Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

RELATÓRIO CONSOLIDADO

GRUPO DE TRABALHO Nº 2 – (GT2)

PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES

Integrantes do CNPD:

Alexandre Zago Boava

Ana Paula Martins Bialer

Bruno Ricardo Bioni

Gabrielle Bezerra Sales Sarlet

Isabella Vieira Machado Henriques (Coordenadora)

João Frederico Chagas Maranhão

Vitor Morais de Andrade

Apoio ao GT por integrantes do Alana:

Emanuella Halfeld

Júlia Mendonça

Luíse Menezes

Apresentação

O presente relatório faz parte do esforço do Grupo de Trabalho (GT) nº 2, sobre proteção de dados de crianças e adolescentes, do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), instituído pela Portaria CNPD nº 2, de 5 de novembro de 2025[1], para subsidiar a Agência Nacional de Proteção de Dados (ANPD) de informações relevantes para a sua atuação no que tange ao tema objeto dos trabalhos do GT.

É notório que passados pouco mais de 4 anos da completa vigência da Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD), ou seja, incluindo a vigência das regras sobre as sanções administrativas, o único artigo que se debruçou, especificamente, sobre a garantia dos direitos de crianças e adolescentes da Lei, o artigo 14, ganhou maior atenção e interesse nos debates nacionais – acadêmicos, políticos e sociais –, bem como pela própria ANPD.

Vale lembrar, a propósito, que a Agenda Regulatória para o biênio 2025-2026, aprovada em dezembro de 2024, por meio da Resolução nº 23/2024[2], incluiu o tema do 'Tratamento de dados pessoais de crianças e adolescentes', em especial no ambiente digital, dentre as suas prioridades da 'fase 1'. É verdade que, mais recentemente, por conta da promulgação da Lei 15.211/2025, Estatuto Digital da Criança e do Adolescente (ECA Digital), e dos seus respectivos desdobramentos, que incluíram a indicação da ANPD como autoridade administrativa autônoma de proteção dos direitos de crianças e adolescentes no ambiente digital, o tema saiu da Agenda Regulatória[3], mas isso para ser tratado de forma ampla pela Agência, dada a sua nova transversalidade nos trabalhos da ANPD[4].

Até por conta disso, o CNPD criou mais um Grupo de Trabalho sobre tema afeto ao interesse de crianças e adolescentes: o GT6, instituído pela Portaria CNPD nº 6, de 5 de novembro de 2025[5], para tratar da "Implementação do ECA Digital".

De qualquer forma, o tema da proteção de dados segue prioritário, em especial no que diz respeito ao ambiente digital. Até porque, "com base em trilhões de pontos de dados alimentados diariamente nas plataformas de tecnologia, os sistemas algorítmicos são usados para microssegmentar (*microtarget*), recomendar

---

[1] Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2a-formacao/2as-grupos-de-trabalho-da-2a-formacao-do-cnpd/portaria_cnpd_gt02_2025.pdf/@@display-file/file Acesso em: 3 Mai. 2026.
[2] Disponível em: https://dspace.mj.gov.br/bitstream/1/14048/2/RES_ANPD_2024_23.pdf Acesso em: 3 Mai. 2026.
[3] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/processo_regulatorio/agenda-regulatoria-1/agenda-regulatoria-2025-2026/balanco-agenda-regulatoria-2025-2026-02-2025.pdf/@@display-file/file Acesso em: 3 Mai. 2026.
[4] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital Acesso em: 3 Mai. 2026.
[5] Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2a-formacao/2as-grupos-de-trabalho-da-2a-formacao-do-cnpd/portaria_cnpd_gt06_2025.pdf/@@display-file/file Acesso em: 3 Mai. 2026.

e influenciar usuárias e usuários". Sistemas tais que hoje têm fundamental importância pois "somos parte de um ecossistema digital global mediado por algoritmos que têm impacto no comportamento coletivo e individual" [6].

Ademais, a humanidade já conta com sociedades e ambientes onde as TICs (tecnologias da informação e da comunicação) e suas capacidades de processamento de dados não são apenas importantes, mas configuram condições essenciais para a manutenção e qualquer desenvolvimento futuro do bem-estar social, do bem-estar pessoal, bem como do florescimento geral[7].

Indubitável, pois, que o tratamento de dados continua sendo tema fundamental para a sociedade brasileira e para a própria ANPD, ganhando prioridade institucional estabelecida em nível constitucional a partir da leitura do art. 227 da Constituição Federal. Assim, o presente relatório, realizado pelo GT2, diz respeito especificamente sobre a proteção de dados desse grupo de pessoas hipervulnerável. Não se confunde com os trabalhos realizados pelo GT6, que também se debruçou sobre os interesses de crianças e adolescentes, mas, como anteriormente dito, em uma outra perspectiva, relacionada aos novos desafios trazidos pela promulgação e vigência do ECA Digital.

É certo que o tema da proteção de dados de crianças e adolescentes atravessa vários assuntos tratados pelo ECA digital, como, por exemplo, a adequação dos mecanismos de aferição de idade ou a vedação de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e adolescentes. Até por isso os integrantes dos dois GTs foram convidados a participar das reuniões dos dois grupos, bem como houve um compartilhamento de informações entre as duas coordenações, que, ademais, participam formalmente uma do GT coordenado pela outra. Também os trabalhos apresentados neste relatório consideram esse campo de intersecção, sem ultrapassar os limites do seu objeto de análise.

No primeiro capítulo, o presente relatório apresenta o estado da arte da proteção de dados de crianças e adolescentes no ambiente digital, com foco no Brasil. Discorre sobre a regulação responsiva e a gestão de riscos na atuação da Agência Nacional de Proteção de Dados e sobre a articulação normativa entre proteção de dados e proteção integral. No segundo capítulo, o relatório aborda as contribuições recebidas de um ambiente multisetorial pelos integrantes do GT2 durante os seus trabalhos de escuta da sociedade civil, da academia, da indústria, do sistema de justiça e da própria ANPD. É apresentada uma sistematização das contribuições e, com isso, organizadas as proposições advindas das diversas partes interessadas ouvidas. O último capítulo oferece um exemplo de atuação concreta no campo, na esfera internacional, como forma de ilustrar a implementação normativa em relação ao tema da proteção de dados de crianças e adolescentes. Vale ressaltar que a escolha da autoridade italiana se deu pela sua ativa e notória atuação no tema, sendo verdade que há outras autoridades ao redor do mundo que poderiam também ter sido foco de estudo, algo que, desde já, recomenda-se para

[6] Mendonça, Ricardo; Filgueiras, Fernando; Almeida, Virgílio. Política dos algoritmos: instituições e as transformações da vida social. São Paulo: Ubu Editora, 2025, pp. 21-22; 219-220.
[7] Floridi, Luciano. The 4th Revolution: How the infosphere is reshaping human reality. Oxford: Oxford University Press, 2016.

futuros trabalhos do CNPD – o que não foi possível no âmbito dos trabalhos deste GT2 em razão do lapso temporal disponível para tanto.

Ao final, as Conselheiras e os Conselheiros integrantes deste GT2 apresentam suas recomendações à ANDP, com a certeza de que as suas contribuições refletem um trabalho dedicado e sensível ao tema proposto, além de inédito e focado na implementação legal, de maneira a subsidiar a efetiva atuação da Agência em relação à devida proteção dos dados de crianças e adolescentes.

S u m á r i o

(1) Panorama da proteção de dados de crianças e adolescentes no ambiente digital[8]

A presente seção tem por objetivo oferecer um panorama do estado da arte da proteção de dados pessoais no Brasil, a partir de um recorte específico: a proteção de crianças e adolescentes no ambiente digital. Parte-se da identificação das principais regras estruturantes do regime brasileiro e avança-se na análise de como tais normas vêm sendo interpretadas e operacionalizadas pela ANPD e pela jurisprudência constitucional, tendo em vista as exigências reforçadas que incidem sobre o tratamento de dados desse público.

O recorte adotado considera o tratamento de dados de crianças e adolescentes, à luz da proteção integral e da prioridade absoluta previstas no art. 227 da Constituição Federal e do art. 14º da Lei Geral de Proteção de Dados (LGPD), que estabelece o melhor interesse da criança e do adolescente como critério fundamental para o tratamento de seus dados pessoais. Mais do que um princípio orientador, esse critério funciona como parâmetro de validade substantiva do tratamento, condicionando a interpretação das bases legais e a própria estruturação das atividades de tratamento em contextos que envolvem sujeitos em desenvolvimento.

A centralidade conferida às crianças e aos adolescentes não decorre apenas de uma opção temática, mas da compreensão de que esse grupo evidencia, de forma mais nítida, as tensões e insuficiências de modelos tradicionais de proteção de dados baseados na autonomia individual. As assimetrias informacionais, a vulnerabilidade decisória e a inserção em ambientes digitais estruturados por lógicas opacas tornam particularmente sensíveis os efeitos do tratamento de dados sobre esse público, exigindo a adoção de parâmetros mais exigentes de controle do fluxo informacional.

1. Estado da arte da proteção de dados pessoais no contexto da proteção de crianças e adolescentes

O estado atual da proteção de dados pessoais no Brasil indica um afastamento da concepção clássica de privacidade, centrada em uma abordagem de ação negativa, em direção a uma compreensão mais ampla, voltada à tutela da personalidade e à autodeterminação informativa. Esse movimento foi consolidado, em grande medida, a partir da obra de Danilo Doneda (2019), que compreende o dado pessoal como dimensão da própria identidade, demandando uma proteção jurídica capaz de acompanhar a circulação e o uso das informações na sociedade digital. Em seu pano de fundo histórico, essa formulação dialoga com a noção de

[8] A escrita deste capítulo do Relatório foi liderada pelos Conselheiros **Bruno Ricardo Bioni** e **Gabrielle Sarlet**, que contaram com a colaboração da equipe Plataformas e Mercados da Associação Data Privacy Brasil de Pesquisa, coordenada por Carla Rodrigues, pela pesquisadora Natasha Novoa e pelo pesquisador Eduardo Mendonça.

autodeterminação informativa afirmada pelo Tribunal Constitucional Federal Alemão no *Volkszählungsurteil.*

Nessa linha, a literatura recente tem evidenciado os limites de uma leitura centrada exclusivamente na manifestação individual de vontade, sobretudo quando o titular dos dados pessoas são crianças e adolescentes. Em contextos marcados por profundas assimetrias informacionais e pela vulnerabilidade decisória, torna-se difícil para o titular ou seus responsáveis apreenderem as consequências futuras e cumulativas do tratamento de dados. A autodeterminação informativa, portanto, não se esgota no consentimento e exige a consideração das condições concretas em que as decisões são produzidas e o respeito à autonomia progressiva da criança e do jovem.

Esse deslocamento conduz à necessidade de observar não apenas a existência de bases legais, mas a forma como o fluxo informacional é estruturado e justificado. A legitimidade do tratamento passa a depender da capacidade de demonstrar que as operações realizadas são compatíveis com os riscos envolvidos e com as expectativas legítimas dos titulares, o que envolve não apenas transparência, mas também a possibilidade de acompanhamento e contestação do tratamento. Quando esse quadro é examinado sob a perspectiva do tratamento de dados de crianças e adolescentes, o regime jurídico assume contornos mais complexos. A proteção deixa de operar apenas como garantia individual e passa a ser estruturada a partir da condição peculiar de pessoa em desenvolvimento e do princípio da prioridade absoluta, nos termos do art. 227 da Constituição Federal. O art. 14 da LGPD, ao estabelecer o melhor interesse como critério central, introduz um parâmetro que opera simultaneamente como referência substantiva, diretriz interpretativa e exigência procedimental.

Nessa configuração, o melhor interesse não se limita a orientar a interpretação das bases legais, mas condiciona a própria validade do tratamento, ao exigir a demonstração de que as escolhas técnicas e organizacionais adotadas são compatíveis com a proteção desse público. Trata-se de um limite material ao exercício do poder informacional, especialmente relevante em contextos de elevada assimetria informacional e vulnerabilidade decisória. A análise, portanto, não pode permanecer ancorada em uma figura abstrata de titular plenamente capaz. As limitações cognitivas, a dificuldade de antecipação de consequências futuras e a inserção em ambientes digitais estruturados por lógicas opacas tornam inadequada uma abordagem fundada exclusivamente na manifestação de vontade. O tratamento de dados de crianças e adolescentes tende, por essa razão, a ser qualificado como atividade de maior risco, cuja legitimidade depende da forma como os fluxos informacionais são estruturados.

Essa preocupação aparece de forma mais concreta na Resolução CD/ANPD nº 2/2022[9], ao tratar do regime aplicável a agentes de pequeno porte, o texto delimita critérios para a identificação de atividades de alto risco e operações que envolvem dados de crianças e adolescentes, sobretudo quando associadas a

[9]Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. 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. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022..

potenciais impactos relevantes sobre direitos fundamentais ou ao uso de tecnologias e modelos de tratamento mais complexos. Nota-se que aqui o ponto não é apenas classificatório, pois ao reconhecer esse tipo de tratamento como potencialmente mais arriscado, a norma explicita que a vulnerabilidade do público infantojuvenil deve ser incorporada desde a etapa de avaliação do risco, e não apenas considerada de forma residual na aplicação das bases legais.

Com isso, a qualificação do tratamento como atividade de maior risco deixa de ser uma inferência doutrinária e passa a integrar o próprio desenho institucional do regime de proteção de dados. A consequência é o deslocamento do foco para a estruturação dos fluxos informacionais: exige-se que o agente seja capaz de antecipar impactos, justificar suas escolhas e demonstrar a adoção de salvaguardas proporcionais ao risco envolvido. No caso de crianças e adolescentes, esse padrão tende a ser mais exigente, justamente porque a legitimidade do tratamento está diretamente vinculada à proteção do seu processo de desenvolvimento.

A licitude do tratamento passa, assim, a exigir a demonstração de que esses fluxos sejam estruturados de maneira compatível com o livre desenvolvimento da personalidade, a autonomia progressiva e o processo de aquisição gradual de competências, compreensão e agência do titular[10]. Esse dever impõe a incorporação da lógica dos direitos das crianças por design desde a fase inicial de concepção dos sistemas, garantindo que a arquitetura tecnológica seja obrigatoriamente adequada às capacidades biopsíquicas de crianças e adolescentes, em vez de explorar sua vulnerabilidade decisória. Sob esse prisma, o regime orienta-se ao controle do fluxo informacional para assegurar que o tratamento de dados promova o desenvolvimento holístico do sujeito, limitando usos potencialmente lesivos e submetendo as operações a uma avaliação contínua de seus impactos sobre a personalidade em formação.

No ordenamento brasileiro, essa exigência não decorre de um capítulo autônomo voltado ao *Children Safety by Design*, na medida que a LGPD adota uma formulação mais concentrada no artigo 14, o que desloca para a interpretação sistemática a tarefa de estruturar esse padrão. A articulação entre o dever de *Privacy by Design* (art. 46, §2º), o mandamento constitucional da prioridade absoluta (art. 227 da Constituição Federal) e o critério do melhor interesse permite extrair uma obrigação de organização prévia dos fluxos informacionais. Nesse sentido, a arquitetura de produtos e serviços deixa de ser um elemento neutro e passa a operar como instrumento de garantia da segurança e do desenvolvimento integral, incorporando salvaguardas técnicas voltadas a impedir a exposição a riscos antes mesmo do início do tratamento.

Essa leitura aproxima o regime brasileiro dos parâmetros delineados no Comentário Geral nº 25 do Comitê dos Direitos da Criança da ONU, ainda que por via interpretativa. A exigência de adequação dos sistemas às capacidades em desenvolvimento do titular encontra respaldo na prática regulatória recente. Na

[10] Esse entendimento dialoga com a orientação principiológica do Comentário Geral n° 25 da Convenção sobre o Direito das Crianças da ONU. Como um dos princípios gerais, tem-se o desenvolvimento progressivo das capacidades.

fiscalização da plataforma TikTok, a ANPD[11] indicou que mecanismos baseados exclusivamente em autodeclaração etária (*age gate*) não atendem aos deveres de prevenção e segurança, por não impedirem, de forma efetiva, a inserção de crianças em ambientes inadequados. O ponto central não está na adoção formal de medidas, mas na sua capacidade de estruturar o fluxo informacional de modo compatível com a vulnerabilidade do público infantojuvenil.

O resultado é a consolidação de um arranjo em que a licitude do tratamento deixa de se apoiar em soluções formais e passa a depender da demonstração de que a tecnologia foi concebida e operada para respeitar essa condição de desenvolvimento. A exigência de salvaguardas estruturais, incorporadas desde a origem, funciona como limite ao uso econômico dos dados e como mecanismo de alinhamento entre inovação e proteção de direitos, assegurando que o ambiente digital não se organize em torno da exploração de processos em formação.

