

REVISTA JURÍDICA DO MPRO

Ano 2025 nº especial

ISSN 2595-3265 DOI:

Data de submissão: 16/09/2025

Data de Aprovação: 31/08/2025

O princípio da minimização de dados na LGPD: análise da aplicação à proteção de informações pessoais de crianças e adolescentes

The principle of data minimization in the LGPD: analysis of the application to the protection of personal information of children and adolescents

Lucas Lemes Sousa de Oliveira¹

Felipe Magno Silva Fonsêca²

1 Graduado em Direito pelo Centro Universitário São Lucas – RO. E-mail: lucaslemespvh@gmail.com.

2 Doutorando em Direito (PUC-PR). Mestre em Direito (UERJ). Especializações em: Proteção de Dados Pessoais: LGPD & GDPR (FMP); Direito Ambiental (Emeron); Direito Público (Uniderp); Gestão Pública (UEPB); Investigação Digital (Vincit - em curso). Graduação em Direito (UEPB). *Data Protection Officer (DPO)*, com certificação internacional EXIN. Promotor de Justiça no MPRO. Coordenador de Proteção de Dados Pessoais do MPRO. Coordenador do Núcleo de Enfrentamento a Crimes Cibernéticos (Nuciber-Gaeco). E-mail: felipe_magno_silva@hotmail.com.



Resumo

Na era digital, marcada pela conectividade constante e pelo uso intensivo de tecnologias, crianças e adolescentes estão inseridos desde cedo em ambientes virtuais, expostos a fluxos de informação, redes sociais e plataformas que moldam seus hábitos, relações e formas de aprendizado. Dessa forma, o presente artigo tem como objetivo analisar o princípio da minimização de dados à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), com ênfase na proteção de crianças e adolescentes em ambientes digitais. A partir de uma abordagem teórico-normativa, examina-se a centralidade do princípio da minimização na estrutura protetiva da LGPD e sua relação com os direitos fundamentais da infância, considerando o crescente uso da internet por esse público e os riscos associados à coleta massiva de dados pessoais. O trabalho também explora decisões recentes da Autoridade Nacional de Proteção de Dados (ANPD) e iniciativas legislativas em tramitação, notadamente o Projeto de Lei nº 4.474/2024, como instrumentos voltados à efetivação de práticas mais seguras e éticas de tratamento de dados no ecossistema digital infantojuvenil. Conclui-se que a minimização de dados se impõe como elemento estruturante da governança informacional, exigindo respostas normativas compatíveis com a condição de hipervulnerabilidade das crianças e com os princípios da proteção integral e da autodeterminação informacional.

Palavras-chave: LGPD; princípio da minimização; crianças e adolescentes; dados pessoais; hipervulnerabilidade.

Abstract

In the digital age, marked by constant connectivity and intensive use of technology, children and adolescents are immersed in virtual environments from an early age, exposed to information flows, social networks, and platforms that shape their habits, relationships, and learning styles. Therefore, this article aims to analyze the principle of data minimization in light of the General Personal Data Protection Law (LGPD), with an emphasis on the protection of children and adolescents in digital environments. Using a theoretical and normative approach, the article examines the centrality of the minimization principle in the LGPD's protective framework and its relationship with children's fundamental rights, considering the growing use of the internet by this population and the risks associated with the mass collection of personal data. The paper also explores recent decisions by the National Data Protection Authority (ANPD) and pending legislative initiatives, notably Bill No. 4474/2024, as instruments aimed at implementing safer and more ethical data processing practices in the digital ecosystem for children and adolescents. It is concluded that data minimization is essential as a structuring element of informational governance, requiring normative responses compatible with the hypervulnerable condition of children and with the principles of comprehensive protection and informational self-determination.

Keywords: LGPD; data minimization; children and adolescents; personal data; hypervulnerability.



