



Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização
Coordenação de Normatização 2

Nota Técnica nº 216/2024/CON2/CGN/ANPD

INTERESSADO: COORDENAÇÃO-GERAL DE NORMATIZAÇÃO

Assunto: Consolidação das contribuições da Tomada de Subsídios referente ao tratamento de dados pessoais de crianças e adolescentes.

1. RELATÓRIO

1.1. Trata-se do projeto que visa à Regulamentação do Item 4 da Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) para o biênio 2025-2026, aprovada pela Resolução nº 23, de 09 de dezembro de 2024 (SEI/ANPD nº 0160131) - Tratamento de dados pessoais de crianças e adolescentes.

1.2. Segundo a Agenda Regulatória, o *objetivo desta ação regulatória é estabelecer procedimentos e orientações com vistas à garantia de direitos e à proteção de dados pessoais de crianças e adolescentes, especialmente no ambiente digital. Conforme abordado na Tomada de Subsídios realizada entre junho e agosto de 2024, integram o escopo do projeto os seguintes temas: (i) o princípio do melhor interesse; (ii) o consentimento fornecido por pais e responsáveis; (iii) a coleta de informações por jogos e aplicações de internet; (iv) a transparência das operações realizadas com dados pessoais de crianças e adolescentes; (v) os mecanismos de aferição de idade de usuários de jogos e aplicações de internet; e (vi) a definição de orientações e a identificação de boas práticas, que expressem um conjunto de princípios normativos, tecnologias e medidas de design, que promovam e assegurem a privacidade e a efetiva proteção de dados pessoais de crianças e adolescentes em jogos e aplicações de internet.*

1.3. Nesse sentido, conforme Termo de Abertura de Projeto (TAP) (SEI/ANPD nº 0051390), o projeto tem por escopo a identificação do problema regulatório e a análise do impacto regulatório sobre o tratamento de dados pessoais de crianças e adolescentes, previsto no art. 14 da LGPD.

1.4. Reconhecendo que a consulta e o envolvimento dos diversos segmentos da sociedade, incluindo organizações, cidadãos e especialistas, nos temas sob regulamentação proporciona uma visão mais ampla, alinhada com os princípios de participação social na atividade regulatória para o

levantamento de informações e evidências, inclusive de padrões de boas práticas regulatórias internacionais, foi proposto a tomada de subsídios, por meio da Nota Técnica nº 210/2024/CON2/CGN/ANPD (SEI/ANPD nº 0126932).

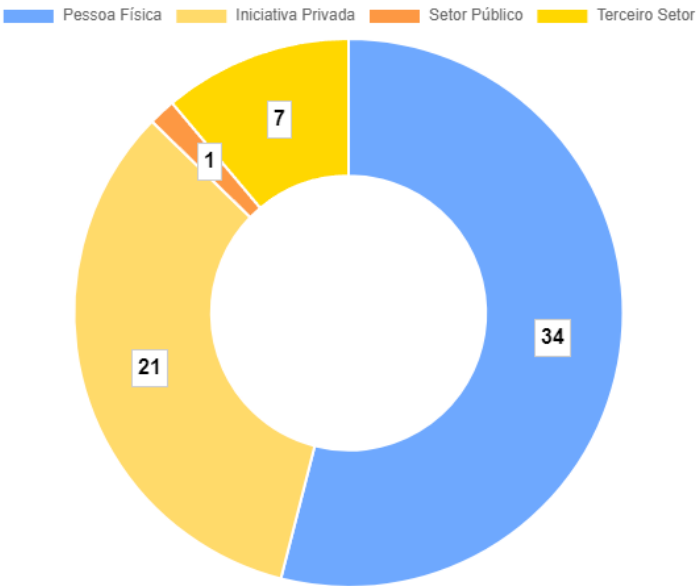
1.5. Nesse sentido, foi aberta a tomada de subsídio sobre o tratamento de dados de pessoais de crianças e adolescentes, pelo período 30 dias, de 18/06 a 17/07/2024 (SEI 0129746), prorrogada posteriormente, por mais 30 dias, até 16/08/2024 (SEI 0132964). A Tomada de Subsídios foi submetida com base em questões relacionadas aos temas do princípio do melhor interesse, consentimento e jogos e aplicações de internet (SEI 0127572), por meio de coleta de contribuições pela plataforma Participa Mais Brasil e arquivos enviados ao e-mail institucional da Coordenação-Geral de Normatização da ANPD.

2. **ANÁLISE**

Das Contribuições Recebida

2.1. Foram recebidas o total de 86 contribuições de 79 contribuintes, totalizando 1.809 laudas contendo comentários, fundamentos e sugestões às questões postas sob consulta à sociedade, de pessoas físicas, organizações, associações em âmbito nacional e internacional.

2.2. As contribuições foram proveniente de pessoas físicas e jurídicas, sendo 34 pessoas físicas e 29 pessoas jurídicas, representando a iniciativa privada (21), o setor público (1) e o terceiro setor (07). Não estão representadas no gráfico as contribuições recebidas do exterior (06).