Nesse contexto, a noção de devido processo informacional emerge como critério mais exigente de legitimidade. Como desdobramento da cláusula do devido processo legal, esse conceito desloca o foco da análise para as condições em que o tratamento é estruturado, exigindo que o exercício do poder informacional seja organizado de modo a permitir sua compreensão, contestação e controle, especialmente quando incide sobre sujeitos em situação de maior vulnerabilidade. Nessa chave, o relatório de impacto a proteção de dados pessoais pode funcionar como instrumento de concretização desse controle, ao exigir descrição técnica do tratamento, identificação dos riscos e indicação de medidas de mitigação adotadas. Em operações que afetem crianças e adolescentes, essa função pode ser reforçada por metodologia que inclua a consulta a partes interessadas e a participação de entidades representativas da infância, de modo a qualificar a identificação dos impactos específicos desse público e a suficiência das salvaguardas previstas.[12][13]

É a partir dessa chave interpretativa que se torna possível compreender a atuação recente da ANPD em casos concretos envolvendo crianças e adolescentes.

2. Regulação responsiva e gestão de riscos na atuação da ANPD

A atuação da ANPD permite observar como os parâmetros delineados no plano normativo e doutrinário vêm sendo progressivamente concretizados na prática regulatória. Em contextos que envolvem o tratamento de dados de crianças e adolescentes, essa atuação assume contornos mais exigentes, na medida em que o critério do melhor interesse e a condição peculiar de desenvolvimento impõem um padrão reforçado de controle sobre o fluxo informacional**.**

---

[11] Nota Técnica nº 50/2023/CGF/ANPD. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf. Acesso em: 31 mar. 2026.

[12] INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. Relatório de Impacto à Proteção de Dados dos microdados dos Censos da Educação. Brasília, 2023. O relatório é descrito no material como contendo seção própria de partes interessadas consultadas.

[13]. Nota Técnica nº 50/2024. No processo de fiscalização relativo ao TikTok, o Instituto Alana, organização da sociedade civil, foi admitido como amicus curiae para apresentação de análises, pesquisas, estudos, pareceres e documentos, o que evidencia a relevância da participação institucional qualificada em casos que envolvem dados de crianças e adolescentes.

Como exemplo dessa abordagem, tem-se o Relatório de Instrução nº 3/2024[14], no caso da SAS-PE. O processo teve origem na apuração de incidente de segurança envolvendo a exposição indevida de dados pessoais de beneficiários de política pública de transporte gratuito para pessoas com deficiência, incluindo informações de saúde e dados de crianças e adolescentes. Ao classificar como infrações graves a ausência de requisitos de segurança e a falha na comunicação individualizada de incidentes, a ANPD firmou o entendimento de que a divulgação genérica em sítios eletrônicos não substitui o dever de notificação direta quando o controlador dispõe de meios de contato. Contudo, em atenção ao princípio da proporcionalidade, a ANPD optou por sanções de advertência cumuladas com medidas corretivas e cronogramas de implementação, focando na capacidade de auto-organização do agente.

Essa compreensão não se limita à dimensão informacional do dever de transparência, mas se vincula à própria estrutura do devido processo informacional. A ausência de ciência direta impede que os titulares adotem medidas para mitigar riscos e compromete a possibilidade de intervenção sobre o tratamento de seus dados, especialmente em contextos de maior vulnerabilidade. Nessa perspectiva, a falha na comunicação deixa de ser um vício periférico e passa a afetar a própria legitimidade do tratamento, na medida em que rompe as condições mínimas de controle do fluxo informacional.

A resposta regulatória adotada pela Agência, centrada na aplicação de medidas corretivas e na fixação de cronogramas de adequação, revela, por sua vez, uma lógica de regulação responsiva que busca recompor as condições de exercício desse processo, em vez de se limitar à punição da conduta. A sanção administrativa passa a operar, assim, como instrumento de reorganização do ambiente informacional, orientado à restauração de salvaguardas compatíveis com a proteção de crianças e adolescentes.

Essa mesma lógica se projeta de forma ainda mais evidente em contextos de plataformas digitais, como na fiscalização sobre a plataforma Tik Tok[15]. A ANPD sinalizou que a mera adesão a “padrões da indústria”, como mecanismos de verificação etária baseados em autodeclaração, é insuficiente diante da hipervulnerabilidade presumida de crianças e adolescentes. O dever de prevenção (art. 6º, VIII, da LGPD) e a lógica do Privacy by Design (art. 46, §2º) passam a ser interpretados como exigências de estruturação prévia do fluxo informacional, de modo a impedir a coleta irregular e o perfilamento antes mesmo de sua ocorrência. Não se trata, portanto, de reagir a violações já consumadas, mas de organizar o ambiente informacional de forma compatível com a proteção desse público.

Situação semelhante pode ser identificada na atuação da ANPD em relação ao WhatsApp, no contexto da atualização de sua Política de Privacidade.[16] Ao examinar as respostas da empresa sobre o tratamento de dados de crianças e

[14]Relatório de Instrução nº 3/2024/CGF/ANPD – versão pública. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/ri-pas-pe-versao-publica.pdf. Acesso em: 4 mar. 2026.
[15]Nota Técnica nº 50/2024, de 4 nov. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf.
[16] Nota Técnica nº 49/2022/CGF/ANPD. Manifestação técnica da Coordenação Geral de Fiscalização acerca da atualização da Política de Privacidade do WhatsApp. Brasília, DF, 2022.

adolescentes, a Agência entendeu que os argumentos apresentados não eram suficientes para afastar o risco de tratamento em desacordo com a LGPD, razão pela qual reiterou a exigência de relatório de impacto específico, com indicação das ferramentas técnicas adotadas ou a serem implementadas, das formas de tratamento, dos tipos de dados tratados, da base legal e da demonstração de compatibilidade com o melhor interesse desses titulares.[17] Embora, para os fins daquele processo, a recomendação tenha sido considerada atendida, a própria ANPD registrou que isso não afastava análise posterior em procedimento específico e assinalou a permanência de pontos de atenção que demandavam atuação preventiva e fiscalizatória ulterior, especialmente a adoção de medidas adicionais de segurança para verificação de idade e de medidas específicas de proteção para usuários adolescentes.

Esse padrão regulatório não emerge de forma isolada, mas se ancora em uma reconfiguração constitucional do regime de proteção de dados. Ao reconhecer a proteção de dados como direito fundamental autônomo nas ADIs 6387[18] e 6388[19], o Supremo Tribunal Federal afastou a ideia de que existiriam dados juridicamente insignificantes, afirmando que, no contexto do Big Data, mesmo informações aparentemente triviais podem ser combinadas para formar perfis com impacto direto sobre a personalidade. Essa premissa reforça a necessidade de controle sobre o fluxo informacional, especialmente quando incide sobre processos de desenvolvimento.

Essa orientação encontra concretização normativa na Lei nº 15.211/2025 (ECA Digital), que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, posteriormente regulamentada pelo Decreto nº 12.880/2026. Ao também incorporar diretrizes alinhadas ao Comentário Geral nº 25,[20] essas normas reconhecem que a exploração econômica baseada em inferências comportamentais afeta de forma desproporcional a autonomia e o desenvolvimento da personalidade de crianças e adolescentes, reforçando a exigência de salvaguardas estruturais no desenho de produtos e serviços digitais.

Essa exigência de justificação reforça a centralidade do devido processo informacional como critério de validade do exercício do poder informacional. O agente de tratamento passa a suportar um ônus argumentativo permanente, devendo demonstrar que a estruturação dos fluxos de dados, desde a concepção dos sistemas até sua operacionalização, é compatível com a proteção da personalidade e, no caso de crianças e adolescentes, com o seu livre desenvolvimento.

---

[17] Nota Técnica nº 49/2022/CGF/ANPD. No exame do tratamento de dados de crianças e adolescentes, a Autoridade registrou a necessidade de medidas adicionais de segurança para verificação de idade e de medidas específicas para usuários adolescentes, sem prejuízo de análise posterior em processo específico.

[18] Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6837. Medida Provisória 954/2020. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relatora: Min. Rosa Weber, 24 de abril de 2020.

[19] Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6388. Medida Provisória 954/2020. Compartilhamento de dados de usuários de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE) durante a emergência de saúde pública da COVID-19. Requerente: Partido da Social Democracia Brasileira. Relatora: Min. Rosa Weber, 17 de novembro de 2020.

[20] *Comentário Geral nº 25 (2021) sobre os direitos das crianças em relação ao ambiente digital*. Genebra: Organização das Nações Unidas, 2021.

3. Articulação normativa entre proteção de dados e proteção integral

A articulação entre a LGPD e o ECA Digital pode ser compreendida a partir da teoria do diálogo das fontes, tal como desenvolvida por Cláudia Lima Marques (2004).[21] Não se trata de relação excludente entre diplomas, mas de aplicação coordenada e complementar de regimes normativos que incidem sobre o mesmo suporte fático a partir de finalidades convergentes de tutela. Nessa perspectiva, a LGPD fornece o regime geral de tratamento de dados pessoais, enquanto o ECA Digital densifica, no ambiente digital, deveres específicos de prevenção, proteção, informação e segurança voltados à tutela de crianças e adolescentes. O resultado é o reforço recíproco de parâmetros protetivos, especialmente em contextos nos quais o tratamento de dados se insere em arquiteturas digitais aptas a explorar vulnerabilidades estruturais e situacionais desse público.[22]

O primeiro eixo deste diálogo diz respeito à vedação ao perfilamento para fins de publicidade comercial. O ECA Digital torna expressa a proibição de utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e adolescentes, bem como do emprego de análise emocional, de realidade aumentada, de realidade estendida e de realidade virtual para esse fim.[23] A norma especial não rompe com a LGPD. Ao contrário, especifica, à luz do melhor interesse e da condição peculiar de pessoa em desenvolvimento, limites mais densos ao tratamento de dados pessoais em contextos de exploração econômica da vulnerabilidade infantojuvenil.

O segundo eixo de articulação refere-se ao combate ao design manipulativo e aditivo. A LGPD já estabelece que as medidas de segurança devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. O ECA Digital aprofunda essa exigência ao determinar que os fornecedores desenvolvam desde a concepção e adotem por padrão configurações que evitem o uso compulsivo por crianças e adolescentes, bem como ao vedar o emprego de recursos que aumentem, sustentem ou estendam artificialmente o uso do produto ou do serviço. Em complemento, também proíbe a projeção, modificação ou manipulação de interfaces com o objetivo ou o efeito de comprometer a autonomia, a tomada de decisão ou a escolha do usuário, especialmente quando disso resulte o enfraquecimento das salvaguardas disponíveis.[24] Nessa leitura

---

[21] MARQUES, Cláudia Lima. Superação das antinomias pelo diálogo das fontes, o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. Revista da ESMESE, n. 7, 2004.

[22] MARQUES, Cláudia Lima; MUCELIN, Guilherme. Vulnerabilidade na era digital, um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. Civilistica.com, a. 11, n. 3, 2022. No artigo, os autores identificam a vulnerabilidade por design, por tratamento de dados pessoais e por atividade como categorias necessárias para a compreensão do ambiente digital contemporâneo.

[23] BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto Digital da Criança e do Adolescente. Arts. 22 e 26. Nos excertos anexados, a lei veda a utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e adolescentes, bem como a criação de perfis comportamentais para esse fim.

[24] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Art. 46, § 2º. BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto Digital da Criança e do Adolescente. Arts. 7º, 8º, IV, 17, § 4º, II, e 18, § 2º. Nos excertos anexados, esses dispositivos tratam

coordenada, o ambiente digital deixa de ser examinado a partir da licitude abstrata do tratamento e passa a ser avaliado também a partir do modo como sua arquitetura técnica é desenhada, o que conduz a uma formulação mais protetiva de *privacy by design* e de *safety by design* voltada a crianças e adolescentes.[25]

A terceira expressão desse diálogo reside no art. 31 do ECA Digital. O dispositivo impõe aos provedores de aplicações de internet com mais de um milhão de usuários na faixa etária a elaboração de relatórios semestrais que contenham, entre outros elementos, o detalhamento dos métodos utilizados e os resultados das avaliações de impacto, identificação e gerenciamento de riscos à segurança e à saúde de crianças e adolescentes. Essa obrigação dialoga diretamente com o art. 38 da LGPD, que faculta à ANPD determinar a elaboração de relatório de impacto à proteção de dados pessoais, e com o art. 50, § 2º, I, d, que incentiva a implementação de programa de governança com base em processo de avaliação sistemática de impactos e riscos à privacidade. No contexto do ECA Digital, a exigência de monitoramento contínuo reforça que as salvaguardas estruturais não se exaurem no momento da concepção do produto, devendo ser permanentemente avaliadas e atualizadas. É nesse ponto que o diálogo entre os diplomas deságua em uma leitura mais exigente de privacy by design e de safety by design, orientada à prioridade absoluta, ao melhor interesse, à autonomia progressiva e ao livre desenvolvimento da personalidade.[26]

Assim, a Lei nº 15.211 de 2025 e a LGPD estabelecem um diálogo sistemático de complementariedade, no qual a primeira opera como norma especial que concretiza e aprofunda, à luz dos princípios da proteção integral e do melhor interesse, as diretrizes gerais da segunda. A vedação ao perfilamento comercial, o combate ao design manipulativo e a exigência de relatórios periódicos de impacto e de gerenciamento de riscos constituem expressões de um modelo em que a proteção de dados e a proteção integral se entrelaçam, exigindo que o exercício do poder informacional seja estruturado de maneira compatível com a proteção de crianças e adolescentes.

Referências

ALEMANHA. Tribunal Constitucional Federal Alemão (Bundesverfassungsgericht). Julgamento da Lei do Censo (Volkszählungsurteil). BVerfGE 65, 1. Decisão de 15 de dezembro de 1983.

---

da configuração por padrão em modelo mais protetivo, da prevenção do uso compulsivo e da vedação de interfaces manipulativas.

[25] MARQUES, Cláudia Lima; MUCELIN, Guilherme. Vulnerabilidade na era digital, um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. Civilistica.com, a. 11, n. 3, 2022. O texto identifica vulnerabilidade por design, por tratamento de dados pessoais e por atividade como categorias relevantes para a compreensão do ambiente digital contemporâneo.

[26] BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto Digital da Criança e do Adolescente. Art. 31, VII. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Art. 38 e art. 50, § 2º, I, d. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica nº 50/2024/FIS/CGF/ANPD, 2024. O conjunto normativo e técnico reforça a necessidade de avaliação sistemática de impactos e riscos e de acompanhamento contínuo de salvaguardas em contextos envolvendo crianças e adolescentes.

BRASIL. ANPD. Relatório de Instrução nº 3/2024/CGF/ANPD – versão pública (Processo Administrativo Sancionador). Brasília, DF, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/ri-pas-pe-versao-publica.pdf. Acesso em: 4 mar. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Coordenação-Geral de Fiscalização; Coordenação de Fiscalização. Nota Técnica nº 50/2024/FIS/CGF/ANPD. Processo nº 00261.004725/2024-81. Tratamento de dados pessoais de crianças e adolescentes pela rede social TikTok e análise de mecanismos de verificação de idade e do "feed sem cadastro". Brasília, DF: ANPD, 4 nov. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf. Acesso em: 4 mar. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 50/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf. Acesso em: 31 mar. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 6/2023/CGF/ANPD – versão pública (processo TikTok). Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf. Acesso em: 31 mar. 2026.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 4 mar. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 mar. 2026.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Diário Oficial da União, Brasília, DF, 18 set. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 4 mar. 2026.

BRASIL. Lei nº 15.352, de 25 de fevereiro de 2026. Transforma a Autoridade Nacional de Proteção de Dados em Agência Nacional de Proteção de Dados e dispõe sobre sua estrutura e cargos. Diário Oficial da União, Brasília, DF, 26 fev. 2026. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=601&pagina=1&data=25/02/2026&totalArquivos=2. Acesso em: 4 mar. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. 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. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 31 mar. 2026

BRASIL, Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6837. Medida Provisória 954/2020. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relatora: Min. Rosa Weber, 24 de abril de 2020. [2020b]. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 4 mar. 2026.

BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6388. Medida Provisória 954/2020. Compartilhamento de dados de usuários de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE) durante a emergência de saúde pública da COVID-19. Requerente: Partido da Social Democracia Brasileira. Relatora: Min. Rosa Weber, 17 de novembro de 2020.. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345022779&ext=.pdf. Acesso em: 4 mar. 2026.

COMMITTEE ON THE RIGHTS OF THE CHILD. *Comentário Geral nº 25 (2021) sobre os direitos das crianças em relação ao ambiente digital*. Genebra: Organização das Nações Unidas, 2021. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/04/comentario-geral-n-25-2021.pdf . Acesso em: 27 mar. 2026.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo ... [et al.] (coord.). Tratado de proteção de dados pessoais. In WIMMER, Miriam. Os desafios do enforcement da LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. Rio de Janeiro: Forense, 2021, p. 386.