Introdução

A centralidade da informação como ativo estratégico na sociedade contemporânea impõe novos desafios à proteção dos direitos fundamentais, especialmente no que se refere à privacidade e à autodeterminação informacional. Em um contexto marcado pela intensificação da coleta e do tratamento automatizado de dados pessoais, a proteção da infância torna-se um eixo sensível e prioritário da agenda regulatória. Crianças e adolescentes, por sua condição peculiar de desenvolvimento, estão particularmente expostos aos riscos da vigilância digital, da formação precoce de perfis comportamentais e da exploração comercial de suas interações *online*.

Diante desse cenário, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) institui um conjunto de princípios e regras voltados à contenção dos excessos informacionais, entre os quais se destaca o princípio da minimização. Previsto no artigo 6º, inciso III, esse princípio estabelece que o tratamento de dados deve limitar-se ao mínimo necessário para a realização de suas finalidades, constituindo verdadeiro parâmetro normativo de proporcionalidade.

À vista desse cenário, este artigo pretende investigar a seguinte questão: de que forma o princípio da minimização de dados pode ser efetivado por instrumentos normativos e mecanismos legais, a fim de garantir uma proteção tangível aos dados pessoais de crianças e adolescentes no ambiente digital? A relevância desta investigação justifica-se pela ubiquidade digital na vida infantojuvenil e pelos riscos concretos decorrentes da coleta massiva de dados, que ameaçam direitos fundamentais como a privacidade, a autonomia e o livre desenvolvimento da personalidade.

Para responder ao problema de pesquisa, este trabalho tem como propósito central analisar a efetivação do princípio da minimização de dados, previsto no art. 6º, III, da LGPD, como instrumento de proteção aos dados pessoais de crianças e adolescentes no ambiente digital. Para tanto, busca-se analisar os fundamentos constitucionais da proteção de dados e o arcabouço principiológico da LGPD; compreender o regime jurídico de proteção integral da criança e do adolescente e sua aplicação ao ambiente digital; identificar os riscos concretos associados ao tratamento de dados infantojuvenis, por meio de casos recentes apurados pela ANPD; e verificar a interseção entre a hipervulnerabilidade desse público e o princípio da minimização, examinando as ferramentas legais para sua efetivação.

Quanto à metodologia, o presente trabalho adota a abordagem qualitativa, amparando-se em pesquisa bibliográfica e documental. Examina-se a doutrina especializada, a legislação pertinente, com ênfase na LGPD e no ECA, e decisões recentes da Autoridade Nacional de Proteção de Dados (ANPD), visando oferecer um diagnóstico crítico e normativamente fundamentado da aplicação do princípio da minimização à luz da proteção infantojuvenil.

O texto está estruturado em quatro seções e uma conclusão. A primeira examina os fundamentos constitucionais da proteção de dados e as diretrizes gerais da LGPD. A segunda investiga o arcabouço normativo de proteção infantojuvenil, incluindo tratamentos com riscos



agravados. A terceira analisa a dimensão digital da infância, com foco na realidade de acesso, nos riscos do tratamento de dados e em casos concretos. Por fim, a quarta seção verifica a interseção entre o princípio da minimização e a hipervulnerabilidade do público infantojuvenil, examinando as ferramentas legais disponíveis que viabilizam a sua efetivação.

1 Do reconhecimento à efetivação: a proteção de dados como direito fundamental no Brasil

A proteção de dados pessoais no Brasil deve ser compreendida a partir da base fundante do direito à privacidade, historicamente consolidado no ordenamento jurídico. A Constituição Federal, em seu art. 5º, inciso X, garante que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;” (Brasil, 1988), estruturando um espaço de resguardo contra interferências indevidas. Complementarmente, o inciso XII do mesmo artigo estabelece a inviolabilidade do sigilo das comunicações, incluindo dados, reforçando a centralidade da privacidade no ordenamento jurídico brasileiro (Brasil, 1988).