2.1. As contribuições se concentraram nas regiões Sudeste 61,29%, Centro-oeste 14,52%, Sul 8,06% e Nordeste 06,45%. Foram recebidas também 9,68% de organizações do exterior do país.

2.2. Das 86 contribuições recebidas, 63 foram provenientes da Plataforma Participa Mais Brasil (SEI 0140377) e 23 contribuições, com 30

arquivos (SEI 0150156), foram enviados ao e-mail institucional da Coordenação-Geral de Normatização (normatizacao@anpd.gov.br).

2.3. Os arquivos enviados por e-mail, representaram o maior volume de laudas para leitura e análise (1543), sendo muitos deles constituídos de artigos publicados, teses de doutorado e publicações advindas de organizações do terceiro setor onde os temas foram tratados de forma esparça e desvinculada da ordem das perguntas, o que trouxe uma demanda maior de tempo para leitura e análise do material.

2.4. Constatou-se que foram apresentados textos iguais na plataforma Participa Mais Brasil, que tinham como pretensão responder a cada uma das 11 questões, com posições genéricas, de reforço à possibilidade de regulação ou fixação de orientações e diretrizes.

2.5. O material serviu de base à análise regulatória e resultou em resumos com contribuições específicas para cada uma das 11 questões apresentadas na Tomada de Subsídios.

2.8. Apresenta-se a seguir o resumos das contribuições para as 11 questões que integram os três blocos temáticas destacados na Tomada de Subsídios.

Síntese das Contribuições da Tomada de Subsídios

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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.3. As contribuições refletem as opiniões sobre como abordar o princípio do melhor interesse, considerando a indefinição do conceito. Enfatizam a necessidade de fornecer orientações claras e diretrizes práticas, considerando a diversidade de contextos e a complexidade do tratamento de dados pessoais, com critérios específicos e uma abordagem equilibrada e equitativa para garantir a proteção eficaz dos dados de crianças e adolescentes.

2.4. Sugere-se considerar tanto a proteção dos direitos das crianças, quanto as necessidades das empresas e as inovações tecnológicas, destacando que a regulamentação deve ser flexível e adaptada às diferentes idades e contextos.

2.5. Também foram sugeridas ações em colaboração com outros órgãos e considere regulamentações internacionais para garantir uma abordagem coesa e eficaz, bem como sobre a importância de educar pais e responsáveis sobre o tratamento de dados no ambiente digital.

- 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.

SÍNTESE DAS CONTRIBUIÇÕES:

2.6. As contribuições apontam para a crescente necessidade de regulamentação e orientação sobre o tratamento de dados pessoais de crianças e adolescentes no contexto digital, com ênfase em diferentes plataformas e serviços. Ele sugere uma série de medidas com equilíbrio e equidade para garantir a privacidade, segurança e o bem-estar desses menores, considerando as particularidades de cada contexto, como educação digital, redes sociais, jogos, dispositivos conectados, e marketing online.

2.7. Sugere-se que se forneça orientações claras e exemplos de boas práticas sobre como os controladores podem aplicar, documentar e demonstrar o cumprimento do princípio do melhor interesse da criança com exemplos concretos, com possível flexibilização para agentes específicos, como educadores e prestadores de serviço.

2.8. A título de exemplo, destaca-se o tratamento de dados em escolas e clínicas, onde o controle e monitoramento de dados devem respeitar a privacidade e os direitos das crianças, prevenindo abusos e garantindo a segurança dos dados pessoais. Proteção de dados sensíveis e garantia de confidencialidade. Orientação para que dados sejam usados apenas para fins educacionais e coleta mínima de dados. Coleta segura de dados com consentimento específico, informado e livre.

2.9. Sites e plataformas devem garantir que dados pessoais de menores, como geolocalização e informações sensíveis, sejam tratados com a devida segurança. Isso inclui a obtenção de consentimento dos pais com transparência e a realização de avaliações regulares de segurança. Imposição de restrições e parâmetros à coleta de dados e implementação de verificação de idade, consentimento e controle parental eficazes. Sugere-se que deve proibir a criação de perfis publicitários para menores.

2.10. Trouxeram ainda, comentário sobre o equilíbrio entre proteção e acesso à internet, a análise de custo-benefício da regulamentação e a responsabilidade das plataformas digitais como aspectos críticos a serem considerados para evitar efeitos colaterais indesejados, como a exclusão das crianças de plataformas digitais. As experiências digitais devem considerar questões éticas, educativas e de segurança, conciliando o melhor interesse das crianças e adolescentes com as práticas comerciais e tecnológicas.

II – CONSENTIMENTO

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

SÍNTESE DAS CONTRIBUIÇÕES:

2.11. Propõe-se uma reflexão detalhada sobre a necessidade de equilibrar a proteção dos dados pessoais de crianças e adolescentes com a inovação no setor digital. Ele reforça que a criação de diretrizes claras e

transparentes para o consentimento é essencial, considerando a especificidade de cada operação de tratamento de dados.