DONEDA, Danilo; ZANATTA, Rafael A. F. Personality rights in Brazilian data protection law: a historical perspective. In: Personality and data protection rights on the internet: Brazilian and German approaches. Cham: Springer International Publishing, 2022. p. 35-53.

(2) Levantamento e avaliação das contribuições recebidas pelo GT2[27]

1. Panorama do *Corpus*

Para fins de elaborar o presente relatório com as devidas contribuições à ANPD, o GT2 do CNPD conduziu, entre dezembro de 2025 e janeiro de 2026, um ciclo de escuta multissetorial inédito sobre proteção de dados de crianças e adolescentes no Brasil. O resultado é uma singela Base de Dados que reúne perspectivas dos diferentes setores que responderam ao chamado do GT2 em torno do tema e que tem o condão de promover oportunidades concretas para pesquisas e análises futuras sobre esse campo em formação.

Celebramos a diversidade do que foi reunido: uma atuante gama de organizações da sociedade civil, pesquisadoras e pesquisadores acadêmicos com trajetórias de referência, representantes do sistema de justiça, empresas e associações representativas do setor privado, além de representantes da própria ANPD. Juntos, contribuíram para uma amostragem qualificada do estado do debate em prol do melhor interesse de crianças e adolescentes.

Quem participou

Setor	Entrevistados	Contribuições escritas	Total
Sociedade Civil	1	12 organizações	13
Academia	5	4 grupos de pesquisa	9
Setor Privado	4	5 empresas e associações	9
Setor Público / ANPD	3	—	3
Sistema de Justiça	3	—	3
Total	14	21	35

As entrevistas foram conduzidas em cinco sessões temáticas e reuniram especialistas selecionados e convidados pelo critério de diversidade multissetorial e expertise temática. As contribuições escritas foram submetidas também em resposta a convite, nesse caso com *template* padronizado, orientado pelos eixos ‘diagnóstico’ e ‘recomendações’.

[27] A contribuição deste capítulo do relatório foi liderada pelo Conselheiro Alexandre Boava, que contou com a pesquisa e redação de Emanuella Halfeld do Instituto Alana e de Valéria Krabzas do Núcleo de Estudos Avançados do 3º Setor e do Grupo de Pesquisa Comunidata.

Nas notas de rodapé desta análise, foram incluídas referências da fonte da informação da qual a informação foi retirada, lastreada na base de dados montada para subsidiar este relatório (**ANEXO I - Banco de Teses**). A Coluna “A” da base de dados, denominada “ID”, atribui um identificador único para cada desafio ou recomendação identificada, e permite que uma tese exposta neste documento seja identificada a partir de sua fonte de origem, seja ela a Ata das Escutas (**ANEXO II**) ou as contribuições escritas recebidas (**ANEXO III)**.

191 teses, 11 categorias

Para fins de sistematização dessa colheita, foram identificadas 191 teses, 92 desafios e 99 recomendações, que foram agrupadas em 11 categorias temáticas. A proporção entre desafios e recomendações em cada categoria revela onde o debate tem diagnóstico robusto e propostas maduras, bem como onde ainda está sendo elaborado.

191	92	99
teses extraídas	desafios identificados	recomendações formuladas

Cód.	Categoria	Desafios	Recomend.	Total
C5	Normatização e Lacunas	39	23	62
C1	Aferição Etária	23	19	42
C3	IA Generativa e Algoritmos	20	9	29
C7	Governança Institucional	7	20	27
C2	Proteção por Design	10	15	25
C11	Saúde, Desenvolvimento e Bem-estar	19	6	25
C6	Fiscalização e Enforcement	6	17	23
C9	Discriminação e Interseccionalidade	11	12	23
C10	Educação e Conscientização	8	14	22
C4	Exploração Sexual Digital	7	8	15
C8	Fluxo de Denúncias e Responsabilização	6	8	14

C5 — Normatização e Lacunas

39	23	62
desafios	recomendações	total

A LGPD existe. O ECA existe. O CDC existe. O que ainda está sendo construído é a regulamentação que torna esses marcos vivos no cotidiano de crianças e adolescentes — e que os articula como um verdadeiro sistema de proteção integral. Enquanto esse espaço não é preenchido por regulamentação, é preenchido pela realidade: dados coletados por brinquedos conectados, perfis criados em aplicativos educacionais sem consentimento, rastros digitais que seguem a criança da creche à adolescência.

Normatização e Lacunas concentra 62 teses — o dobro da segunda categoria. O dado não é crítica ao estado da lei: é o retrato da urgência construtiva do debate. O campo quer regulamentação. Sabe que ela precisa ser responsiva à velocidade das transformações tecnológicas e à diversidade de contextos e infâncias brasileiras.

Destaques do diagnóstico

- Escolas operam como controladoras de dados de crianças sem obrigações claras — apps educacionais entram sem RIPD, DPO ou consentimento parental específico[28]
- Exceções do Art. 4º — doméstica, jornalística, acadêmica, segurança pública — criam zonas sem proteção regulatória para crianças[29]
- Nascituro e adolescente emancipado estão no limbo regulatório[30]
- Memória digital e *sharenting* sem regime regulatório claro — impactos psicológicos de longo prazo não contemplados[31]

Uma reflexão que atravessa o corpus: como construir governança regulatória que atenda tanto aos tempos das demandas territoriais quanto à diversidade de contextos do Brasil? Crianças de 4 anos, adolescentes de 16, famílias periféricas sem letramento digital e escolas públicas com tablets por aluno não podem ser tratados pela mesma régua. Essa pergunta conecta Normatização com Participação.

[28] Plataforma 12, Childhood Brasil, Giselle Santos — T036, T135, T158
[29] Infinis/FJLS — T119, T120, T121, T122
[30] UFRJ — T172
[31] CMDI, Infinis/FJLS, Recria — T050, T119, T142

Onde há alguma convergência

- Necessidade de regulamentação que articule LGPD, ECA, ECA Digital e CDC como sistema coerente de proteção integral — posição compartilhada por todos os setores
- Crianças e adolescentes devem ser tratados de forma graduada por faixa etária, não como grupo homogêneo[32]
- Privacy e Safety by Design como padrão, não opção — a proteção não pode depender de configurações complexas feitas pelos responsáveis[33]

Alguns destaques de posições

- IDEC e OAB/SP defendem vedação expressa do legítimo interesse para fins comerciais com dados de crianças.
- CMDI e Family Talks argumentam que há um problema de ausência de critérios claros — e que vedações amplas criam problemas de insegurança jurídica.
- Conselho Digital defendeu que o mesmo bloqueio para uma criança de 8 anos não serve para adolescente de 16 — a abordagem unificada prejudica tanto a proteção quanto a autonomia.
- ESA e Meta propõem orientações voluntárias; Geledés e Plataforma 12 pedem regras específicas com sanções rigorosas[34].

Panorama de recomendações (lista não exaustiva, ver tabela)

- Publicar diretrizes de harmonização entre LGPD e ECA Digital com atribuições claras por órgão e por etapa[35]
- Consolidar critérios de assentimento progressivo por faixa etária — com reflexos no consentimento parental e na autonomia do adolescente[36]
- Publicar Nota Técnica sobre enquadramento dos arts. 4º e 14 para melhor compreensão do tratamento de dados no melhor interesse da criança e do adolescente — com orientações para escolas, pesquisadores e imprensa[37]
- Estabelecer direito à desindexação e ao esquecimento para conteúdos publicados durante a infância[38]
- Proibir publicidade comportamental por perfilamento de crianças, incluindo perfilamento indireto via contas de adultos[39]
- Obrigar DPO e consentimento parental específico em escolas antes de qualquer cadastro em sistema de terceiro[40]

---

[32]CDR, CMDI, OAB/SP, Conselho Digital, Recria, ANPD — T048, T060, T082, T100, T141, T155, T169
[33] Childhood Brasil, Instituto TecKids, CMDI — T046 , T108, T059
[34]IDEC, OAB/SP, CMDI, Family Talks, ESA, Meta, Geledés, Plataforma 12 — T067, T099, T047, T076, T140
[35]Childhood Brasil — T042
[36]CMDI, Instituto da Hora — T054, T116
[37]Infinis/FJLS — T121, T124
[38]CMDI, CFJ/USP — T058, T175
[39]Plataforma 12, Family Talks — T085, T140
[40]Plataforma 12 — T138

23	19	42
desafios	recomendações	total

Aferição etária é o tema com maior produção de recomendações técnicas no corpus: 19 propostas formuladas por diferentes setores. O que está em aberto não é apenas a técnica em si, mas a estrutura de governança ao redor dela: quem certifica, quem audita, como se garante a participação cívica e a responsabilização democrática dos mecanismos escolhidos.

Onde há alguma convergência

- Autodeclaração de idade isolada é insuficiente — consenso multissetorial que atravessa sociedade civil, setor privado e academia.
- Verificação não pode se tornar pretexto para vigilância massiva ou coleta excessiva de dados.
- Não existe ‘bala de prata’ — abordagem em camadas é o caminho com maior aceitação transversal[41].

Onde há tensão

Posição	Quem defende	Argumento central
Prova de conhecimento zero / tokens anônimos	CDR	Verificar sem identificar — identidade não precisa ser revelada para confirmar faixa etária
CPF como mecanismo a partir do argumento da recusa ao reconhecimento facial	Geledés	Mecanismo estatal existente, menos sujeito a vazamentos biométricos, que podem acarretar riscos para toda vida, incluindo geração de imagens de abuso e exploração sexual
Centralização no SO/App Store	Meta	Uma API de sinal de idade resolve para 100% dos apps sem coleta redundante
Abordagem em camadas por risco	Data Privacy Brasil, Yoti, ESA, Conselho Digital	Combinar estimativa, inferência e verificação conforme o risco do serviço

[41] Data Privacy Brasil, ESA, Yoti, Conselho Digital — T074, T147

O paradoxo regulatório é real: verificar a idade de uma criança ou adolescentes exige usar seus dados. A proteção não pode se transformar em nova forma de exposição. A calibração é o desafio central — não a escolha de uma tecnologia.

Destaques do diagnóstico

- Sistemas biométricos apresentam taxas de erro significativamente maiores para pessoas de pele escura — 90,5% das pessoas presas por reconhecimento facial no Brasil são negras[42]
- 99% dos apps sem capacidade técnica para implementar verificação robusta — barreiras desproporcionais para pequenos desenvolvedores[43]
- Biometria em estádios cadastrou cerca de 30 mil crianças de 2 a 14 anos em um único clube — sem base legal, sem avaliação de impacto[44]

Panorama de recomendações (lista não exaustiva, ver tabela)

- Publicar taxonomia distinguindo *age verification, age estimation* e *age inference* — com abordagem em camadas por nível de risco[45]
- Desenvolver API pública de sinal de idade com retorno binário — modelo em construção na Europa[46]
- Adotar prova de conhecimento zero — confirmar faixa etária sem revelar identidade[47]
- Impor moratória do reconhecimento facial em escolas até comprovação de equidade demográfica por auditoria independente[48]
- Proibir biometria de crianças e adolescentes de até 16 anos em estádios — com exclusão imediata dos dados já coletados[49]
- Separar por norma os agentes que constroem e os que usam mecanismos de aferição — evitar captura e conflito de interesse[50]
- Garantir via de verificação de consentimento parental não digital — para não excluir famílias periféricas[51]

O próximo passo indicado não é apenas técnico — é de governança. Quem certifica os mecanismos de aferição? Quem audita? Como a sociedade civil e as famílias participam? Essa estrutura de responsabilização democrática é o que ainda precisa ser construído.

[42] Grupo ASPAS/UFRPE, Instituto da Hora — T092, T110
[43] Alandar — T165
[44] Plataforma 12 — T136
[45] Data Privacy Brasil — T074
[46] Alandar — T166
[47] CDR — T008
[48] Instituto da Hora — T114
[49] Plataforma 12 — T139
[50] CDR — T015
[51] Instituto da Hora — T117

C3 — IA Generativa e Algoritmos

20	9	29
desafios	recomendações	total

IA generativa representa risco urgente e específico para crianças e adolescentes — diagnóstico compartilhado entre academia, sociedade civil e sistema de justiça. Há uma corrente clara de vedação de ferramentas como aplicativos *nudify* reunindo atores de setores distintos em torno de uma posição comum. O gap entre desafios (20) e recomendações (9) não é omissão, mas convite ao regulador para construir doutrina onde o debate ainda está em formação.

Onde há alguma convergência

- IA generativa produz deepfakes sexuais de crianças em escala — a SaferNet registrou 49.336 denúncias de abuso sexual infantil no primeiro semestre de 2025.
- Aplicativos *nudify* não têm utilidade social legítima — posição convergente de FGV, Geledés, Instituto da Hora e Childhood Brasil[52].
- Dados de crianças não devem ser usados como insumo para treinamento de IA sem regulação específica[53].

Onde há tensão

- FGV e Instituto da Hora defendem vedação categórica de *nudify*; Conselho Digital e ESA, de forma geral, defendem abordagem por risco sem vedação de funcionalidades específicas.
- Responsabilização de buscadores por facilitar acesso a ferramentas abusivas — proposta de Yasmin Curzi, sobre a qual não foi encontrada posição do setor privado no corpus da pesquisa[54].

Destaques do diagnóstico (lista não exaustiva, ver tabela)

- 65% das crianças brasileiras de 9 a 17 anos já usaram IA generativa — inclusive para falar sobre emoções e buscar apoio emocional[55]
- AI *companions* incentivam vínculos emocionais artificiais com crianças e coletam dados sensíveis comportamentais[56]

[52]FGV, Geledés, Instituto da Hora, Childhood Brasil — T040, T087, T090, T170, T171
[53]OAB/SP, Instituto da Hora — T064, T069, T113
[54]FGV/Yasmin Curzi — T170
[55]Childhood Brasil — T034
[56]Grupo ASPAS/UFRPE — T094

- Anti-negritude é a lógica padrão dos sistemas digitais — crianças negras são hipervigiadas e hiperexpostas por algoritmos de recomendação[57]
- 81% dos apps infantis usam rastreadores de dados e 19% têm classificações etárias inconsistentes — falha crítica de Privacy by Design[58]

Panorama de recomendações (lista não exaustiva, ver tabela)

Vedação de *nudify* e proteção contra exploração sexual digital

- Vedar aplicativos *nudify* — sem utilidade social legítima que justifique sua existência[59]; posição que pode caracterizar um conflito com tese de regulação não proibitiva da tecnologia, mas dos usos dela, apresentada por representantes do setor privado.
- Criar classificação de ferramentas geradoras de imagem por nível de risco[60].
- Criminalizar criação de imagens de abuso sexual infantil geradas por IA[61].
- Reforçar a integração do Brasil a redes internacionais de detecção e remoção de material de abuso sexual infantil online[62].

Regulação técnica e design responsável

- Obrigar marca d'água em conteúdos gerados por IA para proteger imagem de crianças e adolescentes[63].
- Exigir filtros e autenticação de identidade em plataformas de IA generativa de imagem e vídeo[64].
- Regular uso de dados de crianças como insumo para treinamento de IA — filtros técnicos obrigatórios[65].
- Exigir segurança por *design* em plataformas de IA usadas como apoio emocional ou terapêutico[66].

C11 — Saúde, Desenvolvimento e Bem-estar

19	6	25
desafios	recomendações	total

[57]Grupo ASPAS/UFRPE — T105
[58]Instituto Teckids — T109
[59]FGV/Yasmin Curzi — T170
[60]FGV — T171
[61]Childhood Brasil — T040
[62]Childhood Brasil — T043
[63]Childhood Brasil — T039
[64]Geledés — T090
[65]Instituto da Hora — T113
[66]Childhood Brasil — T041

Saúde e desenvolvimento é a categoria com maior desequilíbrio entre diagnóstico e proposta: 19 desafios, 6 recomendações. Isso não é ausência de propostas, mas o retrato de um campo que produziu evidências científicas robustas e que ainda está construindo a ponte entre diagnóstico e instrumento regulatório.