Com a ampliação das dimensões dos direitos da personalidade, torna-se evidente a conexão estrutural entre dados pessoais e sua proteção, contexto em que a tutela informacional emerge como desdobramento do direito à privacidade. Nesse sentido, Doneda (2011, p. 94) esclarece:

A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

A centralidade dos dados pessoais na configuração moderna também é destacada por Basan (2022, p. 196), ao afirmar que, atualmente:

[...] parte da personalidade da pessoa humana é constituída de dados [...], e é por isso que é possível defender que a proteção de dados pessoais é hoje uma nova espécie de direito da personalidade, capaz de auxiliar na garantia da dignidade, paridade, não discriminação e liberdade da pessoa humana constituindo, também, nítido direito fundamental.

Essa centralidade dos dados na constituição da identidade pessoal se acentuou com os avanços da globalização e da revolução tecnológica, transformando profundamente os modos de interação social, econômica e institucional (Fonsêca, 2023). O cotidiano passou a ser permeado por dados, os quais se ajustam continuamente às preferências do usuário, muitas vezes sem seu conhecimento consciente. Harari (2023, p. 341) sintetiza essa lógica ao afirmar que:

Todos os dias, bilhões de seres humanos realizam numerosas transações com os gigantes da tecnologia, mas não dá para adivinhar olhando para as nossas contas bancá-



rias, porque é como se nenhum dinheiro saísse do lugar. Recebemos informações dos gigantes da tecnologia e lhes pagamos com informações.

Nessa perspectiva, a proteção de dados surge como resposta normativa à insuficiência da tutela dos direitos da personalidade em uma sociedade marcada pela “vigilância líquida”. Este fenômeno, conforme Lyon interpreta Bauman no prefácio da obra homônima, caracteriza-se por um controle fluido e descentralizado, no qual dados pessoais são coletados e reutilizados de maneira imprevisível, adaptando-se às lógicas contemporâneas do consumo, da mobilidade e da insegurança (Bauman, 2014).

Esse cenário impulsionou o fortalecimento da leitura constitucional da proteção de dados, culminando na promulgação da Emenda Constitucional nº 115/2022, que inseriu o inciso LXXIX ao artigo 5º da Constituição Federal, estabelecendo que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (Brasil, 2025).

No entanto, ainda que a Emenda Constitucional nº 115, de 2022, tenha positivado expressamente a proteção de dados pessoais no rol dos direitos fundamentais, tal reconhecimento já havia sido antecipado pelo Supremo Tribunal Federal. Em decisão proferida em maio de 2020, o Plenário da Corte reconheceu a proteção de dados pessoais como direito fundamental autônomo, ao referendar medida cautelar que suspendeu a eficácia da Medida Provisória nº 954/2020.

Essa medida previa o compartilhamento massivo de dados de usuários de telefonia com o IBGE, o que levou o STF a consolidar um novo paradigma: o reconhecimento da proteção de dados como direito fundamental independente daquele à privacidade, este último, tradicionalmente concebido como garantia de abstenção do Estado frente à esfera individual. Na ocasião, a Ministra Rosa Weber ressaltou que o compartilhamento de dados pessoais sem mecanismos adequados de salvaguarda “descumpra as exigências que exsurge do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros” (Brasil, 2020, p. 3).

Diante desse contexto, foi sancionada a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), em 14 de agosto de 2018, com início de vigência em 1º de agosto de 2020. Essa legislação tem como finalidade central a regulamentação do tratamento de dados pessoais, fixando princípios orientadores, diretrizes operacionais e assegurando uma série de direitos individuais relacionados à proteção da privacidade e da informação, representando a concretização legislativa de um regime normativo voltado a enfrentar os desafios impostos pelo tratamento de dados na era digital.

Botelho (2020, p. 202), ao analisar os fundamentos da LGPD, afirma que “a proteção aos dados pessoais ofertada pela LGPD tem como objetivo a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural”. Essa afirmação evidencia que a LGPD se apoia em fundamentos constitucionais para efetivar, no ambiente digital, o direito fundamental à privacidade e à autodeterminação informacional³.