2.12. Cita a importância de que o consentimento seja obtido de forma ética, transparente, com manifestação consciente e informada, promovendo a proteção dos dados pessoais de crianças e adolescentes conforme a LGPD. A prestação de informações de forma clara e acessível usando linguagem simples, quanto à finalidade; a coleta; o uso; o compartilhamento; a retenção e à eliminação dos dados, evitando termos técnicos ou jurídicos que possam causar confusão e, se possível com recursos visuais, também contribuem para o entendimento para que os pais compreendam plenamente as implicações de suas decisões, com destaque para as consequências de não conceder o consentimento. Sugere-se que o entendimento dado aos termos “específico e em destaque” (LGPD, Art. 14, §1º) e “livre, informado e inequívoco” seja esclarecido dado as incertezas jurídicas.

2.13. Sugere-se que o consentimento seja apartado de outras informações, como os termos de uso e as políticas de privacidade, para garantir que os responsáveis possam identificá-lo claramente com a utilização de métodos de verificação, como autenticação multifator, confirmação por e-mail ou SMS, prova de identidade, entre outros, de acordo com a sensibilidade dos dados tratados.

2.14. A necessidade de especificidade no consentimento assume papel relevante, de forma que cada operação de tratamento de dados deve ser aprovada separadamente, permitindo que os pais compreendam as implicações de cada ato e autorizem de forma distinta, conforme as finalidades do tratamento. Esse consentimento deve também ser adaptável aos diferentes contextos sociais, geográficos e tecnológicos.

2.15. A progressividade no consentimento é outro ponto central, sugerindo que o processo seja ajustado conforme o desenvolvimento das crianças e adolescentes. Inspirado pelo *Age Appropriate Design Code* do Reino Unido, propõe-se que as crianças e adolescentes possam participar do processo de consentimento de acordo com sua idade e compreensão, respeitando princípios legais como o Estatuto da Criança e do Adolescente (ECA).

2.16. Sugere-se, também, que o processo de consentimento deve ser proporcional ao risco envolvido, com o rigor das exigências diretamente proporcionais à elevação do impacto potencial sobre os direitos dos menores. Oferecer meios simples e claros para que os responsáveis possam revogar o consentimento a qualquer momento, podendo o menor, ao atingir a idade adequada, assumir controle sobre seus próprios consentimentos.

2.17. A abordagem progressiva do consentimento, a adaptabilidade aos contextos e a segurança na verificação da identidade dos responsáveis, mantendo registros seguros e detalhados dos consentimentos obtidos, são fundamentais para garantir que os direitos das crianças sejam protegidos sem inibir o desenvolvimento de novos serviços digitais.

2.18. A conscientização dos pais sobre a importância da proteção de dados pessoais é fundamental. A criação de materiais educativos, como vídeos

e infográficos, guias e tutoriais educativos, pode ajudar a esclarecer o processo de consentimento e a importância de proteger os dados das crianças.

2.19. Houve também crítica à flexibilização das hipóteses legais para o tratamento de dados sem consentimento parental, sugerindo que isso poderia enfraquecer a proteção e comprometer a transparência exigida pela LGPD.

4. Considerando as boas práticas, as tecnologias disponíveis, e os princípios da LGPD, em especial os da finalidade, necessidade e 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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.20. Sugere-se a adoção de diretrizes flexíveis e proporcionais às diferentes plataformas, garantindo a segurança sem sobrecarregar os agentes de tratamento ou comprometer a privacidade dos dados, buscando um equilíbrio entre a proteção infantil e o acesso a serviços e informações online com medidas proporcionais ao risco, evitando tratamento excessivo de dados e a “fadiga do consentimento”.

2.21. As boas práticas para a obtenção do consentimento parental no tratamento de dados pessoais de crianças devem observar o alinhamento da Lei Geral de Proteção de Dados (LGPD) com as regulamentações internacionais. Entre as principais recomendações, destacam-se:

1. Design Intuitivo e Informações Claras: Interfaces devem ser claras e acessíveis, com descrições detalhadas sobre os dados coletados, seu uso, armazenamento e compartilhamento. O processo deve ser transparente e adaptado às particularidades de crianças e adolescentes, seguindo os princípios de necessidade, adequação e proporcionalidade;

2. Verificação de Identidade: Métodos robustos, como biometria facial, autenticação multifator, envio de documentos, sistemas de pagamento, assinaturas digitais, e-mails ou SMS de confirmação e videoconferências, devem ser usados, sempre respeitando o princípio da minimização de dados e de forma menos invasiva possível, para garantir que o consentimento seja dado por responsáveis legais;

3. Processo de Consentimento Destacado: O consentimento deve ser obtido de forma destacada, com ações afirmativas claras para cada finalidade de uso dos dados;

4. Documentação e Armazenamento Seguros: Manter registros detalhados e seguros do consentimento, permitindo a fácil auditoria e conformidade;

5. Facilidade de Revogação: Garantir que os

responsáveis possam revogar o consentimento de forma simples e sem burocracia;