Destaques do diagnóstico

- Desenvolvimento incompleto do córtex pré-frontal torna crianças e adolescentes estruturalmente mais vulneráveis a algoritmos de engajamento — não é falha comportamental, é biologia[67].
- 28% das crianças brasileiras de 9 a 17 anos começaram a usar internet antes dos 6 anos — dado de saúde pública[68].
- OMS reconhece Hazardous Gaming como categoria diagnóstica na CID-11 — uso problemático de telas causa danos em quatro grandes áreas de saúde[69].
- Criança planejou suicídio com apoio de IA generativa — risco terapêutico real e documentado[70].
- Metadados escolares persistem ao longo da vida — uma palavra registrada num sistema pode seguir a criança ou e adolescente para sempre[71].
- *Sharenting* por pais e escolas viola direito à imagem e à privacidade — casos de judicialização crescentes no Brasil[72]

Recomendações formuladas (lista não exaustiva, ver tabela)

- Exigir segurança por *design* em plataformas de IA usadas como consulta emocional ou terapêutica[73]
- Criar Diretriz Nacional *anti-sharenting* com checklists e modelos de pedido de remoção para famílias[74]
- Estabelecer direito ao esquecimento e desindexação para conteúdos da infância[75]
- Integrar proteção digital à atenção primária à saúde da infância nos órgãos governamentais[76]

> *O campo indica um horizonte regulatório ainda pouco explorado: a saúde mental de crianças e adolescentes como critério de design — não apenas como consequência a ser remediada. A conexão entre proteção de dados e proteção*

[67]CEIIAS, Instituto Teckids, CEIIAS — T016, T129
[68]CEIIAS — T017
[69]CEIIAS — T019, T022
[70]Childhood Brasil — T035
[71]Giselle Santos — T159
[72]CMDI, CEIIAS, Recria — T018, T050, T142
[73]Childhood Brasil — T041
[74]Infinis/FJLS — T125
[75]CMDI — T058
[76]CEIIAS — T030

biopsicossocial está colocada. O próximo passo é garantir linguagem regulatória, participativa e responsável, para percorrê-la.

C6 — Fiscalização e *Enforcement*

6	17	23
desafios	recomendações	total

A LGPD vigora desde 2020. O ECA Digital acabou de entrar em vigor, em março de 2026. O *corpus* aponta que a lei ainda não se consolidou de forma plena para crianças e adolescentes, não por falta de instrumentos jurídicos, mas por falta de fiscalização ativa, de cultura de proteção de dados que chegue aos territórios e de dosimetria que efetivamente desincentive o descuido.

Onde há alguma convergência

- LGPD e ECA Digital existem mas *enforcement* ainda não se consolidou — diagnóstico compartilhado por todos os setores.
- Em relatório prévio produzido pelo GT Educação deste mesmo biênio do CNPD, foi recomendado, por um grupo multissetorial de conselheiros, a intensificação da fiscalização de grandes plataformas digitais com provável acesso, atratividade ou impacto relevante sobre crianças e adolescentes, aspecto que reflete-se em parte das contribuições da sociedade civil, academia e Sistema de Justiça recebidos (**ANEXO IV - Resumo das Recomendações do GT Educação para DCAs e PPDs**)

Onde há tensão

- ESA e Meta preferem orientações voluntárias e conformidade por incentivo; OAB/SP, Geledés e Plataforma 12 exigem sanções rigorosas e auditoria obrigatória[77]. Por sua vez, CDR pede o reconhecimento da presunção de violação quando tratamento de dados de crianças resultar em dano ou risco demonstrado[78].

Recomendações formuladas

- Fiscalização ativa e setorizada com agendas periódicas — sem depender exclusivamente de denúncias[79].

[77] ESA, Meta, OAB/SP, Geledés, Plataforma 12 — T066, T068, T075
[78] OAB/SP — T066
[79] OAB/SP — T068

- Protocolo de Supervisão por Risco com padrão mínimo de evidências de conformidade para plataformas com dados de crianças[80].
- Estender fiscalização à presença de crianças em plataformas generalistas — não apenas em versões nominalmente infantis[81].
- Criar CRIA — Relatório de Impacto sobre Direitos de Crianças e Adolescentes — em diálogo com a UNICEF[82].
- Proibir dark patterns em interfaces para crianças com auditoria periódica por especialistas independentes[83].

C7 — Governança Institucional

7	20	27
desafios	recomendações	total

Governança é a categoria com maior desequilíbrio positivo do *corpus* — quase três recomendações para cada desafio. O que o debate pede, em essência, é que a ANPD não aja sozinha. O convite é à articulação com uma rede que já existe, que já atua e que já tem acúmulo.

Onde há alguma convergência

- ANPD não deve agir isoladamente — articulação com SGD, CONANDA e sociedade civil é posição compartilhada transversalmente.
- Guia de conceitos gerais do ECA Digital é prioridade antes da regulamentação técnica[84].

Onde há tensão

- Parte das contribuições projeta na ANPD capacidade de coordenação que ainda está sendo construída — Fabrício Guimarães (ANPD) nomeou o risco: 'meu receio é achar que a ANPD virá para resolver crianças e adolescentes — isso é subestimar a rede de proteção que vem atuando no tema'[85].
- Centralização regulatória *versus* articulação em rede — onde fica o protagonismo é uma questão ainda em aberto.

Recomendações — normatização e orientação

[80]Data Privacy Brasil — T075
[81]Data Privacy Brasil — T163
[82]UFRJ — T173
[83]Instituto da Hora — T115
[84]ANPD/Rodrigo Santana — T156
[85]ANPD/Fabrício Guimarães — T154

- Publicar Guia de conceitos gerais do ECA Digital antes de avançar na regulamentação técnica[86].
- Criar reconhecimento regulatório específico para dados tratados por organizações da sociedade civil com finalidade de defesa de direitos[87].
- Regulamentar direito à explicabilidade algorítmica por faixa etária — com linguagem adaptada a 6-9, 10-12 e 13-17 anos[88].

Recomendações — cooperação com SGD e sociedade civil

- Mapear e dialogar formalmente com CONANDA, MDHC e comitê intersetorial antes de agir[89].
- Formar grupo consultivo intersetorial com especialistas em infância e adolescência[90].
- Fomentar parcerias entre empresas de tecnologia, big tech e sociedade civil para implementação conjunta do ECA Digital e da LGPD[91].
- Publicar guia conjunto ANPD–CONANDA–Abraji para jornalismo com crianças[92].
- Incorporar perspectiva interseccional e fomentar pesquisas nacionais sobre impacto de IA em crianças negras, periféricas e com deficiência[93].

Para onde vai o debate

A leitura transversal das 191 teses aponta quatro eixos estruturantes — não como lista de tarefas, mas como horizontes de um sistema de proteção que ainda está sendo construído. Cada um exige atores e atrizes diferentes, tempos diferentes, e a compreensão de que proteção de dados de crianças e adolescentes é, antes de tudo, dimensão da proteção integral.

Normatização

A lei deixa espaço. Enquanto esse espaço não é preenchido por regulamentação, é preenchido pela realidade. Tecnologias já entraram em escolas, brinquedos e lares antes de qualquer marco regulatório específico estar consolidado. O horizonte não é corrigir uma lei — é fazer com que LGPD, ECA, ECA Digital e CDC funcionem como um sistema vivo de proteção integral, responsivo à velocidade das transformações tecnológicas e à diversidade de

[86]ANPD/Rodrigo Santana — T156
[87]CMDI — T057
[88]Instituto da Hora — T116
[89]ANPD/Lucas Borges — T157
[90]CEIIAS — T029
[91]CEIIAS — T031
[92]Infinis/FJLS — T126
[93]Instituto da Hora — T118

contextos e infâncias brasileiras. A regulamentação em construção é, pois, um ato de cuidado.

Responsabilidade

A LGPD vigora. O ECA Digital entrou em vigor. O que o *corpus* pede — com urgência e clareza — é que *enforcement* aconteça de forma consistente. Cultura de proteção de dados não se constrói só com norma: constrói-se com fiscalização ativa, com dosimetria que desincentiva o descuido, com responsabilização que opera independentemente de denúncia prévia. O ECA Digital elevou o teto de sanção para 10% do faturamento. O convite é para que os instrumentos disponíveis sejam usados quando há violação — com fundamentação, articulação e integração com os demais marcos do sistema de proteção integral. Há um cenário identificado de descumprimento sistemático de normas, dano e risco gerado para futuras gerações, tratando-se da responsabilização pela violação da legislação elemento constitutivo de uma cultura de proteção.

Participação

Proteção de dados de crianças e adolescentes não se faz só de regulação técnica. A Lei da Escuta Protegida, o SGD, os Conselhos Tutelares, as escolas, as famílias: todos são parte do sistema. Um fluxo de denúncias que funcione como o PROCON, um letramento que chegue aos territórios, uma ANPD que dialogue com o CONANDA antes de agir: essas são as dimensões participativas que o corpus pede. Participação é tanto das crianças e adolescentes como sujeitos de direitos quanto das redes que os protegem no cotidiano — e que já estão no campo, construindo proteção integral muito antes do ECA Digital.

Continuidade ECA/SGD

A ANPD não inaugura esse campo. Chega a uma rede que tem décadas de acúmulo — doutrina da proteção integral, Sistema de Garantia de Direitos, mecanismos de escuta e participação construídos ao longo do ECA e agora reforçados pelo ECA Digital. O convite é à articulação, não à sobreposição. O que está sendo construído agora, regulação de dados, aferição etária, governança de IA, tem mais força quando se apoia no que já existe.

A pesquisa produzida pelo GT2 apoia um debate múltiplo em prol do melhor interesse das crianças e dos adolescentes: reuniu participantes representantes de diversos setores, em uma perspectiva multissetorial, e transformou perspectivas diversas em uma amostragem qualificada que pode subsidiar pesquisas, políticas e regulamentações futuras. O levantamento foi feito. A construção continua.

(3) O caso da Autoridade Italiana na implementação regulatória[94]

1. Introdução

O presente relatório tem como objetivo apoiar a atuação da Agência Nacional de Proteção de Dados (ANPD) na implementação das regras de proteção de dados pessoais de crianças e adolescentes, com foco na identificação de caminhos institucionais e regulatórios que contribuam para o fortalecimento do *enforcement*.

Parte-se do entendimento de que a efetividade da proteção reforçada prevista na Lei Geral de Proteção de Dados (LGPD), em especial no seu art. 14, depende não apenas da existência de normas, mas de estratégias institucionais de aplicação, fiscalização, prevenção e responsabilização, capazes de responder às especificidades da relação entre crianças, adolescentes e os produtos e serviços de tecnologia amplamente utilizados por esse grupo hipervulnerável.

Nesse contexto, a efetividade da proteção jurídica depende da capacidade institucional de operacionalizar o *enforcement* de forma consistente, contínua e tecnicamente fundamentada. O debate desloca-se, assim, do plano normativo para o plano da aplicação prática das normas, exigindo o fortalecimento de instrumentos de monitoramento, fiscalização, prevenção e responsabilização capazes de responder às especificidades da relação entre crianças, adolescentes e os produtos e serviços digitais que estruturam sua experiência contemporânea.

Por isso, o eixo central de análise do presente capítulo consiste no exame de casos concretos de *enforcement* conduzidos pelo *Garante per la protezione dei dati personali* (doravante "Garante"), autoridade italiana reconhecida por sua atuação firme e inovadora na proteção de dados de crianças e adolescentes, especialmente em contextos envolvendo plataformas digitais e sistemas de inteligência artificial. Esses casos, que envolvem serviços amplamente utilizados por crianças e adolescentes, como *chatbots*, sistemas de IA generativa e redes sociais, permitem observar, de forma concreta, como instrumentos regulatórios são mobilizados para enfrentar riscos estruturais no ambiente digital.

A escolha do contexto italiano se justifica tanto pela relevância temática quanto pela proximidade institucional com o contexto brasileiro. Assim como a ANPD, o Garante atua em relação a empresas globais cujos modelos de negócio são definidos fora do território nacional, enfrentando desafios relacionados à verificação etária, ao design de serviços digitais e à exploração econômica de dados pessoais. Sua atuação recente, especialmente a partir de 2020, revela um padrão de *enforcement* caracterizado pela adoção de instrumentos de fiscalização diversificados, por meio de medidas cautelares imediatas, imposição de obrigações técnicas detalhadas, monitoramento contínuo e aplicação de sanções estruturais, além do fomento a práticas educativas e formativas.

A partir da análise desses casos, o relatório busca identificar padrões regulatórios, estratégias de intervenção e combinações de instrumentos que possam informar o fortalecimento da atuação da ANPD. O objetivo não é apenas

[94] A escrita deste capítulo do relatório foi liderada pela **Conselheira Isabella Henriques**, que contou com a colaboração de Júlia Mendonça e Luíse Menezes do Instituto Alana.

descrever experiências internacionais, mas extrair aprendizados concretos sobre como o *enforcement* pode ser estruturado para garantir a efetiva proteção de crianças e adolescentes no ambiente digital.

2. Metodologia

A análise adota abordagem qualitativa, de caráter documental e analítico, orientada à compreensão de como o *enforcement* da proteção de dados pessoais de crianças e adolescentes pode ser efetivamente operacionalizado.

A escolha do enfoque no fortalecimento do *enforcement* foi informada por insumos técnicos provenientes das entrevistas com especialistas já realizadas no âmbito do atual GT2 do CNPD ("Proteção de Dados de Crianças e Adolescentes"), bem como de análises prévias realizadas pelo GT1 "Educação e Capacitação em Proteção de Dados"[95], nas quais emergiram, de forma recorrente, referências à necessidade de aprimoramento do *enforcement* brasileiro para garantia efetiva da proteção normativa na LGPD[96].

A partir desse diagnóstico, o relatório estrutura sua análise com base no exame de casos concretos de atuação regulatória, privilegiando a observação de como instrumentos jurídicos são mobilizados na prática para enfrentar riscos associados ao tratamento de dados pessoais de crianças e adolescentes.

Como eixo central da análise comparada, foi selecionada a atuação do *Garante per la protezione dei dati personali*[97]*,* autoridade italiana de proteção de dados pessoais. A escolha se justifica por sua atuação consistente e, em diversos casos, mais incisiva no uso de instrumentos de *enforcement,* especialmente em contextos envolvendo plataformas digitais de grande escala e tecnologias emergentes, como sistemas de inteligência artificial, redes sociais e ambientes digitais imersivos. Além da relevância temática, a experiência italiana apresenta proximidade institucional com o contexto brasileiro. Assim como a ANPD, o Garante atua sobre agentes econômicos globais cujos modelos de negócio são definidos fora do território nacional, demandando estratégias regulatórias que combinem medidas cautelares, ordens de adequação, sanções e mecanismos de acompanhamento contínuo. Também se observa, em ambos os contextos, a necessidade de articulação entre fiscalização, orientação pública e iniciativas de caráter educativo.

O recorte temporal adotado, a partir de 2020, permite capturar um período de intensificação do uso de plataformas digitais por crianças e adolescentes, bem como

---

[95] Coordenado pelo Conselheiro Rodrigo Borges Valadão, com a participação dos Conselheiros Alexandre Zago Boava, Ana Paula Moraes Canto de Lima, Gabrielle Bezerra Sales Sarlet, Gisela Carvalho de Freitas, Isabella Vieira Machado Henriques e Tiago Lopes de Aguiar. Contou, também, com a participação de Emanuella Halfeld e Renato Godoy, do Instituto Alana, como apoiadores técnicos.

[96] Elementos que foram apresentados na frente anterior do relatório "Proteção de Dados Pessoais de Crianças e Adolescentes no Brasil: desafios e recomendações a partir de diálogos com setores da sociedade brasileira"

[97] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Garante per la protezione dei dati personali. [Itália], 2026. Disponível em: https://www.garanteprivacy.it/. Acesso em: 23 abr. 2026.

de consolidação de debates regulatórios centrais para o *enforcement* da proteção de pessoas em desenvolvimento, incluindo verificação etária, design de serviços digitais e exploração econômica de dados pessoais.

No recorte temporal adotado, a partir de 2020, foram levantados e analisados documentos, decisões e provimentos relativos a 38 casos envolvendo o tratamento de dados pessoais de crianças e adolescentes no contexto italiano. Esse volume de casos permitiu identificar padrões consistentes de atuação regulatória ao longo do tempo. Observou-se, ainda, um paralelo relevante com o contexto brasileiro: no mesmo período, segundo dados do painel de fiscalização da ANPD[98], a autoridade iniciou 30 procedimentos relacionados ao tratamento de dados de crianças e adolescentes, incluindo atividades de monitoramento, procedimentos fiscalizatórios, preparatórios e sancionadores. Esse dado reforça a pertinência da análise comparada, ao evidenciar a centralidade do tema em ambas as jurisdições.

A partir desse conjunto, foi realizada uma seleção analítica de casos, com o objetivo de aprofundar a compreensão dos instrumentos de *enforcement*. Foram priorizados dois casos principais, representativos de diferentes setores de atuação, o que permite observar como estratégias regulatórias são mobilizadas em contextos distintos, ampliando a capacidade analítica do relatório.

Outros casos de elevada relevância pública, como os envolvendo TikTok/ByteDance[99] e OpenAI/ChatGPT[100], também foram considerados ao longo da análise, especialmente para identificação de padrões e instrumentos específicos de *enforcement*. No caso do TikTok, destaca-se a adoção de medida cautelar de ampla repercussão, consistente na limitação integral do tratamento de dados em território italiano, com caráter urgente, destinada a interromper riscos e prevenir novas violações aos direitos de crianças e adolescentes.[101]. Contudo, a existência de procedimento fiscalizatório e sancionador com relação ao mesmo agente regulado atualmente em curso no Brasil, justificou a seleção de outros casos para análise, de modo a preservar a utilidade analítica do relatório para o contexto nacional.