3 A autodeterminação informativa, conforme Leonardo Roscoe Bessa (2020), refere-se ao direito fundamental que todo indivíduo possui de controlar seus próprios dados pessoais. Esse conceito está intimamente ligado



Segundo Bioni (2021), a LGPD, assim como as demais leis de proteção de dados, se caracteriza por sua elevada complexidade e não se limita a regular um setor específico, vez que abrange todas as atividades econômicas que envolvem o uso de dados pessoais, tanto no setor público quanto no privado.

Diante desse cenário, torna-se evidente que o uso da tecnologia por crianças e adolescentes impõe diversos desafios à garantia dos seus direitos. Por conseguinte, em razão da exigência jurídica e ética que se avulta diante da crescente exploração informacional, os ordenamentos jurídicos brasileiro e internacional convergem no sentido de conferir especial atenção ao tratamento de dados desses indivíduos vulneráveis, consoante destacado no tópico seguinte.

2 Visão geral das leis e atos normativos voltados à tutela da criança e adolescente na internet

Visando à adequada concatenação de ideias e fluidez da pesquisa, é imprescindível, doravante, analisar os instrumentos jurídicos do Brasil e do exterior voltados à proteção de crianças e adolescentes no âmbito digital, com o fim de aclarar o regime jurídico aplicável a esses sujeitos, uma vez que a condição de vulnerabilidade demanda proteção diferenciada, com o objetivo de promover seu desenvolvimento integral.

Internacionalmente, a Convenção sobre os Direitos da Criança, ratificada pelo Brasil, estabelece em seu artigo 16 que “nenhuma criança deve ser submetida a interferências arbitrárias ou ilegais em sua vida particular, sua família, seu domicílio ou sua correspondência, nem a ataques ilegais à sua honra e à sua reputação” (Brasil, 1990).

Complementarmente, no âmbito digital, o Comentário Geral nº 25 do Comitê sobre os Direitos da Criança da ONU reconhece que o “[...] ambiente digital não foi originalmente desenvolvido para crianças, mas desempenha um papel significativo na vida das crianças” (Alana; São Paulo, 2022, p. 49), devendo os Estados partes “assegurar que, em todas as ações relativas ao fornecimento, regulação, *design*, gestão e uso do ambiente digital, o melhor interesse de cada criança seja uma consideração primordial” (São Paulo, 2022, p. 49).

Em consonância com os instrumentos internacionais, o ordenamento jurídico brasileiro organiza a proteção digital de crianças e adolescentes a partir de um sistema normativo hierarquizado, cujo fundamento se estabelece no artigo 227 da Constituição Federal, que dispõe ser:

[...] dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão (Brasil, 1988).

à noção de privacidade e proteção de dados na era digital, garantindo que as pessoas tenham autonomia sobre como suas informações são coletadas, utilizadas e compartilhadas.



Tal diretriz é concretizada no plano infraconstitucional pela Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente – ECA), na medida em que o *caput* do artigo 1º incorpora, de maneira clara, a doutrina da proteção integral, reafirmando a transformação normativa inaugurada pela Constituição de 1988 a fim de reconhecer crianças e adolescentes como titulares plenos de direitos, cuja condição peculiar de desenvolvimento demanda proteção especial e abrangente, a ser promovida de forma articulada entre Estado, família e sociedade.

Em conformidade com os ensinamentos de Amin *et al* (2019), a proteção integral pode ser definida como um sistema jurídico composto por normas interligadas, orientadas por um valor ético fundamental, cuja base se encontra no artigo 227 da Constituição Federal e que se harmoniza com a dignidade da pessoa humana como princípio estruturante.