6. Uso de Tecnologias Avançadas e inovação: Adoção de IA e blockchain para monitorar e garantir a integridade do processo de consentimento, com orientações flexíveis para acompanhar a evolução tecnológica e permitir que as empresas adaptem suas práticas de acordo com seus contextos específicos;

7. Esforços Razoáveis: Considerar limitações financeiras e tecnológicas ao implementar medidas de segurança, adotando "esforços razoáveis" para verificar o consentimento;

8. Risco e Proporcionalidade: As medidas devem ser proporcionais ao risco do tratamento dos dados, com métodos mais rigorosos para situações de maior risco;

9. Inclusão e Equidade: Garantir que o processo de proteção de dados não crie barreiras para famílias de baixa renda ou sem acesso à tecnologia, assegurando que todos os grupos tenham acesso à proteção digital;

10. Inclusão e Equidade: Evitar barreiras decorrentes de diferenças culturais, linguísticas e de acesso à tecnologia, especialmente para famílias de baixa renda ou que não possuem documentos específicos. Esses esforços visam garantir que o processo de proteção de dados de crianças e adolescentes não crie barreiras adicionais que possam resultar na exclusão digital de grupos já vulneráveis; e

11. Colaboração entre Controladores e Responsáveis Legais: A responsabilidade de proteger as crianças no ambiente digital também envolve os pais e responsáveis, além das plataformas e controladores que devem prover o suporte de ferramentas adequadas.

2.22. Houve também menções sobre a importância de desenvolver materiais educativos e campanhas de conscientização sobre a proteção de dados para pais e responsáveis.

5. 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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.23. Destacou-se as diferentes abordagens no tratamento de dados pessoais de crianças e adolescentes e a complexidade de equilibrar a proteção dos menores com a promoção da sua autonomia progressiva, especialmente

no contexto digital. Em linhas gerais não há opinião predominante ou consensual sobre o tema.

2.24. Algumas contribuições sugerem o entendimento que a LGPD tenha uma interpretação restritiva, defendendo que a exigência de consentimento dos responsáveis se aplique apenas a crianças até 12 anos incompletos, sem se estender a adolescentes entre 12 e 18 anos, indo além da interpretação tradicional do Código Civil, que considera menores de 16 anos como incapazes. Defendeu-se também a necessidade de diferenciar o consentimento para dados pessoais do regime de capacidades cíveis para celebração de negócios jurídicos, que ainda requer a assistência ou representação dos pais.

2.25. Nessa abordagem, o princípio da autonomia progressiva também é enfatizado, sendo essencial para o desenvolvimento de habilidades cognitivas e de responsabilidade nos adolescentes, permitindo que eles participem ativamente em decisões que os afetam, especialmente em ambientes digitais.

2.26. Sugeriu-se que adolescentes acima de 16 anos possam, em alguns casos, fornecer consentimento autônomo, atos simples e rotineiros, reconhecendo sua capacidade de consentir de forma autônoma em determinados contextos, desde que haja critérios para avaliar sua maturidade e compreensão. Considera-se que tratamentos de baixo risco e com claro benefício para o adolescente não precisariam da autorização dos responsáveis, evitando barreiras ao acesso a benefícios digitais. Atividades digitais comuns, como jogar, utilizar redes sociais ou plataformas educacionais, devem ser vistas de forma diferente de transações financeiras. Para menores de 16 anos, ainda é recomendado o consentimento conjunto entre pais e adolescentes.

2.27. Além disso, há uma presunção de que os pais estão cientes dessas atividades online, sendo suficiente uma supervisão geral, sem a necessidade de consentimento formal para cada interação do cotidiano, podendo o consentimento ser revogado.

2.28. Abordagem contrária surge ao comentar a questão da vulnerabilidade dos adolescentes em ambientes digitais e o risco de exposição a conteúdos inadequados, enfatizando a necessidade de seguir as regras de capacidade civil e envolver os pais ou responsáveis na tomada de decisões, especialmente devido aos riscos do ambiente digital, em seu papel como orientadores nesse processo de transição para uma autonomia progressiva. A cautela é necessária para garantir que a autonomia progressiva não ultrapasse os limites da responsabilidade jurídica.

2.29. Por fim, comentou-se que o consentimento digital de adolescentes seja adaptado a sua realidade, alinhado com o Estatuto da Criança e do Adolescente (ECA) e o Código Civil, enquanto a responsabilidade penal e outras áreas de maior risco ainda devem envolver a supervisão ou autorização dos responsáveis legais.

2.30. Houve também comentários sobre a necessidade de se oferecer mecanismos adequados de verificação de idade, além de avisos de privacidade compreensíveis para os jovens, garantindo a proteção dos seus direitos e a

segurança no ambiente digital.

III – JOGOS E APLICAÇÕES DE INTERNET

6. 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?