Já no caso envolvendo a Open AI/ChatGPT, a autoridade determinou a realização de uma campanha institucional obrigatória de comunicação, com duração de seis meses, a ser veiculada em múltiplos meios, incluindo rádio, televisão,

---

[98] Agência Nacional de Proteção de Dados. Painel da fiscalização da ANPD. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiYmZlMmM5YzItMzQ1MS00N2E2LThhYTctMTYwZTliOGJmZWM0IiwidCI6IjVhYmEwNGExLWY4NjMtNGI1Ni04MTdkLTQ0MjkxYzkwZDFiOCJ9. Acesso em: 4 maio 2026.

[99] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 22 de janeiro de 2021 [9524194] Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524194. Acesso em 31 mar. 2026.

[100] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. COMUNICATO STAMPA - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432. Acesso em 22 abr. 2026.

[101] LA REPUBBLICA. Antonella, morta per sfida su TikTok. La sorellina: "Era il gioco dell'asfissia". Disponível em: https://www.repubblica.it/cronaca/2021/01/22/news/antonella_morta_per_sfida_su_tiktok_la_sorellina_era_il_gioco_dell_asfissia_-283731985/. Acesso em 16 abr. 2026.

imprensa escrita e internet[102]. O conteúdo da campanha, sujeito à aprovação prévia do Garante, deve esclarecer o funcionamento da plataforma, explicar as práticas de coleta e uso de dados pessoais de usuários e não usuários para o treinamento da IA, bem como informar, de forma acessível, os direitos dos titulares, especialmente os direitos de oposição, retificação e exclusão, com vistas a viabilizar seu exercício efetivo[103]. Esse tipo de medida evidencia a ampliação do escopo do *enforcement* para além dos mecanismos tradicionais de sanção, incorporando estratégias voltadas à conscientização pública e ao fortalecimento da capacidade informacional da sociedade.

3. Casos selecionados e Quadro-Resumo

A presente seção analisa dois casos emblemáticos de *enforcement* da proteção de dados pessoais de crianças e adolescentes conduzidos pelo *Garante per la protezione dei dati personali* entre 2020 e 2025. Os casos selecionados - Replika (Luka Inc.) e Corte Suprema Di Cassazione/Sentenzeweb - ilustram estratégias regulatórias concretas para a efetivação da proteção reforçada prevista no Regulamento Geral de Proteção de Dados (GDPR).

A análise adota uma matriz analítica estruturada em quatro eixos integrados: (1) Identificação do Produto/Serviço, (2) Infrações Identificadas, (3) Instrumentos de *enforcement* adotados pela Autoridade, e (4) Contexto nacional e atuação da ANPD. Essa abordagem permite identificar padrões regulatórios, combinações de instrumentos de implementação e aprendizados transferíveis ao contexto brasileiro, com vistas ao fortalecimento da atuação da Agência Nacional de Proteção de Dados (ANPD).

Eixo Analítico	Replika / Luka Inc.	Corte Suprema Di Cassazione/Sentenzeweb
Produto/ Serviço	Chatbot de IA generativa apresentado como 'amigo virtual' e 'parceiro romântico'. Público declarado: adultos. Público real: amplamente acessado por adolescentes e crianças.	Portal público de consulta de decisões judiciais da Suprema Corte italiana (SentenzeWeb), com instrumento de busca por palavras-chave, livremente acessível na internet.

[102] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. COMUNICATO STAMPA - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432. Acesso em 22 abr. 2026.

[103] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. COMUNICATO STAMPA - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432. Acesso em 22 abr. 2026.

Eixo Analítico	Replika / Luka Inc.	Corte Suprema Di Cassazione/Sentenzeweb
Infrações observadas	Inexistência de mecanismos de verificação de idade; exposição de crianças e adolescentes a conteúdos sexualizados e emocionalmente perturbadores; ausência de identificação granular das bases jurídicas (inclusive para treinamento do LLM); opacidade informacional grave; falha em *privacy by design* e minimização.	Difusão ilícita de dados sensíveis de saúde (HIV, doenças oncológicas), dados de vítimas de violência sexual e dados de crianças e adolescentes em decisões judiciais pesquisáveis por nome, patologia ou palavra-chave; ausência de mecanismos técnicos eficazes de restrição; falha em *privacy by design* e no princípio de minimização e integridade e confidencialidade dos dados.
Instrumentos de *Enforcement* adotados pela Autoridade Italiana de Proteção de Dados	Limitação provisória do tratamento (fev./2023); suspensão condicional com prescrições técnicas detalhadas, incluindo *cooling-off period* e plano técnico de *age gate* (jun./2023); declaração final de ilicitude, obrigações corretivas estruturais e sanção pecuniária (abr./2025 + mai./2025).	Três inspeções de iniciativa própria (nov./2022 e mar./2023); pedido formal de informações com convite à adoção de medidas cautelares; abertura de procedimento (mar./2023); acompanhamento das medidas corretivas ao longo da instrução; advertência formal sem sanção pecuniária; *ingiunzione* de prestação de contas em prazo determinado sobre implementação das novas diretivas e do sistema de pseudonimização automática (mai./2024).
Fundamentos Jurídicos	Arts. 5º §1º 'a' e 'c', 6º, 12, 13, 24, 25 §1º GDPR (decisão final 2025). Arts. 5º, 6º, 8º, 9º, 25 GDPR (*procedimentos* de urgência 2023). Princípio do melhor interesse; *privacy by design; accountability;* proporcionalidade ao risco.	Arts. 5º §1º 'a', 'c' e 'f', 9º e 32 do GDPR; arts. 52 §5º e 2-*septies* do Código italiano de proteção de dados; proibição de difusão de dados de saúde e de dados identificativos de crianças e adolescentes em decisões judiciais.
Contexto Brasileiro (ANPD)	Sem procedimento formal identificado junto à ANPD em relação à Replika/Luka Inc. O serviço permanece acessível no Brasil sem salvaguardas equivalentes às exigidas na Itália.	Sem procedimento formal identificado junto à ANPD sobre o tema. O vazamento de dados de crianças e adolescentes oriundos de processos judiciais é um problema sistêmico no Brasil, com casos documentados envolvendo tribunais e plataformas privadas de consulta jurídica, sem resposta regulatória estruturada até o momento.

4. Caso Chatbot Replika (Luka Inc.)

O caso Replika representa uma das intervenções regulatórias mais inovadoras e estruturalmente complexas do Garante no período analisado. Envolvendo um *chatbot* baseado em inteligência artificial generativa apresentado como 'companheiro virtual' (*AI Companion*), o caso atravessou três decisões em um arco temporal de dois anos (2023–2025), consolidando um modelo regulatório que envolveu o estabelecimento de medidas, a adoção de condições técnicas progressivas a serem implementadas e o acompanhamento contínuo do seus respectivos andamentos.

O Replika, desenvolvido e operado pela empresa Luka Inc., consiste em um chatbot baseado em inteligência artificial generativa que se apresenta ao usuário sob a forma de “amigo virtual”, “parceiro romântico” ou “mentor emocional”[104]. Sua proposta central reside na oferta de interações conversacionais altamente personalizadas, orientadas ao chamado “bem-estar emocional”, com a possibilidade de construção de vínculos afetivos simulados entre o usuário e o agente artificial.

Nesse contexto, a gravidade do caso extrapolava a mera insuficiência das salvaguardas declaradas, intensificando-se em razão do modelo de negócios e da própria arquitetura do serviço. Diferentemente das plataformas digitais convencionais, a Replika opera sob uma lógica de engajamento afetivo, estruturada para simular intimidade e suporte psicológico. Essa dinâmica relacional amplia a vulnerabilidade de crianças e adolescentes ao fomentar a dependência emocional e reduzir o discernimento crítico diante de respostas automatizadas. Tal cenário expõe o público infantojuvenil a riscos severos, incluindo o contato com conteúdos de natureza sexualizada. Depreende-se, portanto, que a convergência entre falhas na governança de dados e um *design* voltado à exploração de vulnerabilidades subjetivas resulta em um perigo agravado, o que exige padrões de proteção rigorosos, em estrita observância ao melhor interesse da criança.

(a) Infrações identificadas

O Garante identificou um conjunto consistente e sistemático de violações praticadas pela Luka Inc. no contexto da operação da aplicação Replika, revelando falhas estruturais tanto na governança de dados quanto no próprio desenho do serviço.

Em primeiro lugar, destacou-se a inexistência de mecanismos efetivos de verificação etária. O processo de cadastro limitava-se à coleta de informações básicas, como nome, e-mail e gênero, sem qualquer procedimento técnico destinado à aferição da idade do usuário. Ademais, a plataforma não implementava qualquer forma de bloqueio ou restrição de acesso mesmo quando o próprio usuário declarava ter menos de 13 anos, evidenciando não apenas a ausência de controles preventivos, mas também a inexistência de respostas automatizadas a sinais explícitos de vulnerabilidade.

[104] LUKA INC. *Replika*. [S. l.], 2026. Disponível em: https://replika.com/. Acesso em: 23 abr. 2026.

No que diz respeito à proteção material de crianças e adolescentes, a Autoridade constatou a exposição desse público a conteúdos manifestamente inadequados ao seu estágio de desenvolvimento. Foram identificadas interações em que o sistema de IA fornecia respostas de cunho sexual ou emocionalmente perturbador, potencialmente prejudiciais à saúde psicológica de usuários em condição de especial vulnerabilidade, sobretudo em razão da natureza relacional e imersiva da ferramenta.

Sob a perspectiva informacional, verificou-se grave deficiência na política de privacidade, em violação ao artigo 13 do GDPR. O documento não apresentava de forma clara as finalidades do tratamento, as categorias de dados pessoais coletados nem as bases jurídicas utilizadas, o que comprometia a boa fé, transparência e inviabilizava a compreensão, inclusive pelo próprio regulador, das operações realizadas. Essa opacidade mostrava-se particularmente crítica no que se refere ao uso de dados para o treinamento dos sistemas de inteligência artificial.

O Garante também rejeitou expressamente a utilização da base legal de execução de contrato como fundamento jurídico para o tratamento de dados pessoais de crianças e adolescentes, reafirmando entendimento já consolidado em precedentes anteriores. Considerou-se que crianças não possuem capacidade civil para celebrar contratos que envolvam a disponibilização significativa de dados pessoais, o que invalidava a invocação dessa hipótese legal nesses contextos.

Por fim, a Autoridade apontou a possível ocorrência de tratamento de categorias especiais de dados pessoais (no contexto brasileiro, os chamados “dados sensíveis”), nos termos do artigo 9º do GDPR, a partir da inferência de informações sensíveis relacionadas à saúde mental e à vida afetiva dos usuários, extraídas das interações com o chatbot. Tal prática, associada à ausência de salvaguardas adequadas, agravava substancialmente o quadro de ilicitude identificado.

Em síntese, as violações então constatadas podem ser sistematizadas em quatro eixos principais: (i) ausência de verificação etária, com inexistência de mecanismos técnicos e de bloqueio, mesmo diante de autodeclaração informando tratar-se de pessoa com menos idade do que a exigida para acessar a plataforma; (ii) exposição de crianças e adolescentes a conteúdos inadequados, inclusive de natureza sexual ou psicologicamente prejudicial; (iii) opacidade informacional e ausência de base legal válida, em razão de uma política de privacidade deficiente e da inadequação da base contratual; e, por fim, (iv) violação de princípios estruturantes do GDPR, como transparência e minimização, bem como a inobservância dos deveres de proteção de dados desde a concepção e por padrão.

(b) Instrumentos de enforcement adotados pela Autoridade Italiana de proteção de dados

A atuação do *Garante* italiano no caso Replika evidenciou um modelo de *enforcement* rigoroso e proativo. Diante da gravidade dos riscos a crianças e adolescentes, a autoridade optou pela interrupção imediata do serviço. Essa medida, fundamentada no exercício direto de poderes corretivos, ocorreu sem a

precedência de ritos dialógicos ou negociais, reafirmando o caráter impositivo da proteção de dados em cenários de alto risco.

O caso ilustra um modelo de atuação em três etapas, composto por intervenção emergencial, suspensão condicionada e decisão final de caráter estrutural.

No primeiro momento, em Disposição de 2 de 2023 [9852214][105], diante da constatação de risco concreto e imediato, a autoridade adotou uma medida de limitação provisória do tratamento com fundamento no artigo 58, §2º, alínea "f", do GDPR. Na prática, isso significou a suspensão do funcionamento do serviço no território italiano. A medida teve caráter amplo e atingiu todos os usuários localizados na Itália, e não apenas crianças e adolescentes, justamente porque a ausência de mecanismos confiáveis de verificação etária tornava impossível a distinção entre públicos. Esse ponto é central para compreender a lógica de adotada, uma vez que, na dúvida sobre a extensão do risco, a autoridade opta pela máxima proteção,_suspendendo integralmente a operação até que condições mínimas de segurança sejam estabelecidas.

Em um segundo momento, na Disposição de 22 de junho de 2023 [10013893][106], ao analisar o pedido de revisão da medida, o Garante não simplesmente restabeleceu o serviço, mas condicionou qualquer eventual retomada ao cumprimento de um conjunto detalhado e tecnicamente orientado de obrigações. Dessa forma, tratou-se de uma suspensão condicional, na qual a empresa somente poderia voltar a operar mediante a demonstração concreta de adequação.

Entre as exigências impostas destacam-se a disponibilização da política de privacidade antes do cadastro, a implementação de mecanismos efetivos de verificação etária em todas as etapas de registro, a adoção de um período de resfriamento (*cooling-off*)[107] para evitar o contorno dos bloqueios mediante inserção de dados falsos, a apresentação prévia de um plano técnico de verificação etária para validação pela autoridade e a criação de ferramentas de denúncia de conteúdos inadequados. Esse conjunto de medidas revela um nível elevado de sofisticação regulatória, com foco não apenas na conformidade formal, mas na eficácia técnica das soluções implementadas.

Por fim, no terceiro momento, ao concluir o procedimento principal, o Garante proferiu decisão definitiva em Disposição de 10 de abril de 2025 [10130115][108],

---

[105] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 2 de fevereiro de 2023 [9852214]. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9852214>. Acesso em 22 abr. 2026.

[106] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 22 de junho de 2023 [10013893]. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10013893>. Acesso em 22 abr. 2026.

[107] YOU EUROPE. Right of withdrawal: a 14-day cooling-off period. Disponível em: https://europa.eu/youreurope/citizens/consumers/shopping/returns/index_en.htm#:~:text=Right%20of%20withdrawal:%20a%2014,until%20the%20next%20working%20day. Acesso em 16 abr. 2026.

[108] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 10 de abril de 2025 [10130115]. Disponível em:

reconhecendo a ilicitude do tratamento de dados pessoais pela Luka Inc., com fundamento em múltiplos dispositivos do GDPR, incluindo os princípios de boa-fé, transparência e minimização, bem como os deveres de descrição de base legal, transparência informacional, responsabilidade e proteção de dados desde a concepção e por padrão. A autoridade determinou a adequação integral das práticas da empresa no prazo de trinta dias e aplicou sanção pecuniária no valor de 5 milhões de euros, considerando a gravidade das infrações, a natureza dos dados tratados, o elevado risco imposto a crianças e adolescentes e a persistência das irregularidades ao longo do procedimento.

A decisão final também evidencia outro aspecto central da postura de fiscalização do Garante, que é a recusa em se basear exclusivamente em declarações de conformidade por parte do controlador, uma vez que a autoridade realizou verificações técnicas independentes e identificou falhas relevantes nos mecanismos implementados pela empresa. O período de resfriamento (*cooling-off*)[109] de 24 horas não se mostrava eficaz em navegação anônima, bastando a criação de um novo e-mail para contornar o bloqueio, e a data de nascimento podia ser alterada livremente após o cadastro, sem qualquer revalidação. Esses achados reforçam a ideia de que, em contextos de alto risco, especialmente envolvendo crianças e adolescentes, o *enforcement* exige não apenas compromissos formais, mas comprovação técnica verificável e contínua da efetividade das medidas adotadas.

Em perspectiva, o caso demonstra um modelo de atuação regulatória marcado por continuidade e progressividade: o procedimento foi inaugurado com a adoção de medida de suspensão imediata do serviço, seguido de monitoramento ativo e imposição de obrigações técnicas intermediárias, e culminou na aplicação de sanção definitiva após a verificação concreta do descumprimento e da insuficiência das medidas adotadas. Trata-se, portanto, de um *enforcement* que não se limita à reação pontual, mas se estrutura como um processo contínuo de acompanhamento, verificação e intervenção, orientado à efetiva mitigação de riscos e à proteção integral de crianças e adolescentes no ambiente digital.