Exemplificativamente, o art. 17 do ECA assegura o direito ao respeito, entendido como a inviolabilidade da integridade moral, incluindo a preservação da imagem, da identidade e da intimidade do infante. Esses dispositivos, embora anteriores à concepção moderna de dados pessoais, já estabeleciam fundamentos jurídicos para a proteção da identidade e da intimidade no ambiente digital, conforme reinterpretados pela Resolução CONANDA nº 245/2024, que dispõe “a privacidade de crianças e adolescentes deve ser respeitada e protegida, por padrão, em todos os ambientes e serviços digitais, inclusive quanto ao tratamento e armazenamento de seus dados pessoais” (Brasil, 2024a).

No campo específico da proteção de dados infantojuvenil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), ao tratar expressamente, em seu artigo 14, do tratamento de dados pessoais de crianças e adolescentes, afirma que tal ato “deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente” (Brasil, 2018).

Destaca-se a exigência prevista no art. 14, §1º, da LGPD, segundo a qual o tratamento de dados pessoais de crianças torna imprescindível o “consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal” (Brasil, 2018). Adicionalmente, o § 5º dispõe de maneira complementar que “o controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis” (Brasil, 2018).

Sob a mesma inteligência, a regulação norte-americana, por meio da *Children’s Online Privacy Protection Act* (COPPA), impõe a obrigatoriedade de consentimento parental verificável para o tratamento de dados de crianças menores de 13 anos, conferindo à família papel central na autorização e fiscalização do uso de dados por provedores *online* (Wright, 2024).

Apesar das normativas que proíbem a participação de menores de 13 anos em redes sociais, a ausência de mecanismos eficazes de verificação de idade e de consentimento parental torna essa restrição ineficaz.

Diante dessa fragilidade operacional – que expõe crianças a riscos sistêmicos mesmo com previsões legais, o Projeto de Lei nº 4.474/2024, atualmente em tramitação na Câmara dos



Deputados, propõe uma inovação normativa ao alterar o Estatuto da Criança e do Adolescente. Inspirado no modelo da COPPA, o projeto reforça o papel da família no controle do acesso digital, ao introduzir o art. 79-A, que consagra a obrigação de acompanhamento direto e contínuo das atividades *online* de crianças e adolescentes, nos seguintes termos “todo acesso à internet por criança ou adolescente dever ser monitorado pelos pais ou responsável. Parágrafo único. O monitoramento pode se dar presencialmente ou por meio de ferramentas tecnológicas de supervisão parental” (Brasil, 2024d, art. 79-A).

Essa presunção protetiva procura substituir a lógica reativa do consentimento por um modelo preventivo, alinhado ao melhor interesse do art. 14 da LGPD.

Todavia, a exigência de consentimento como fundamento primário para o tratamento de dados enfrenta críticas, especialmente no que concerne à sua efetividade prática, uma vez que:

Enabling parental consent to substitute for children's consent may be one way of ensuring children's rights are protected, but given the shortfall in digital literacy for adults, particularly in emerging markets and developing countries, parents' consent may not always be an effective way to protect the privacy rights of children (Unicef, 2022 p. 14)⁴.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) publicou o Enunciado CD/ANPD nº 1 (2023), buscando padronizar as interpretações sobre a aplicação de atos normativos para a tutela de dados pessoais do público infantojuvenil, ressaltando, de forma expressa, que:

O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei (Brasil, 2023).

É nesse entrecruzamento de atos normativos que se consolidam as bases para um modelo jurídico que compreenda a proteção de dados infantojuvenis como instrumento de promoção da dignidade humana, e não meramente como restrição à inovação tecnológica.

