pessoais previstos na LGPD são capazes de indicar as limitações a serem observadas pelas plataformas digitais na coleta de dados pessoais de menores. Por exemplo: quando uma determinada plataforma induz um menor a oferecer dados pessoais para obter acesso a determinadas ferramentas, temos uma atividade que contraria, por exemplo, o princípio da necessidade.

Em relação à formação de perfis comportamentais, consideramos que nem sempre

representam algo prejudicial ao melhor interesse do menor. É o caso, por exemplo, da criação de perfis comportamentais de menores por determinada instituição financeira, a fim de avaliar os seus comportamentos para fins de prevenção à fraude.

4. Quais mecanismos e boas práticas podem ser adotados para ampliar o controle de pais e responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes no ambiente digital?

R.: Conforme mencionamos nas seções anteriores, nem sempre o controle de pais e responsáveis legais sobre o tratamento dos dados pessoais dos menores sob sua responsabilidade vai ao encontro do melhor interesse do menor. Justamente por essa razão, entendemos que essas medidas de controle devem ser proporcionais às capacidades e necessidades das faixas etárias dos menores, diminuindo gradativamente em relação ao aumento da sua idade.

- De todo modo, algumas medidas passíveis de serem aplicáveis enquanto boas práticas são: (i) envio de notificações aos pais ou responsáveis legais para informá-los sobre a realização de transações financeiras das crianças sob a sua responsabilidade; (ii) criação de dashboard de privacidade na qual os pais ou responsáveis legais podem selecionar os controles sobre o tratamento de dados pessoais dos menores sob a sua responsabilidade, mantendo os controles acionados por padrão.

5. Quais as boas práticas relacionadas à transparência e ao fornecimento de informações de maneira simples, clara e acessível podem ser observadas por plataformas digitais quanto ao tratamento de dados pessoais de crianças e adolescentes?

R.: É recomendável a adoção de mecanismos que (i) transmitam informações sobre o tratamento de dados de forma adequada ao público (como vídeos, gamificação etc); e (ii) sejam capazes de atrair a sua atenção e consolidar a absorção das informações que lhe são apresentadas (como materiais lúdicos e ilustrados). Um exemplo recente e bastante divulgado no mercado é a Política de Privacidade da Lego, apresentada em seu site no formato de vídeo curto, instrutivo e ilustrado com brinquedos da própria marca, a fim de aproximar o seu conteúdo do seu público-alvo e facilitar a sua absorção.

6. Há outras questões relacionadas ao tratamento de dados pessoais de crianças e adolescentes que merecem esclarecimentos ou regulamentação adicional?

R.: Aproveitamos para ressaltar a necessidade de consolidação, por parte da ANPD, do entendimento apresentado no seu Enunciado nº 1/2022, no sentido de que o tratamento de dados pessoais de menores pode ser justificado por qualquer uma das bases legais da LGPD, bem como da ausência de hierarquia entre as bases legais trazidas pela LGPD. Isso trará um ambiente de maior segurança jurídica para o tratamento de dados de crianças e adolescentes, criando assim a possibilidade de mais espaço para o desenvolvimento de iniciativas inovadoras e efetivas para viabilizar o tratamento desses dados em prol do melhor interesse dos seus titulares. Por exemplo: é possível que uma iniciativa de coleta de dados de menores para fins de combate à fraude e baseada no consentimento não seja tão eficaz pelo fato de os menores terem a possibilidade de revogar esse consentimento, o que reforça o argumento já defendido de que o consentimento não

necessariamente é a base legal mais adequada para o tratamento de dados de crianças e adolescentes.

Também seria interessante que a ANPD, por meio de guias orientativos, apresentasse exemplos de medidas que considera como recomendáveis para um adequado tratamento de dados de menores em consonância com o seu melhor interesse, especialmente aquelas endereçadas a temas como consentimento parental, verificação de idade, medidas de transparência e autonomia progressiva do menor.

Do compromisso da Zetta com a proteção integral de crianças e adolescentes

A Zetta reconhece a proteção integral e o melhor interesse como princípios jurídicos fundamentais a nortearem todas as atividades de tratamento de dados pessoais de crianças e adolescentes por parte de suas associadas. Neste sentido, relembramos a Convenção sobre Direitos das Crianças, adotada em 1990 pela Organização das Nações Unidas, ratificada pelo Brasil e por mais 195 países, que dispõe que todas as ações relativas às crianças devem considerar primordialmente o seu melhor interesse. Ressaltamos, ainda, a centralidade do art. 227 da Constituição Federal que preconiza o princípio da proteção integral de crianças e adolescentes, atribuindo à família, à sociedade e ao Estado assegurar a essas pessoas com absoluta prioridade direitos e garantias fundamentais. E, por fim, a existência do Estatuto da Criança e do Adolescente, que, igualmente, faz menção ao princípio da proteção integral em seus artigos 1º e 3º.

***