(c) Contexto Brasileiro e atuação da ANPD

No contexto brasileiro, até o momento, não se identifica atuação específica da Agência Nacional de Proteção de Dados em relação a um caso com contornos semelhantes ao Replika, o que não impede, contudo, a extração de aprendizados institucionais relevantes a partir da experiência conduzida pelo *Garante per la protezione dei dati personali.* De forma significativa, o modelo italiano evidencia caminhos possíveis de aprimoramento do *enforcement,* especialmente no que se refere à adoção de estratégias de acompanhamento contínuo dos casos, com monitoramento técnico ao longo de todo o ciclo regulatório, e não apenas em momentos pontuais de intervenção.

---

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10130115>. Acesso em 22 abr. 2026.

[109] YOU EUROPE. Right of withdrawal: a 14-day cooling-off period. Disponível em: https://europa.eu/youreurope/citizens/consumers/shopping/returns/index_en.htm#:~:text=Right%20of%20withdrawal:%20a%2014,until%20the%20next%20working%20day. Acesso em 16 abr. 2026.

Outro aspecto que merece atenção diz respeito à utilização de medidas mais incisivas, como a suspensão integral do serviço e não apenas uma das suas funcionalidades diante da verificação de riscos relevantes, como instrumento legítimo para induzir a implementação efetiva de salvaguardas. Trata-se de uma abordagem que prioriza a prevenção de danos, sobretudo em contextos de elevada vulnerabilidade, e que pode contribuir para fortalecer a efetividade das obrigações regulatórias.

Adicionalmente, a experiência italiana reforça a importância de não se admitir a autodeclaração do agente regulado como evidência suficiente de conformidade, mas exigir uma prestação de contas mais robusta, detalhada e auditável.

Por fim, é importante reconhecer que a lógica da regulação responsiva pressupõe, de fato, um espaço de cooperação entre regulador e regulado. Contudo, essa cooperação precisa assumir caráter substantivo, traduzindo-se em medidas concretas, verificáveis e eficazes, e não se limitando a declarações formais de adequação. A experiência comparada indica que a combinação entre abertura ao diálogo e rigor na verificação pode constituir um caminho promissor para o fortalecimento da atuação regulatória em contextos de risco elevado, especialmente quando estão em jogo direitos de crianças e adolescentes.

5. Caso Corte Suprema Di Cassazione/Sentenzeweb

O caso da Corte Suprema di Cassazione[110] representa um dos precedentes mais relevantes da atuação do Garante no setor público, ao demonstrar que a publicidade formal de atos judiciais não equivale a uma autorização ilimitada para a difusão irrestrita de dados pessoais sensíveis, inclusive envolvendo titulares crianças e adolescentes. O caso é igualmente notável pelo modelo de *enforcement* adotado: o Garante conduziu um ciclo fiscalizatório completo – composto por inspeções e testes sucessivos, abertura formal de procedimento, acompanhamento das medidas corretivas adotadas e determinação de prestação de contas dentro de prazo fixado –, consolidando uma abordagem que combina responsabilização, correção estrutural, supervisão continuada, ainda que sem a adoção de sanção pecuniária.

O procedimento teve origem em solicitação encaminhada ao Garante pelo Ministério da Justiça Italiano, a pedido de um particular, que denunciava a possibilidade de pesquisar livremente decisões da Suprema Corte Italiana por meio do portal *SentenzeWeb*[111], gerido pelo Centro Eletrônico de Documentação (CED) da própria Corte. O denunciante alertava que, ao digitar no mecanismo de busca a palavra "HIV", era possível visualizar todas as decisões em que pessoas portadoras do vírus figuravam como parte, com acesso irrestrito a seus nomes completos, dados anagráficos e informações sobre as demandas judiciais correspondentes.

---

[110] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 9 de maio de 2024 [10054644]. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10054644. Acesso em 31 mar. 2026.

[111] Ministero della giustizia. Corte Suprema di Cassazione. Portale SentezeWeb. Disponível em: https://www.italgiure.giustizia.it/sncass/. Acesso em 4 mai. 2026.

A partir dessa sinalização, o Garante realizou, por iniciativa própria, três acessos sequenciais ao portal: em novembro de 2022, em março de 2023 e em uma terceira verificação também em março de 2023[112]. Os resultados foram expressivos. Por meio de pesquisas simples com as palavras-chave "HIV", "violenza sessuale" , "minore sessuali", "malato" e "malattia"[113], o portal retornava centenas e até milhares de decisões judiciais, muitas das quais traziam em texto integral os nomes e dados de identificação direta de pessoas afetadas por essas condições. Em novembro de 2022, foram identificadas 43 decisões com dados em claro de pessoas diagnosticadas com HIV, além de duas decisões contendo o nome completo de vítimas de crimes sexuais. Em março de 2023, novas pesquisas revelaram três decisões com identificação completa de pessoas portadoras de doenças oncológicas, todas ainda publicadas e livremente acessíveis ao momento da abertura formal do procedimento. Importante destacar que em todos casos encontrados havia, em maior ou menor medida, dados de titulares crianças e adolescentes envolvidos, com maior incidência em casos de violência sexual.

(a) Infrações identificadas

A infração central consiste na difusão e exposição ilícita de dados pessoais sensíveis por meio de um portal público de acesso irrestrito, em violação ao art. 9º do GDPR e ao art. 2-*septies*[114], parágrafo 8º, do Código italiano de proteção de dados. A publicação de decisões judiciais pesquisáveis por nome de pessoa, por patologia ou por palavra-chave – incluindo termos como "violenza sessuale" ou "minore" – produzia um resultado estruturalmente incompatível com a tutela de dados sensíveis: qualquer usuário, com um único comando de busca, podia acessar e baixar decisões contendo informações de saúde, histórico de vitimização sexual e dados de crianças e adolescentes vinculados a seus nomes reais.

Inicialmente, a Corte sustentou que parte dessas decisões não trazia determinação explícita de necessidade de sigilo ou anonimização no corpo da respectiva sentença/decisão, mas o Garante rejeitou esse argumento com firmeza, afirmando que a obrigação de proteção decorre diretamente da lei, independentemente de qualquer indicação no dispositivo decisório.

A segunda infração diz respeito à violação do art. 52, parágrafo 5º, do Código italiano, que determina a supressão obrigatória dos dados identificadores de vítimas de violência sexual e de crianças e adolescentes em qualquer decisão judicial divulgada ao público, norma que cujo cumprimento, conforme apurado, dependia quase exclusivamente de procedimentos manuais realizados por diferentes servidores e magistrados.

---

[112] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 9 de maio de 2024 [10054644]. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10054644. Acesso em 31 mar. 2026.

[113] Traduzidas seriam “HIV", "violência sexual", "abuso sexual infantil", "doente" e "doença", respectivamente.

[114] "Septies" é um termo de origem latina que significa "sete vezes" ou "pela sétima vez". É usado para indicar um sétimo parágrafo, artigo ou item adicionado a uma lei, após o sexto (que seria sexties). Disponível em: https://pt.wiktionary.org/wiki/septies. Acesso em 4 mai. 2026.

A terceira infração abrange a violação dos princípios de boa-fé, minimização, segurança e prevenção previstos no art. 5º, parágrafo 1º, alíneas a), c) e f), do GDPR, bem como outros deveres de segurança estabelecidos no art. 32 do mesmo regulamento. As medidas adotadas até a abertura formal do procedimento, baseadas predominantemente em controles organizacionais descentralizados e em intervenções humanas ao longo das diferentes etapas da cadeia de publicação, mostraram-se estruturalmente insuficientes para assegurar, de forma contínua e sistemática, a não divulgação de dados sensíveis. O sistema de filtragem por palavras-chave era aplicado de maneira residual e não abrangia categorias relevantes de dados, como aqueles relacionados à saúde, o que se revela especialmente grave em um banco de dados público de acesso irrestrito.

(b) Instrumentos de *enforcement* adotados pela Autoridade Italiana de proteção de dados

O caso da Corte Suprema di Cassazione é singular no espectro de casos analisados neste relatório por apresentar um ciclo de fiscalização completo, conduzido de forma iterativa e com acompanhamento efetivo das medidas corretivas ao longo do tempo, a partir de uma postura proativa da autoridade, que iniciou, de maneira diligente, sequências de testes práticos e documentados, logo após tomar ciências das potenciais infrações envolvidas.

A trajetória do *enforcement* iniciou-se com uma fase de inspeções de iniciativa própria do Garante: três acessos ao portal foram realizados em novembro de 2022, novembro de 2022 (segunda visita) e março de 2023, com registro formal em verbais de operações realizadas. Essa postura ativa contrasta com modelos reativos de fiscalização e evidencia a capacidade da autoridade de transformar uma denúncia individual em procedimento de abrangência sistêmica. Seguiu-se, em novembro de 2022, o envio de pedido formal de informações à Corte e ao Ministério da Justiça, acompanhado de convite para adoção imediata de medidas cautelares.

Diante das justificativas insatisfatórias da Corte, o Garante instaurou formalmente o procedimento em 8 de março de 2023. A resposta institucional foi imediata: no dia seguinte, 9 de março de 2023, a Corte suspendeu preventivamente o portal SentenzeWeb, sinalizando o início de uma fase de cooperação ativa com a autoridade. Em 1º de abril de 2023, a Presidente da Corte à época emitiu novas e abrangentes diretivas internas, que atualizaram e substituíram as normas anteriores de 2016, estabelecendo procedimentos detalhados para cada etapa do ciclo de publicação de decisões, da inscrição no registro geral até a inserção no banco de dados público.

A Corte também comunicou ao Garante o início de cooperação com o Ministério da Justiça para desenvolvimento de sistema automático de pseudonimização baseado em inteligência artificial, que utiliza tecnologia de *Named Entity Recognition*[115] para identificar e substituir dados identificáveis nos textos das

[115] MEDIUM. Uma Visão Geral sobre Named Entity Recognition (NER). Disponível em: https://medium.com/elinttech/uma-vis%C3%A3o-geral-sobre-named-entity-recognition-ner-4dc4e3b5e37a. Acesso em 4 mai. 2026.

decisões. O Garante reconheceu o avanço, mas formulou ressalva técnica de considerável relevância: a mera substituição de nomes por pseudônimos não configura anonimização eficaz, pois o contexto das decisões – incluindo informações sobre localidade, datas, empregadores ou circunstâncias específicas dos fatos narrados – pode permitir a reidentificação indireta dos interessados. Nesse ponto, o *procedimento* consolida um princípio regulatório de alta importância: a pseudonimização automatizada não configura anonimização suficiente com relação à dados sensíveis, além de não dispensar análise contextual humana dos riscos de identificabilidade residual.

Na decisão de 9 de maio de 2024[116], o Garante declarou a ilicitude do tratamento, optou pela aplicação de advertência formal com fundamento no art. 58, parágrafo 2º, alínea b), do GDPR - afastando a sanção pecuniária em razão da ausência de dolo, da cooperação integral da Corte, da suspensão imediata do portal e da adoção de medidas corretivas relevantes durante a instrução – e determinou que a Corte apresentasse ao Garante, em até três meses, informações detalhadas sobre: (i) as eventuais dificuldades surgidas na aplicação das novas diretivas e as medidas adotadas para superá-las; e (ii) a eventual implementação do sistema automático de pseudonimização e as medidas adotadas para mitigar os riscos residuais de reidentificação.

Essa obrigação de prestação de contas com prazo fixado demonstra que o encerramento formal do procedimento fiscalizatório não implica o abandono do acompanhamento do caso e do ciclo de fiscalização: o Garante mantém abertura de supervisão sobre o titular, exigindo transparência sobre a implementação das medidas prometidas e reservando-se o poder de atuar novamente caso as informações prestadas revelem inadequação das soluções adotadas.

(c) Contexto Brasileiro e atuação da ANPD

No contexto brasileiro, o referido caso encontra paralelo similar na realidade brasileira, considerando que o vazamento e a difusão indevida de dados pessoais de crianças e adolescentes, oriundos de processos judiciais, já ocorreu. Um exemplo recente e emblemático é o do Tribunal de Justiça do Estado de São Paulo (TJ-SP)[117], cujas decisões judiciais contendo dados sigilosos de crianças e adolescentes – incluindo nomes completos, detalhes processuais e informações relacionadas a crimes sexuais, violência e atos infracionais – passaram a ser indexadas e replicadas por plataformas privadas de consulta jurídica, tornando-se acessíveis ao público em geral. Os impactos documentados foram concretos e graves: adolescentes demitidos após a localização de seus processos por

[116] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Disposição de 9 de maio de 2024 [10054644]. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10054644. Acesso em 31 mar. 2026.

[117] ACAYABA, Cíntia. **Como ocorreu o vazamento de dados de crianças e adolescentes de processos de SP: veja as principais suspeitas.** G1, São Paulo, 12 dez. 2025. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2025/12/12/como-ocorreu-o-vazamento-de-dados-de-criancas-e-adolescentes-de-processos-de-sp-veja-as-principais-suspeitas.ghtml. Acesso em: 18 dez. 2025.

empregadores, jovens estigmatizados em seus territórios de convivência, casos de abandono escolar e comprometimento do desenvolvimento emocional[118].

A similitude estrutural com o caso italiano é notável. Em ambos os contextos, a violação não emerge de uma conduta isolada e deliberada de um agente privado, mas de falhas sistêmicas na governança do fluxo de dados judiciais: publicação sem anonimização adequada e ausência de mecanismos técnicos eficazes de controle. Em ambos os casos, os titulares mais vulneráveis – crianças, adolescentes, vítimas de violência – são os que experimentam os efeitos mais duradouros e irreparáveis da exposição.

Esse episódio, contudo, é apenas um entre os inúmeros incidentes de segurança e falhas técnicas registrados no setor público brasileiro. Os dados do painel de monitoramento da ANPD revelam que o setor público concentra parcela expressiva dos casos fiscalizatórios acompanhados pela Agência, evidenciando um ambiente de governança de dados ainda em consolidação em órgãos estatais de diferentes esferas e poderes. Dados do painel de monitoramento da Agência revelam que infrações envolvendo proteção de dados pessoais no setor público corresponde a 36% dos procedimentos acompanhados, incluindo as espécies preparatórias, fiscalizatórias e sancionadoras[119].

O caso italiano oferece, nesse contexto, um modelo de atuação especialmente relevante por três razões. A postura investigativa ativa do Garante – que realizou inspeções sucessivas, documentou evidências e acompanhou as medidas corretivas ao longo do tempo – demonstra que o ciclo de fiscalização pode ser conduzido de forma iterativa, sem limitar-se a uma sequência linear de abertura e encerramento formal de procedimento. A utilização da *ingiunzione* de prestação de contas com prazo definido representa, ademais, uma solução regulatória que mantém o ator público sob monitoramento mesmo após ter sido verificada a conformidade regulatória inicial do agente regulado.

Por fim, a advertência técnica sobre os limites da pseudonimização automatizada mostra-se diretamente relevante para o contexto brasileiro. O uso crescente de sistemas de inteligência artificial para a publicização de decisões judiciais, especialmente por meio de sua replicação por empresas privadas, pode gerar uma percepção equivocada de conformidade, enquanto o risco de reidentificação contextual permanece elevado.

Nesse sentido, o caso evidencia que a atuação regulatória sobre entes públicos pode ser firme, estruturada e efetiva mesmo na ausência de sanções pecuniárias, desde que o ciclo fiscalizatório seja integralmente percorrido, incluindo inspeção, instauração de procedimento, acompanhamento das medidas corretivas,

---

[118] ACAYABA, Cíntia. **Dados sigilosos de crianças e adolescentes de processos do TJ-SP vazam em sites jurídicos e expõem jovens a constrangimentos e riscos.** G1, São Paulo, 11 dez. 2025. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2025/12/11/dados-sigilosos-de-criancas-e-adolescentes-de-processos-do-tj-sp-vazam-em-sites-juridicos-e-expoem-jovens-a-constrangimentos-e-riscos.ghtml. Acesso em: 18 dez. 2025.

[119] ANPD. Coordenação-Geral de Fiscalização - CGF. Estatísticas dos processos. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiYmZlMmM5YzItMzQ1MS00N2E2LThhYTctMTYwZTliOGJmZWM0IiwidCI6IjVhYmEwNGExLWY4NjMtNGI1Ni04MTdkLTQ0MjkxYzkwZDFiOCJ9. Acesso em 4 mai. 2026.

decisão formal e supervisão posterior. Esse modelo permite afirmar a autoridade regulatória ao mesmo tempo em que preserva a cooperação institucional necessária em contextos que envolvem o setor público.