Contudo, apesar do avanço do aparato normativo, persiste o desafio de efetivar concretamente os direitos das crianças no ambiente digital, tendo em vista que, em muitos momentos, a legislação revela limitações para acompanhar a fluidez e a velocidade das transformações sociais contemporâneas. O mesmo pensamento é compartilhado por Özkul, Vosloo e Baghdasaryan ao determinar que:

[...] fully realizing the child's best interests requires considering the short-, medium-, and long-term impacts of decisions on a child's development over time. While the challenge of forecasting the future complicates best interests assessments in many fields, making them reliant on existing facts and circumstances, the digital envi-

4 Permitir que o consentimento dos pais substitua o das crianças pode ser uma forma de garantir a proteção dos direitos infantis. No entanto, considerando a deficiência na alfabetização digital dos adultos —especialmente em mercados emergentes e países em desenvolvimento—, o consentimento dos pais nem sempre será um método eficaz para proteger os direitos à privacidade das crianças (Tradução própria).



ronment is unique due to its rapid evolution. This creates a different dynamic when applying the Principle in such a fast-paced environment where legislations and regulations need to be future-proof, and where research needs to follow the technological changes rapidly (2025 p. 17)⁵.

Diante desta dificuldade de eficácia das normas do tipo regra, impõe-se a fundamentação em princípios jurídicos estruturantes que possam assegurar proteção integral aos modernos mecanismos de coleta e tratamento de dados, particularmente no contexto digital contemporâneo, onde imperam relações assimétricas de poder e a mercantilização de dados pessoais.

3 A dimensão digital da infância: realidade de acesso, tratamento de dados e riscos

Para dimensionar a urgência do problema, vale olhar os dados atuais sobre o uso da internet por crianças e adolescentes, os quais revelam tanto a ubiquidade dessas tecnologias na infância, quanto os perigos já materializados. Tal cenário exige que se vá além dos números, compreendendo as estruturas invisíveis que sustentam esse ambiente digital.

Dessa forma, com o objetivo de compreender esse público vulnerável no âmbito digital, a recente edição da pesquisa *TIC Kids Online Brasil* (2024) aponta que a grande maioria dos brasileiros entre 9 e 17 anos já utiliza a internet, totalizando aproximadamente 24,5 milhões de usuários, sendo o celular o principal meio de acesso entre esse público.

A pesquisa também aponta que o *WhatsApp* é a plataforma digital mais utilizada por crianças e adolescentes de 9 a 17 anos (71%), seguido pelo *YouTube* (66%), *Instagram* (60%) e *TikTok* (50%). A frequência de uso varia conforme a idade: entre os mais jovens, de 9 a 10 anos (70%) e de 11 a 12 anos (71%), o *YouTube* predomina; já os adolescentes de 13 e 14 anos acessam mais o *Instagram* (78%) e o *WhatsApp* (73%); enquanto na faixa de 15 a 17 anos, o *WhatsApp* (91%) e o *Instagram* (81%) são os mais recorrentes (*TIC Kids Online Brasil*, 2024).

Nesse contexto, é necessário reconhecer que, apesar do elevado número de crianças presentes na internet, essa não deve ser interpretada como um ambiente neutro de interação, mas sim como um ecossistema estruturado por dinâmicas de consumo e pela extração massiva de dados pessoais. Esse fenômeno é elucidado por Zuboff (2018, p. 18), ao descrever o chamado capitalismo de vigilância, definindo-o como “*new form of information capitalism aims to predict and modify human behavior as a means to produce revenue and market control*”⁶.

5 [...] garantir plenamente o melhor interesse da criança exige que se considerem os impactos de curto, médio e longo prazo das decisões sobre o seu desenvolvimento ao longo do tempo. Embora a dificuldade de prever o futuro torne complexa a avaliação do melhor interesse em diversas áreas — fazendo com que ela dependa de fatos e circunstâncias já conhecidos —, o ambiente digital é singular devido à sua evolução acelerada. Isso cria uma dinâmica diferente na aplicação desse princípio em um contexto tão dinâmico, onde as leis e regulamentações precisam ser à prova de futuro e as pesquisas devem acompanhar as mudanças tecnológicas com agilidade (Tradução própria).