SÍNTESE DAS CONTRIBUIÇÕES

2.31. Propõe-se a aplicação de princípios como Finalidade, Necessidade, Adequação e Transparência no tratamento dos dados dos menores, destacando a importância de obter consentimento explícito dos pais. Sugere também que a coleta de dados seja limitada a finalidades específicas e a implementação de medidas de segurança para proteger contra riscos como conteúdo prejudicial, *bullying* e práticas comerciais inadequadas.

2.32. Sugere-se a adaptação das ferramentas de privacidade conforme as crianças amadurecem, dando-lhes mais controle sobre seus dados e o desenvolvimento cognitivo, ferramentas de controle parental e ações educativas. Considerando os riscos que crianças e adolescentes enfrentam online, como o acesso a conteúdo prejudicial, *bullying* e relações comerciais inadequadas, propõe-se uma abordagem baseada em um conjunto de medidas de segurança.

2.33. O uso de ferramentas, como as definidas pelo *Age Appropriate Design Code* do Reino Unido, Comentário Geral nº 25 da Organizações das Nações Unidas (ONU) e legislações de outros países, como referências que fornecem um contexto robusto, que impõem altos padrões de privacidade e segurança para crianças evidenciando a relevância de alinhar suas políticas às melhores práticas globais, tais como:

1. observância do melhor interesse de crianças e adolescentes, com foco no bem-estar, direitos e transparência.

2. verificação de idade, os controles parentais, uso de AI, a autenticação multifatorial, a supervisão e a limitação de tempo de uso para crianças, como alertas de pausa e incentivo ao uso moderado das plataformas, bloqueio de notificações e mensagens diretas aos mais jovens;

3. elaboração de relatórios de impacto à proteção de dados, com avaliação contínua dos riscos

4. vedação de práticas prejudiciais aos direitos dos jovens usuários e evitar a exploração dos dados pessoais pelas plataformas com a perfilização algorítmica;

5. definição de responsabilidade das plataformas para implementar e promover a segurança online, com equilíbrio entre a proteção da privacidade e a autonomia dos jovens usuários;

6. restrições ao uso de tecnologias de rastreamento;

7. utilização de técnicas como pseudonimização e criptografia para salvar dados sensíveis.

8. aplicação do *Privacy by Design*, privacidade desde a concepção, design dos produtos e serviços digitais, bem como diretrizes e configurações enfatizando a importância de adaptar essas medidas às diferentes faixas etárias e níveis de maturidade dos usuários; e

9. implementação de interfaces inclusivas e ajustadas ao desenvolvimento cognitivo das crianças, garantindo que elas compreendam as funcionalidades e implicações do tratamento de dados.

2.34. Houve contribuição, ainda, da autorregulação da indústria de jogos, da necessidade de auditorias periódicas e de garantir o armazenamento seguro e por tempo limitado dos dados pessoais. Destaca-se a importância de políticas alinhadas com as melhores práticas globais, como as do Reino Unido e da ONU e sugere-se, ainda, a fiscalização rigorosa e penalizações para plataformas que não cumprirem as normas de proteção à privacidade e segurança online.

7. 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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.35. Destacou-se os desafios técnicos e regulatórios relacionados à implementação de ferramentas de verificação de idade em plataformas digitais, principalmente no contexto da proteção de dados de crianças e adolescentes. Ressalta que não há um método único ou infalível para a verificação de idade, e as soluções devem ser adaptadas ao tipo de serviço e ao estado da arte da tecnologia disponível, e as técnicas devem ser proporcionais ao objetivo e à plataforma.

2.36. Sugere-se uma abordagem multifacetada para a verificação de idade, combinando técnicas de baixo custo e alta eficácia, destacando alguns desafios e limitações dessas técnicas, como o risco de invasão de privacidade e a necessidade de equilibrar a coleta de dados com a mitigação do risco. Sugere-se o uso de soluções menos invasivas, como a autenticação por terceiros e o modelo de "*zero knowledge proof*", que permite verificar informações sem revelar dados pessoais.

2.37. Reconhece-se a possibilidade de contorno desses mecanismos por menores e responsáveis, sublinhando que a verificação de idade não deve substituir o papel dos pais, podendo cumular verificação de idade com consentimento parental, quando aplicável. Dessa forma, é necessário a busca pelo equilíbrio entre segurança, privacidade e a necessidade de garantir a idade do usuário, com observância dos princípios da Lei Geral de Proteção de Dados (LGPD), considerando tanto a proteção de dados quanto a viabilidade técnica de implementação, sempre priorizando o melhor interesse das

crianças e adolescentes com objetivo de evitar que os sistemas de verificação de idade tornem-se sistemas de vigilância, que prejudiquem direitos e liberdades.

2.38. Enfatiza-se que a transparência no processo de verificação de idade, a proporcionalidade das medidas empregadas e a minimização dos dados, pois o uso excessivo de dados pode ser contraproducente, são essenciais para a mitigação dos riscos à liberdades e direitos das crianças e adolescentes.