6. Considerações finais

A análise dos casos conduzidos pelo Garante per la protezione dei dati personali evidencia um modelo de *enforcement* caracterizado por elevada densidade técnica, continuidade procedimental e centralidade na verificação concreta da efetividade das medidas adotadas. Mais do que a aplicação isolada de sanções ou a imposição de obrigações formais, observa-se uma atuação orientada à transformação estrutural das práticas dos agentes regulados, especialmente em contextos de risco elevado envolvendo crianças e adolescentes.

Nesse sentido, os casos analisados indicam que o *enforcement* eficaz não depende apenas da existência de instrumentos normativos, mas da forma como esses instrumentos são mobilizados de maneira estratégica, coordenada e tecnicamente fundamentada ao longo do tempo. Destacam-se, nesse contexto, os seguintes elementos:

- **Atuação preventiva com uso de medidas cautelares incisivas**
  A autoridade atua de forma precoce diante de riscos relevantes, inclusive com suspensão integral de serviços ou limitação ampla do tratamento, priorizando a interrupção imediata de potenciais danos quando não há garantias técnicas mínimas de proteção.
- **Estruturação do *enforcement* como processo contínuo e iterativo**
  O enforcement não se limita a uma decisão pontual, mas se desenvolve em múltiplas fases articuladas, com decisões sucessivas que combinam intervenção emergencial, condicionamento da operação e revisão posterior das medidas implementadas.
- **Centralidade da comprovação técnica da efetividade das medidas**
  A conformidade regulatória exige demonstração documentada, verificável e, sempre que possível, testável da eficácia das salvaguardas adotadas, afastando a suficiência de declarações unilaterais, planos de ação ou dados agregados apresentados pelos controladores.
- **Rejeição de soluções formais ou meramente declaratórias**
  O modelo analisado afasta a ideia de que compromissos formais, termos de uso ou políticas declaradas sejam suficientes para caracterizar conformidade, exigindo alinhamento efetivo entre o desenho do sistema e as obrigações legais.
- **Incorporação de instrumentos de natureza pedagógica e informacional**
  A atuação regulatória inclui medidas voltadas à conscientização pública, como campanhas obrigatórias de comunicação, reconhecendo que a proteção de dados também depende da capacidade informacional dos titulares e da sociedade.
- **Adoção de um padrão de accountability material e contínua**
  A responsabilidade do controlador é compreendida como dever permanente de demonstrar conformidade ao longo de todo o ciclo de vida do sistema, incluindo fases de desenvolvimento, implementação e operação.

- **Recusa da inação diante da ausência de soluções técnicas perfeitas**
  A inexistência de mecanismos ideais não é aceita como justificativa para a ausência de salvaguardas, sendo exigida a implementação de medidas proporcionais ao risco, ainda que imperfeitas, desde que efetivas e progressivamente passíveis de aprimoramento.

Em conjunto, esses elementos indicam que o *enforcement*, especialmente em contextos que envolvem crianças e adolescentes, tende a se estruturar como um processo dinâmico, orientado à mitigação efetiva de riscos e à adaptação contínua das práticas tecnológicas. A experiência analisada demonstra que a combinação entre rigor técnico, flexibilidade procedimental e acompanhamento prolongado pode contribuir para a construção de respostas regulatórias mais aderentes à complexidade dos serviços digitais contemporâneos. Ao evidenciar padrões de atuação que privilegiam a efetividade material da proteção, os casos examinados oferecem parâmetros relevantes para o aprimoramento de estratégias regulatórias em diferentes contextos institucionais, especialmente diante de desafios comuns associados à atuação sobre plataformas digitais de escala global.

(4) Recomendações à ANPD

1) Que a ANPD constitua um ‘lócus’ de discussão, trabalho e até deliberação sobre o entrelaçamento dos temas relacionados à proteção de dados de crianças e adolescentes e ao ECA Digital. De forma a transformar a teoria do diálogo das fontes em exercício prático da autoridade administrativa.

2) Que a ANPD se debruce sobre as 99 recomendações advindas das contribuições multisetoriais que o GT2 recebeu e já estão divididas nos temas respectivos e avalie aquelas que (i) já serão respondidas com ações mais imediatas da Agência; (ii) já estão na perspectiva de atuação da Agência em um futuro próximo; e (iii) são novas e ainda não estavam no radar da Agência. Em relação às que não estavam no radar da Agência, que a ANPD separe as que julgar mais relevantes das outras. Ao final, sugere-se que a ANPD volte ao CNPD com essas informações para darmos sequência ao diálogo. Abaixo, uma visualização simplificada das recomendações. A versão completa pode ser consultada no “Banco de Teses (**ANEXO I**)”.

Grande Tema	Recomendação	Organização	Página
C1 — Aferição Etária	**Proibir reconhecimento facial para aferição etária**	Coalizão Direitos na Rede (CDR)	p. 3
C1 — Aferição Etária	**Adotar prova de conhecimento zero como mecanismo de aferição etária**	Coalizão Direitos na Rede (CDR)	p. 3
C1 — Aferição Etária	**Aferição etária não deve gerar custos aos usuários nem prejudicar pequenas empresas**	Coalizão Direitos na Rede (CDR)	p. 4
C1 — Aferição Etária	**ANPD deve publicar taxonomia de técnicas de aferição etária com abordagem em camadas por nível de risco**	Data Privacy Brasil	p. 3

C1 — Aferição Etária	**Aferição etária por CPF em vez de reconhecimento facial ou token etário para evitar vazamentos e violência sexual**	Geledés - Instituto da Mulher Negra	p. 2
C1 — Aferição Etária	**Proibir biometria de menores de 16 anos em estádios e determinar exclusão imediata dos dados já coletados**	Plataforma 12	p. 3
C1 — Aferição Etária	**Brasil deve adotar abordagem em camadas para aferição etária em redes sociais inspirada no modelo australiano de idade mínima**	Yoti	p. 1–2
C1 — Aferição Etária	**Concentrar aferição de idade no nível do SO/App Store — Google e Apple já têm APIs de idade disponíveis**	Meta	p. 1
C1 — Aferição Etária	**Controle parental deve ser reforçado no nível do dispositivo — pais aprovam ou revogam acesso a apps conforme necessário**	Meta	p. 1
C1 — Aferição Etária	**Observar exemplos de API pública de sinal de idade com retorno binário — Europa já está desenvolvendo esse modelo**	Alandar	Ata 3ª Entrevista — 22/1/2026
C1 — Aferição Etária; C2 — Proteção por Design	**ANPD deve publicar guias setoriais de privacy by default, consentimento informado por idade e dark patterns proibidos**	Family Talks	p. 3
C1 — Aferição Etária; C2 — Proteção por Design	**APIs de aferição etária devem compartilhar apenas sinal de idade — não dados pessoais completos — garantindo privacidade por design**	Meta	p. 1

C1 — Aferição Etária; C5 — Normatização e Lacunas	**Permitir múltiplos métodos de consentimento parental adaptados à plataforma — modelo COPPA como referência**	Entertainment Software Association (ESA)	p. 2
C1 — Aferição Etária; C5 — Normatização e Lacunas	**Reconhecer juridicamente distinção entre plataformas generalistas e plataformas de acesso restrito por idade**	ESAPIENS Tecnologia S/A (Sexlog) / ABIPEA	p. 4
C1 — Aferição Etária; C5 — Normatização e Lacunas	**ANPD deve definir normativamente o conceito de 'acesso' a conteúdo adulto e parâmetros de retenção de dados de bloqueio**	ABIPEA	p. 1
C1 — Aferição Etária; C5 — Normatização e Lacunas	**ANPD deve estabelecer padrões de verificação de idade interoperáveis com minimização de dados — foco em certificações**	PUC-Rio / Legalite	Ata 4ª/5ª Entrevista — 29/1/2026
C1 — Aferição Etária; C9 — Discriminação e Interseccionalidade	**Moratória imediata do reconhecimento facial em escolas até comprovação de equidade demográfica por auditoria independente**	Instituto da Hora	p. 4
C1 — Aferição Etária; C9 — Discriminação e Interseccionalidade	**Criar Diretriz Nacional anti-sharenting e campanha escolar de literacia em privacidade para famílias**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 3
C1 — Aferição Etária; C9 — Discriminação e Interseccionalidade	**Consentimento parental deve ter via não digital obrigatória para não excluir famílias periféricas e rurais**	Instituto da Hora	p. 5

C2 — Proteção por Design	**Exigir proteção por design em brinquedos conectados com bloqueio de liberação**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C2 — Proteção por Design	**Criar selo de qualidade de proteção digital para escolas, clubes e espaços públicos (WI-FI-CA)**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C2 — Proteção por Design	**Configuração padrão de contas de crianças como privadas e bloqueio de contato com desconhecidos**	Childhood Brasil	p. 2
C2 — Proteção por Design	**Exigir Privacy by Design e Security by Default como obrigação legal para sistemas que tratam dados de crianças**	Centro Marista de Defesa da Infância (CMDI)	p. 5
C2 — Proteção por Design	**Proibir design enganoso e manipulativo em serviços digitais voltados a crianças**	Grupo ASPAS / UFRPE	p. 2
C2 — Proteção por Design	**Classificar como alto risco ou proibir smart toys com coleta intensiva de dados de voz e emoções de crianças**	Grupo ASPAS / UFRPE	p. 3
C2 — Proteção por Design	**Regulamentar Safety, Privacy e AI Safety by Design obrigatórios em serviços acessíveis a crianças**	Instituto Teckids	p. 13
C3 — IA Generativa e Algoritmos; C2 — Proteção por Design	**Proibir perfilamento comportamental comercial e publicidade por perfil para crianças; permitir apenas publicidade contextual**	Family Talks	p. 4

C4 — Exploração Sexual Digital; C2 — Proteção por Design	**Classificar ferramentas geradoras de imagem por risco e vedar aplicações nudify — regulamentação via ISO para privacy by design**	FGV	Ata 4ª/5ª Entrevista — 29/1/2026
C2 — Proteção por Design; C6 — Fiscalização e Enforcement	**Proibir dark patterns em interfaces para menores com auditoria periódica por especialistas em interação humano-computador**	Instituto da Hora	p. 4–5
C2 — Proteção por Design; C6 — Fiscalização e Enforcement	**Instituições que lidam com dados de crianças devem revisar rotinas — escolas, prédios comerciais e condomínios incluídos**	Rede de Pesquisa em Comunicação, Infâncias e Adolescências (Recria)	p. 2
C9 — Discriminação e Interseccionalidade; C2 — Proteção por Design	**Regulação e design tecnológico devem incorporar perspectiva crítico-racial e centrar vozes de jovens negros**	Grupo ASPAS / UFRPE (artigo submetido — Tanksley, 2024)	p. 2
C10 — Educação e Conscientização; C2 — Proteção por Design	**Estabelecer critérios de avaliação de risco e transparência obrigatória para ferramentas edtech nas escolas**	Childhood Brasil	p. 2
C3 — IA Generativa e Algoritmos; C4 — Exploração Sexual Digital	**Obrigar marca d'água em conteúdos gerados por IA para proteger imagem de crianças**	Childhood Brasil	p. 2

C3 — IA Generativa e Algoritmos; C4 — Exploração Sexual Digital	**Exigir filtro de palavras restritas e autenticação de identidade em plataformas de IA generativa de imagem e vídeo**	Geledés - Instituto da Mulher Negra	p. 2
C4 — Exploração Sexual Digital; C3 — IA Generativa e Algoritmos	**ANPD deve promover letramento digital e midiático com articulação com sistemas educacionais e obrigatoriedade na BNCC**	Instituto Teckids	p. 17
C4 — Exploração Sexual Digital; C3 — IA Generativa e Algoritmos	**Regular uso de dados de crianças em treinamento de IA generativa e fomentar ferramentas abertas de detecção de deepfakes**	Instituto da Hora	p. 4
C3 — IA Generativa e Algoritmos; C5 — Normatização e Lacunas	**Regulamentar frameworks obrigatórios de Safety, Privacy e AI Safety by Design em serviços acessíveis a crianças**	Instituto Teckids	p. 13
C3 — IA Generativa e Algoritmos; C5 — Normatização e Lacunas	**Proibir publicidade comportamental a menores incluindo perfilamento indireto por contas de adultos**	Plataforma 12	p. 4
C3 — IA Generativa e Algoritmos; C6 — Fiscalização e Enforcement	**ANPD deve estabelecer que qualidade dos dados em datasets de IA exige rastreabilidade e filtros para dados de crianças**	Comissão de Defesa dos Direitos da Criança e do Adolescente GT Digital / OAB-SP	p. 5

C3 — IA Generativa e Algoritmos; C11 — Saúde, Desenvolvimento e Bem-estar	**Exigir segurança por design em plataformas de IA usadas como consulta terapêutica**	Childhood Brasil	p. 2
C4 — Exploração Sexual Digital	**Criminalizar criação de imagens de abuso sexual infantil geradas por IA**	Childhood Brasil	p. 2
C8 — Fluxo de Denúncias e Responsabilização; C4 — Exploração Sexual Digital	**Integrar Brasil a redes internacionais de detecção e remoção de material de abuso sexual infantil**	Childhood Brasil	p. 2
C8 — Fluxo de Denúncias e Responsabilização; C4 — Exploração Sexual Digital	**Fomentar parcerias internacionais para desmantelar redes criminosas de abuso sexual infantil**	Childhood Brasil	p. 2
C5 — Normatização e Lacunas	**ANPD deve incorporar princípios do ECA Digital e LGPD na regulação de aferição etária**	Coalizão Direitos na Rede (CDR)	p. 3–4
C5 — Normatização e Lacunas	**Separar por norma os agentes que constroem e os que usam mecanismos de aferição etária**	Coalizão Direitos na Rede (CDR)	p. 4

C5 — Normatização e Lacunas	**ANPD deve elaborar diretrizes de consentimento com assentimento progressivo por faixa etária**	Centro Marista de Defesa da Infância (CMDI)	p. 4
C5 — Normatização e Lacunas	**Incorporar binômio proteção-benefício como eixo interpretativo central da regulação**	Centro Marista de Defesa da Infância (CMDI)	p. 4
C5 — Normatização e Lacunas	**ANPD deve densificar normativamente o Art. 14 com interpretação sempre mais protetiva ao titular vulnerável**	Comissão de Defesa dos Direitos da Criança e do Adolescente GT Digital / OAB-SP	p. 3
C5 — Normatização e Lacunas	**ANPD deve restringir bases legais de legítimo interesse, execução de contrato e proteção ao crédito para dados de crianças**	Comissão de Defesa dos Direitos da Criança e do Adolescente GT Digital / OAB-SP	p. 4
C5 — Normatização e Lacunas	**ANPD deve esclarecer interpretação do melhor interesse conforme Comentário Geral nº 14 da ONU adaptado a dados**	Idec - Instituto de Defesa de Consumidores	p. 2
C5 — Normatização e Lacunas; C7 — Governança Institucional	**Publicar diretrizes de harmonização entre LGPD e ECA Digital com atribuições claras por órgão**	Childhood Brasil	p. 2
C5 — Normatização e Lacunas; C7 — Governança Institucional	**Regulação de proteção de dados de crianças em jogos deve ser flexível — orientações voluntárias em vez de prescrições rígidas**	Entertainment Software Association (ESA)	p. 1
C5 — Normatização e Lacunas; C7 — Governança	**ANPD deve publicar Nota Técnica consolidando limites práticos das exceções do Art. 4º para proteção de crianças**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4

Institucional			
C5 — Normatização e Lacunas; C7 — Governança Institucional	**ANPD deve publicar Nota Técnica consolidando limites práticos das exceções do Art. 4º para crianças**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4
C5 — Normatização e Lacunas; C7 — Governança Institucional	**Regulação deve ser baseada em risco e proporcional ao porte — não prescrever tecnologia específica nem solução única**	Conselho Digital	Ata 3ª Entrevista — 22/1/2026
C10 — Educação e Conscientização; C5 — Normatização e Lacunas	**Exigir avisos de privacidade em linguagem acessível e adequada à faixa etária**	Centro Marista de Defesa da Infância (CMDI)	p. 4
C5 — Normatização e Lacunas; C10 — Educação e Conscientização	**ANPD deve publicar Nota Técnica sobre Art. 4º para consolidar limites das exceções e orientar cenários extracomerciais**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4
C5 — Normatização e Lacunas; C10 — Educação e Conscientização	**Regulamentar direito à explicabilidade algorítmica por faixa etária (6-9, 10-12, 13-17 anos)**	Instituto da Hora	p. 5
C10 — Educação e Conscientização; C5 — Normatização e Lacunas	**Obrigar DPO e política de proteção de dados em escolas; consentimento específico antes do cadastro de alunos em plataformas**	Plataforma 12	p. 3–4