2.39. A verificação de idade em plataformas digitais pode ser realizada por meio de várias opções que podem ser adotadas pelos agentes de tratamento de dados, com o objetivo de garantir a segurança de menores sem comprometer sua privacidade. Cita-se guias como o "*Age Appropriate Design Code*" e o "*Children's Online Privacy Protection Rule*" (COPPA) como exemplos que oferecem diferentes métodos de verificação, dentre eles destaca-se:

- a) autodeclaração de idade, que pode ser combinada com questionários para desincentivar declarações falsas;
- b) uso de documentos comprobatórios, como RG ou CPF e data de nascimento em bases públicas ou privadas, utilizando tecnologias de reconhecimento óptico (OCR) para validação automática;
- c) uso de autenticação multifator (MFA), em que o usuário confirma sua identidade por meio de dois ou mais métodos, como SMS ou e-mail;
- d) possibilidade de integração de serviços de verificação de idade de terceiros, que utilizam bases de dados públicas e privadas;
- e) biometria facial como uma forma de estimar a idade do usuário, embora essa técnica pode ser invasiva e suscetível a vieses, dado o risco à privacidade e a possíveis falhas na identificação de crianças;
- f) validação por meios de pagamento como o cartão de crédito;
- g) uso de inteligência artificial para analisar padrões de comportamento;
- h) implementação de ferramentas de controle parental para monitoramento e restrição de acesso;
- i) uso de tecnologias de geolocalização para garantir que as leis locais de verificação de idade sejam respeitadas.

2.40. A educação e conscientização dos pais e usuários sobre a importância da veracidade das informações também é abordada, bem como a necessidade de implementar revisões regulares dos métodos de verificação para garantir sua eficácia e conformidade com as melhores práticas.

2.41. Por fim, propõe-se considerar os esforços razoáveis dos agentes

de tratamento de dados ao implementar essas ferramentas, sempre levando em conta a minimização dos dados pessoais coletados, bem como a promoção de pesquisas e desenvolvimento de novas tecnologias por meio de um ambiente de testes (*sandbox regulatório*), além de manter práticas acessíveis, flexíveis e proporcionais para diferentes tipos de empresas.

8. 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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.42. Destaca-se a importância de que as plataformas digitais forneçam informações claras e acessíveis sobre a coleta e uso dos dados, com finalidade clara, específica e justificada, limitada ao necessário para o serviço oferecido e com o consentimento informado dos pais ou responsáveis, garantindo que estejam sempre agindo no melhor interesse das crianças e adolescentes, sempre avaliando os riscos associados e buscando equilibrar a proteção dos dados com o desenvolvimento e a autonomia das crianças.

2.43. Com foco específico no art. 14, § 4º, que restringe a coleta de dados de menores, ressalta a importância de diretrizes rígidas e bem definidas para a proteção de dados desse grupo, propondo que se adote uma postura proativa na fiscalização e na orientação sobre essas práticas. Deve respeitar princípios fundamentais, como a necessidade e a proporcionalidade, ao tratar dados sensíveis, incluindo dados biométricos e de saúde;

2.44. Deve-se proibir o uso de dados de crianças para a criação de perfis comportamentais, identificação de emoções e manipulação de pensamentos, que possam ser usados para publicidade direcionada ou manipulação. Sugere-se a edição de orientações claras para evitar abusos, mesmo não proibindo de forma absoluta a formação de perfis, desde que seja demonstrado o interesse legítimo da criança.

2.45. O perfilamento pode oferecer benefícios, como a personalização de conteúdos adequados e a proteção contra fraudes. Contudo, as plataformas poderiam padronizar a desativação do perfilamento para publicidade, com controles parentais e configurações adequadas à idade.

2.46. Ressalta-se, ainda, a observância das diretrizes da Resolução n.º 245 do CONANDA e outras normativas, visando a proteção da privacidade e segurança das crianças e adolescentes.

9. 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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.47. Comenta-se que as empresas e as plataformas digitais também têm a responsabilidade de proteger os dados das crianças, respeitando

princípios legais e éticos, como a responsabilidade compartilhada, e adotando práticas que considerem a diversidade sociocultural do Brasil.

2.48. Sugere-se que os sistemas operacionais adotem "*bandeiras de crianças confiáveis*", em que os pais ou responsáveis marquem a opção que sinalizem se um usuário é menor de idade, bloqueando conteúdo inapropriado, como alternativa à verificação de idade, sem exigir compartilhamento de documentos de identidade.

2.49. Levar-se em consideração uma abordagem proporcional à idade e ao grau de discernimento, levando em consideração a idade e o desenvolvimento, equilibrando a proteção de dados com o respeito à autonomia progressiva de crianças e adolescentes.

2.50. O controle parental deve ser visto como medida de segurança e não de vigilância. Assim, os mecanismos de controle parental precisam ser transparentes e respeitar a privacidade do menor.

2.51. Com esse enfoque, sugere-se a criação de mecanismos de supervisão menos invasivos para adolescentes, que preservem sua privacidade e incentivem o diálogo aberto com os responsáveis. Observando práticas internacionais, há recomendações de que os jovens sejam informados, de forma clara, sobre a utilização de medidas de controle parental e que ferramentas de monitoramento ou rastreamento estão em uso, como uma abordagem mais equilibrada em relação à autonomia e privacidade dos jovens.

2.52. Sugere-se diversas ferramentas e práticas que podem ser implementadas para garantir a proteção de dados de crianças e adolescentes e ampliação da supervisão parental. Entre as medidas sugeridas estão:

1. Painéis de Controle Parental: Ferramentas que permitem aos pais a visualização, gerenciamento e controle as informações coletadas e as configurações de privacidade sobre seus filhos de forma intuitiva. O consentimento parental inicial deve ser granular, mas à medida que a criança desenvolve, mais decisões sobre o uso de seus dados podem ser delegadas a ela;

2. Medidas de segurança: uso de ferramentas e configurações avançadas que permitam aos pais monitorarem e ajustar a privacidade, o conteúdo acessado, o tempo de uso e as atividades online, sempre respeitando a progressão da autonomia dos jovens;

3. Notificações e Alertas: Avisos regulares sobre atividades de coleta de dados, processos de verificação de identidade, alterações de políticas e consentimentos;

4. Ferramentas de Consentimento: Mecanismos para que o consentimento dos pais seja obtido de forma clara, com informações transparentes e acessíveis sobre o uso dos dados. Além disso, mecanismos para a revogação do consentimento;

5. Relatórios de Atividade: Relatórios periódicos detalhando o tratamento dos dados coletados;

6. Configurações de Privacidade Personalizáveis: Opções para ajustar os níveis de privacidade e limitar a coleta de dados. Garantir o consentimento informado dos pais ou responsáveis sobre o tratamento de dados pessoais de crianças e adolescentes, propondo o uso de checkboxes para que eles possam autorizar individualmente cada finalidade do tratamento, adaptáveis ao nível de maturidade dos menores, permitindo supervisão e controle adequado por parte dos pais; e

7. Direito dos titulares: É necessário simplificar o exercício dos direitos dos titulares, tornando fácil e informada as possibilidades do exercício dos direitos dos titulares, em especial a eliminação e a anonimização de dados.

2.53. Comentou-se, também, a importância de campanhas educativas para orientar pais e responsáveis sobre as melhores práticas para o uso dessas ferramentas e a proteção de dados, parcerias com escolas para conscientizar sobre os riscos e benefícios da internet, promovendo um ambiente digital seguro para o desenvolvimento de crianças e adolescentes, priorizando a inclusão de famílias de diferentes contextos sociais.

10. 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?

SÍNTESE DAS CONTRIBUIÇÕES:

2.54. Propõe-se adaptar a comunicação conforme a faixa etária e maturidade dos usuários, para garantir que as informações sejam compreensíveis tanto para pais quanto para jovens usuários, como sugere o *Children's Code* do Reino Unido:

1. Comunicação adaptada: uso de avisos de privacidade em linguagem adequada para crianças e adolescentes, evitando jargões técnicos, e o uso de recursos visuais, como infográficos e vídeos explicativos, que tornam as informações mais intuitivas, a criação de sumários simplificados dessas práticas e interfaces fáceis de navegar para consentimento e gestão de dados;

2. Diversificação de formatos: Além dos documentos tradicionais, sugere-se o uso de materiais audiovisuais e técnicas lúdicas, como quadrinhos e animações, para tornar as informações mais acessíveis e atrativas. Sessões educativas interativas, notificações proativas sobre mudanças nas políticas de privacidade e ferramentas para revisão e revogação de consentimentos também são sugeridas;

3. Canais de comunicação: Facilitar o contato com um responsável pela privacidade e implementar recursos interativos para resolver dúvidas de usuários e seus responsáveis. Com acessibilidade universal, que abranja pessoas com deficiências, e de interfaces de usuário amigáveis, que facilitem a navegação e

entendimento; e

4. Comunicação contínua e aberta com os usuários: através de feedback e workshops, além de oferecerem documentação clara sobre consentimentos e opções de privacidade, oferecendo canais de comunicação acessíveis para esclarecer dúvidas e permitir o exercício de direitos relacionados aos dados.

2.55. Ainda foram comentadas a necessidade de prover educação digital, como instrumento fundamental, tanto para crianças quanto para pais e responsáveis, que devem ser envolvidos no processo para promover uma compreensão mais profunda sobre a privacidade online. É importante que se promova campanhas de conscientização sobre o uso seguro da internet, possivelmente em parceria com escolas, criação de guias específicos para pais e responsáveis, campanhas de educação sobre privacidade e a disponibilização de notificações contextuais para lembrar os usuários sobre o uso de seus dados de forma clara e objetiva

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

SÍNTESE DAS CONTRIBUIÇÕES:

2.56. Sugere-se a divulgação de diretrizes claras sobre o Relatório de Impacto à Proteção de Dados (RIPD) e a classificação de tratamentos de dados pessoais de crianças e adolescentes como de alto risco, considerando que essa classificação não deve ser aplicada automaticamente no tratamento de dados de menores por gerar ineficiências.