C11 — Saúde, Desenvolvimento e Bem-estar; C5 — Normatização e Lacunas	**Estabelecer direito ao esquecimento e desindexação para conteúdos publicados durante a infância**	Centro Marista de Defesa da Infância (CMDI)	p. 5
C6 — Fiscalização e Enforcement	**Provedores de aferição etária devem publicar relatórios periódicos auditáveis**	Coalizão Direitos na Rede (CDR)	p. 4
C6 — Fiscalização e Enforcement	**Reconhecer presunção de violação quando tratamento de dados de crianças resultar em dano ou risco demonstrado**	Comissão de Defesa dos Direitos da Criança e do Adolescente GT Digital / OAB-SP	p. 4
C6 — Fiscalização e Enforcement	**ANPD deve implementar fiscalização ativa e setorizada por agendas periódicas sem necessidade de denúncia**	Comissão de Defesa dos Direitos da Criança e do Adolescente GT Digital / OAB-SP	p. 4
C6 — Fiscalização e Enforcement	**ANPD deve instituir Protocolo de Supervisão por Risco com padrão mínimo de evidências de conformidade**	Data Privacy Brasil	p. 3
C6 — Fiscalização e Enforcement	**Fiscalização e sanções devem cobrir crianças em plataformas generalistas — não apenas em versões 'infantis'**	Data Privacy Brasil	Ata 2ª Entrevista — 8/1/2026
C6 — Fiscalização e Enforcement; C7 — Governança Institucional	**ANPD deve publicar guia de rastreabilidade da cadeia de tratamento em produtos acessados por crianças**	Data Privacy Brasil	p. 2

C6 — Fiscalização e Enforcement; C7 — Governança Institucional	**Padronizar template nacional de RIPD acadêmico para pesquisas com dados de crianças nos CEP/CONEP**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4
C6 — Fiscalização e Enforcement; C7 — Governança Institucional	**ANPD deve criar CRIA — Relatório de Impacto sobre Direitos de Crianças e Adolescentes — em diálogo com UNICEF**	UFRJ	Ata 4ª/5ª Entrevista — 29/1/2026
C9 — Discriminação e Interseccionalidade; C6 — Fiscalização e Enforcement	**Dados raciais devem constar nos relatórios de transparência do ECA Digital de forma anônima e auditável em tempo real**	Geledés - Instituto da Mulher Negra	p. 2
C6 — Fiscalização e Enforcement; C9 — Discriminação e Interseccionalidade	**Regular e fiscalizar dark patterns direcionados a crianças que exploram impulsividade e recompensa**	Instituto Teckids	p. 14
C6 — Fiscalização e Enforcement; C9 — Discriminação e Interseccionalidade	**Exigir RIPD com métricas desagregadas por raça, gênero e faixa etária para todo sistema de IA que processe dados de menores**	Instituto da Hora	p. 3–4
C6 — Fiscalização e Enforcement; C9 — Discriminação e	**Instituir relatórios semestrais obrigatórios sobre uso de biometria e IA pela segurança pública em espaços com crianças**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4

Interseccionalidade			
C6 — Fiscalização e Enforcement; C9 — Discriminação e Interseccionalidade	**Instituir relatórios semestrais e auditorias independentes sobre uso de biometria e IA pela segurança pública em espaços com crianças**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4–5
C10 — Educação e Conscientização; C6 — Fiscalização e Enforcement	**Criar hub 'Privacidade para Crianças' e exigir RIPD antes do lançamento de novos produtos com IA**	Family Talks	p. 4
C7 — Governança Institucional	**Criar estrutura federal de auditoria pública com participação da sociedade civil**	Coalizão Direitos na Rede (CDR)	p. 3
C7 — Governança Institucional	**Formar grupo consultivo intersetorial com especialistas em infância e adolescência**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C7 — Governança Institucional	**Parcerias entre TICs, BTechs e Sociedade Civil para implementar ECA Digital e LGPD**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C7 — Governança Institucional	**Criar reconhecimento regulatório do tratamento de dados por OSCs com finalidade de defesa de direitos**	Centro Marista de Defesa da Infância (CMDI)	p. 4
C7 — Governança Institucional	**Instituir governança multissetorial de segurança, privacidade e IA para o ambiente digital infantojuvenil**	Instituto Teckids	p. 12–13

C7 — Governança Institucional	**ANPD deve priorizar guia de conceitos gerais do ECA Digital — acesso provável, serviços de terceiros, aferição etária — antes da regulamentação técnica**	ANPD	Ata 1ª Entrevista — 4/12/2025
C7 — Governança Institucional; C8 — Fluxo de Denúncias e Responsabilização	**ANPD deve mapear e dialogar com ecossistema de proteção da criança — CONANDA, MDHC, comitê intersetorial — antes de agir isoladamente**	ANPD	Ata 1ª Entrevista — 4/12/2025
C9 — Discriminação e Interseccionalidade; C7 — Governança Institucional	**Padronizar RIPD acadêmico obrigatório para pesquisas com dados de crianças e protocolo de scraping ético**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4–5
C9 — Discriminação e Interseccionalidade; C7 — Governança Institucional	**ANPD deve incorporar perspectiva interseccional e fomentar pesquisas nacionais sobre impacto de IA em crianças brasileiras**	Instituto da Hora	p. 5–6
C10 — Educação e Conscientização; C7 — Governança Institucional	**Guia conjunto ANPD–CONANDA–Abraji para jornalismo com menores: teste de essencialidade e anonimização por padrão**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 4
C10 — Educação e Conscientização; C7 — Governan	**Instituir Programa Nacional de formação de educadores em educação midiática, segurança digital e IA com plano em 3 horizontes temporais**	Instituto Teckids	p. 16–17

ça Institucional			
C11 — Saúde, Desenvolvimento e Bem-estar; C10 — Educação e Conscientização; C7 — Governança Institucional	**Criar Diretriz Nacional anti-sharenting, RIPD acadêmico padronizado e guia de jornalismo com menores**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 3–4
C8 — Fluxo de Denúncias e Responsabilização	**Criar Disque-Denúncia Digital federal (0-800) com bloqueio imediato e rastreamento de IP**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C8 — Fluxo de Denúncias e Responsabilização	**Dados de denúncias devem ser públicos com responsabilização de BTechs via ANPD, MPF e PF**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C8 — Fluxo de Denúncias e Responsabilização	**Regulação brasileira de dados de crianças deve ser alinhada com GDPR, AADC e COPPA para consistência global**	Entertainment Software Association (ESA)	p. 2
C8 — Fluxo de Denúncias e Responsabilização	**ANPD, SGDCA e SNDC devem aprimorar canais de denúncia de violações a direitos de crianças com dados abertos**	Idec - Instituto de Defesa de Consumidores	p. 3
C8 — Fluxo de Denúncias e Responsabilização	**Criar fluxo de atendimento acessível para denúncias de violação de dados de crianças — modelo CDC/PROCON como referência**	Agência Curumin Erê	Ata 2ª Entrevista — 8/1/2026

C9 — Discriminação e Interseccionalidade	**Adotar abordagem interseccional na regulação de dados infantis para reduzir impactos sobre crianças negras e vulneráveis**	Grupo ASPAS / UFRPE	p. 2
C10 — Educação e Conscientização	**Campanha pública de conscientização sobre aferição etária para toda a população**	Coalizão Direitos na Rede (CDR)	p. 4
C10 — Educação e Conscientização	**MEC, ANPD e Conanda devem promover participação de crianças nas escolas**	Coalizão Direitos na Rede (CDR)	p. 4
C10 — Educação e Conscientização	**Campanhas públicas de conscientização sobre ecossistema digital e saúde para infância**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3
C10 — Educação e Conscientização	**Usar escolas como locus de pensamento reflexivo sobre LGPD com formação adequada de docentes e gestores**	Rede de Pesquisa em Comunicação, Infâncias e Adolescências (Recria)	p. 1
C11 — Saúde, Desenvolvimento e Bem-estar; C10 — Educação e Conscientização	**Criar Diretriz Nacional anti-sharenting com checklists e modelos de pedido de remoção para famílias**	Infinis / Fundação José Luiz Setúbal (FJLS)	p. 3
C11 — Saúde, Desenvolvimento e Bem-estar	**Proibir venda e uso de celular para crianças menores de 2 anos; desaconselhar até 5 anos**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3

C11 — Saúde, Desenvolvimento e Bem-estar	**Integrar proteção digital à atenção primária à saúde da infância nos órgãos governamentais**	CEIIAS – Centro de Estudos Integrados, Infância, Adolescência e Saúde	p. 3

3) Que a ANPD avalie, à luz de suas competências legais e regulatórias, os instrumentos de enforcement, estratégias procedimentais e mecanismos de supervisão destacados nos casos da Autoridade Italiana analisados, a fim de identificar pontos de convergência com as práticas já adotadas pela Agência, distinções relevantes e eventuais possibilidades de aprimoramento institucional.

Em especial, recomenda-se a análise de aspectos como: (i) utilização de medidas cautelares e preventivas em contextos de risco elevado; (ii) adoção de modelos de fiscalização contínua e interativa; (iii) exigência de comprovação técnica documentada da efetividade das salvaguardas implementadas; (iv) utilização de instrumentos de prestação de contas com acompanhamento posterior à decisão; e (v) incorporação de medidas de caráter pedagógico e informacional no âmbito do enforcement regulatório.

Ponto de análise	**Replika / Luka Inc.**	**Corte Suprema di Cassazione / SentenzeWeb**
(i) Medidas cautelares e preventivas	Suspensão provisória do serviço na Itália diante do risco imediato a crianças e adolescentes, em razão da ausência de verificação etária eficaz e da exposição a conteúdos inadequados.	Realização de inspeções e adoção de medidas cautelares após identificação de exposição pública de dados sensíveis e de crianças e adolescentes em decisões judiciais.
(ii) Fiscalização contínua e iterativa	Enforcement desenvolvido em múltiplas etapas: suspensão inicial, imposição progressiva de obrigações técnicas e decisão final após monitoramento contínuo.	Procedimento estruturado com inspeções sucessivas, abertura formal de procedimento, acompanhamento das medidas corretivas e supervisão posterior à decisão.
(iii) Comprovação técnica da efetividade das medidas	O Garante realizou verificações técnicas independentes e identificou falhas concretas nos mecanismos de verificação etária e bloqueio implementados pela empresa.	A autoridade conduziu testes práticos no portal e apontou a persistência de riscos de reidentificação mesmo após a pseudonimização automatizada.

(iv) Prestação de contas e acompanhamento posterior	Exigência de plano técnico de verificação etária e monitoramento contínuo da implementação das salvaguardas impostas.	Determinação de prestação de informações detalhadas sobre a implementação das novas diretrizes e das medidas técnicas adotadas pela Corte.
(v) Medidas pedagógicas e informacionais	Exigência de maior transparência informacional, revisão da política de privacidade e criação de mecanismos acessíveis de denúncia.	Emissão de novas diretrizes internas para orientar magistrados e servidores sobre anonimização e proteção de dados sensíveis.

3.1) Sugere-se, ainda, que os resultados dessa avaliação possam ser posteriormente compartilhados e debatidos no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), a fim de permitir a continuidade do diálogo técnico-institucional sobre desafios regulatórios relacionados à proteção de dados de crianças e adolescentes.

4) Este relatório vem, ainda, reiterar as conclusões e recomendações do GT1 de Educação da primeira fase, apresentadas de forma sintética abaixo, considerando a interconexão desse tema com o tema de trabalho deste GT2 e as diversas contribuições recebidas na direção de que a ANPD também se debruce ao tema da educação da proteção de dados no país (**ANEXO II - Resumo das Recomendações do GT Educação para DCAs e PPDs**).

4.1. Governança, articulação institucional e parcerias

- Fortalecimento de parcerias interinstitucionais com o Sistema de Garantia de Direitos, o Ministério da Educação (MEC), a comunidade escolar e conselhos da área.
- Estabelecimento de mecanismos formais de coordenação entre órgãos reguladores, educacionais e de proteção de direitos da criança e do adolescente.
- Estabelecimento de mecanismos de cooperação institucional para apoiar ações educativas, campanhas e programas nacionais de conscientização em proteção de dados.

4.2. Marco regulatório, instrumentos normativos e apoio à gestão escolar

- Criação de instrumentos regulatórios e orientativos voltados a gestores escolares, com diretrizes práticas para a adoção e o uso de tecnologias digitais em conformidade com a LGPD (p. 48).

- Elaboração de guias, modelos e parâmetros mínimos para contratação e uso de plataformas educacionais digitais.

- Fomento a um ambiente regulatório favorável à inovação, desde que seguro, proporcional e adequado à idade, especialmente no uso de tecnologias digitais na educação básica (p. 48).

4.3. Educação formal, capacitação e integração curricular

- Desenvolvimento de materiais didáticos oficiais sobre proteção de dados pessoais e LGPD, adaptados às diferentes etapas da educação básica (p. 48).

- Inserção estruturada e transversal do tema da proteção de dados e da privacidade nos currículos escolares (p. 48).

- Capacitação continuada de educadores e profissionais da educação para o tratamento responsável de dados pessoais no ambiente escolar.

- Criação de conteúdos específicos sobre proteção de dados voltados a grupos vulneráveis, considerando desigualdades sociais, digitais e educacionais (p. 50).

4.4. Alfabetização digital e desenvolvimento de competências para a cidadania digital

- Criação de um Programa Nacional de Alfabetização Digital para Proteção de Dados, inspirado no Safer Internet Programme europeu, contemplando:
    - Recursos educacionais adequados à faixa etária;
    - Ferramentas de avaliação, orientação e suporte para escolas e famílias;
    - Instrumentos para a promoção de hábitos digitais seguros, éticos e responsáveis.

- Promoção de estratégias amplas, contínuas e preventivas de conscientização sobre proteção de dados e privacidade, voltadas a crianças, adolescentes, famílias e educadores (p. 48), apontados focos temáticos como **prevenção à exposição excessiva ou abusiva de imagens de crianças e adolescentes e prevenção ao abuso e exploração sexual,** inclusive por meio de IA.

- Reforço à proposta do mandato prévio de criação do Dia Nacional da Proteção de Dados Pessoais.

4.5. Fiscalização, enforcement e responsabilização de agentes

- Ampliação da fiscalização do tratamento de dados pessoais em plataformas educacionais, públicas e privadas, utilizadas no ensino básico (p. 48).

- Intensificação da **fiscalização de grandes plataformas digitais** com provável acesso, atratividade ou impacto relevante sobre crianças e adolescentes (p. 48).

4.6. Canais de denúncia, resposta e proteção contra danos

- Criação e fortalecimento de canais de denúncia descentralizados para o combate a conteúdos ilegais e violações de direitos digitais de crianças e adolescentes, com financiamento previamente definido (p. 97);
- Estruturação de fluxos claros de resposta, encaminhamento e apoio às vítimas, com integração entre autoridades e organizações da sociedade civil (p. 97);
- Incentivos à expansão da rede de atendimento e ao fortalecimento dos canais de comunicação com o público infantojuvenil e suas famílias (p. 97);

4.7. Produção, sistematização e transparência de dados

- Coleta, sistematização e divulgação periódica de dados quantitativos e qualitativos sobre denúncias, violações e riscos relacionados à proteção de dados de crianças e adolescentes (p. 97);
- Uso desses dados para orientar políticas públicas, ações de fiscalização e estratégias educativas, garantindo transparência e prestação de contas (p. 97)

4.8. Engajamento social, comunicação pública e inovação participativa

- Realização de pesquisas e consultas com a participação de grupos vulneráveis, incluindo crianças e adolescentes, para identificar suas necessidades e desafios específicos em relação à proteção de dados pessoais (p. 65);
- Promoção de hackathons e iniciativas de inovação aberta voltadas à proteção de dados, segurança digital e soluções para o público infantojuvenil, incluindo protagonismo de estudantes, crianças e adolescentes (p. 65);
- Parcerias com organizações da sociedade civil, influenciadores, lideranças comunitárias e iniciativas existentes, para ampliar alcance e engajamento de ações de comunicação e conscientização (p. 61);
- Desenvolvimento de campanhas de conscientização pública sobre segurança e privacidade na internet, utilizando-se de estratégias de linguagem simples e acessível (p. 71);
- Garantia de campanhas massivas e contínuas direcionadas a estudantes, professores e famílias, com ênfase em boas práticas de segurança e privacidade online (p. 65);
- Uso de estratégias de engajamento, como desafios digitais, linguagem acessível e formatos participativos (p. 65);
- Participação em podcasts, lives e eventos públicos com personalidades e comunicadores de ampla audiência (p. 71)

5) Que o CNPD identifique a relevância perene dos temas afetos ao ECA Digital, notadamente diante da nova incumbência da ANPD como autoridade administrativa

autônoma responsável pela fiscalização e regulamentação da nova lei. Dessa forma, a recomendação segue na direção de que o CNPD aprofunde seus trabalhos e contribuições com a ANPD no que tange aos temas afetos ao ECA Digital.