2.57. Ressalta-se a importância de ter flexibilidade e equidade na regulamentação para se adaptar a diferentes contextos e inovações tecnológicas, mantendo o foco no melhor interesse e proteção das crianças e adolescentes.

2.58. Aponta necessidade de regulamentação e medidas específicas para garantir segurança e privacidade no ambiente digital para as seguintes temáticas:

1. Uso de IA e Algoritmos: É necessário regulamentar o uso de inteligência artificial, algoritmos e dispositivos inteligentes no tratamento de dados de crianças, como *smartwatches*, para garantir a privacidade e segurança e evitar práticas prejudiciais ou exploratórias;

2. Publicidade Direcionada: Regras mais rígidas devem ser estabelecidas para evitar manipulação de crianças e adolescentes por meio de perfilamento e de marketing direcionado a menores, assegurando que não sejam explorados comercialmente;

3. Educação Digital: Programas educativos voltados a pais e responsáveis sobre a proteção de dados e privacidade digital

são essenciais, além de abordar medidas de segurança para crianças no ambiente digital. Realizar parcerias com outros órgãos para disseminar informações sobre proteção de dados de menores, visando um melhor interesse e proteção integral dessas pessoas. É essencial que os dados coletados por plataformas educacionais sejam usados apenas para fins educacionais, com consentimento adequado;

4. Transferência Internacional de Dados: Critérios claros devem ser definidos para garantir que os dados de crianças transferidos internacionalmente estejam protegidos conforme a LGPD;

5. Direitos dos Menores: Deve-se esclarecer como as crianças e adolescentes podem exercer seus direitos de titulares de dados, com a participação de pais ou responsáveis, conforme a maturidade;

6. Medidas Proativas de Segurança: Plataformas digitais devem adotar medidas proativas de segurança, como auditorias e protocolos de resposta a incidentes. Testes baseados em riscos para determinar quando é necessária a coleta de dados de idade e reforça a importância de garantir que as regulamentações acompanhem o avanço tecnológico;

7. Consentimento Parental: Regras claras sobre como obter o consentimento em contextos como saúde digital e mídias sociais são necessárias;

8. Exceção de Consentimento: O parágrafo 3º do art. 14 da LGPD permite o tratamento de dados sem consentimento parental em situações de proteção à criança, mas há falta de clareza sobre essa exceção. Sugere-se que se defina uma interpretação alinhada aos direitos do Estatuto da Criança e do Adolescente;

9. Geolocalização: O tratamento de dados de localização é considerado crítico e precisa de diretrizes específicas para garantir a segurança física das crianças;

10. Criptografia: O uso de criptografia é destacado como uma ferramenta essencial para proteger os dados pessoais de crianças em diversas situações;

11. Código de Design Adequado à Idade: a criação de diretrizes específicas que garantam que práticas de coleta e tratamento de dados sejam adequadas ao melhor interesse de crianças e adolescentes.

2.59. Sugere-se, ainda, a realização de consultas públicas e "sandboxes" regulatórios para temas como verificação de idade e criptografia, sugerindo maior articulação com o Sistema de Garantia de Direitos da Criança e do Adolescente e outras autoridades internacionais.

2.60. Ao longo das contribuições a menção para a necessidade de

execução de ações educativas de forma significativa. Entende-se que é necessário um esforço do regulador e dos agentes de tratamento no esclarecimento sobre a proteção de dados e a privacidade, bem como para o entendimento dos riscos inerentes ao convívio no meio digital.

3. CONCLUSÃO

3.1. Concluída a fase de coleta de subsídios, passaremos a fase de análise das contribuições que subsidiarão a tomada de decisão quanto ao instrumento de regulamentação passível de ser adotado no processo SEI nº 00261.001660/2023-31, relativo ao item 14 da Agenda Regulatório da ANPD para o biênio 2023-2024, bem como o mérito contido na proposta.

3.2. Diante do exposto, propõe-se o encerramento do processo, considerando que já foi atingido o seu objetivo de obter a participação da sociedade fornecendo contribuição por meio dessa Tomada de Subsídios.

3.3. À consideração superior.

Brasília, na data da assinatura.

PAULO CESAR DOS SANTOS

Especialista em Regulação
em exercício na ANPD

CARLOS FERNANDO DO NASCIMENTO

Especialista em Regulação
Coordenador de Normatização 2

3.4. De acordo. Encaminha-se o presente processo na forma sugerida.

Brasília, na data da assinatura.

RODRIGO SANTANA DOS SANTOS

Coordenador-Geral de Normatização



Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral de Normatização**, em 04/04/2025, às 14:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Paulo Cesar dos Santos**, **Coordenador(a), Substituto(a)**, em 04/04/2025, às 16:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0150239** e o código CRC **514BAD5D**.

Referência: Caso responda a este documento, indicar expressamente o
Processo nº 00261.004146/2024-39

SEI nº 0150239