6 Uma nova forma de capitalismo informacional visa prever e modificar o comportamento humano como meio de gerar lucro e controle de mercado (Tradução própria).



Ou seja, tal lógica, ao incidir sobre indivíduos em condição peculiar de desenvolvimento que, progressivamente, ocupam o espaço digital, fragiliza a proteção integral assegurada pelo ordenamento jurídico, expõe crianças e adolescentes, hipervulneráveis nesse ecossistema, a riscos sistêmicos como a exploração comercial de dados proibida expressamente no art. 15 da Resolução CONANDA nº 245/2024, ao dispor que:

Os dados pessoais de crianças e adolescentes não devem ser utilizados para fins comerciais, como criação e definição de perfis de comportamento, consumo e segmentação mercadológica, tampouco para direcionamento de publicidade ou ampliação de seu alcance, conforme disposto na Resolução CONANDA nº 163 de 13 de março de 2014 (Brasil, 2024a).

O fato é que as plataformas digitais utilizadas pelo público infantojuvenil funcionam com base em sistemas algorítmicos que estimulam a produção constante de conteúdos por parte dos usuários, inclusive crianças e adolescentes. Esses mecanismos não apenas viabilizam a participação digital, mas “estimula a superexposição das crianças e adolescentes por meio dos recursos de engajamento (curtidas, compartilhamentos, números de visualizações, números de seguidores ou inscritos, etc.)” (Frazão, 2021, p. 96).

No mesmo sentido, em entrevista à Agência Brasil, Pedro Hartung, diretor do Instituto Alana, faz uma análise crítica sobre os riscos digitais para crianças e adolescentes, ao destacar que:

A gente acha que o espaço digital das plataformas digitais é um ambiente como se fosse uma praça pública, em que a criança e a família estão lá para brincar, com essa ideia ilusória de que aquilo é um espaço público democrático. Mas não é. A arquitetura digital foi pensada para viciar, para engajar na economia da atenção e prender crianças e adolescentes, explorando-as comercialmente (Hartung, 2025).

Não por acaso, casos concretos demonstram a importância de cuidados específicos no tratamento de dados pessoais do público infantojuvenil. A Autoridade Nacional de Proteção de Dados (ANPD), entidade incumbida de garantir a salvaguarda dos dados pessoais no território brasileiro, instaurou procedimento investigativo com base em denúncias relacionadas à plataforma TikTok, acusada de tratar dados pessoais de crianças e adolescentes em desconformidade com os princípios da legislação vigente (Brasil, 2024b). Conforme apurado pela Coordenação-Geral de Fiscalização, na Nota Técnica nº 6/2023, “a atuação do *TikTok* estaria em desacordo com os princípios elencados no art. 6º da LGPD, especialmente os de finalidade, adequação, necessidade, livre acesso e transparência” (ANPD, 2023, p. 1).

O caso investigou a forma como a plataforma realizava o tratamento de dados mesmo de usuários não cadastrados. Tal prática ocorria por meio do chamado “*feed* sem cadastro”, funcionalidade que permitia a coleta e processamento de informações técnicas e comportamentais de crianças sem qualquer mecanismo robusto de verificação etária ou consentimento válido (Brasil, 2024). A Nota Técnica nº 50/2024 evidenciou que a:



Violação ao dever de demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas, em contraposição ao disposto no art. 6º, X, LGPD. A ByteDance, ao permitir o acesso universal à plataforma TikTok por meio do feed sem cadastro, **de modo a otimizar o seu modelo de negócio, baseado no tratamento intensivo de dados pessoais de usuários**, sem que fossem adotados quaisquer mecanismos técnicos de segurança que evitassem a interação de crianças e adolescentes, deixou de se assumir responsabilidade razoavelmente esperada do controlador, consoante o disposto no art. 49, LGPD (ANPD, 2024, p. 21) (grifo nosso).

Entre os dados coletados pela plataforma estavam endereço IP, modelo do dispositivo, sistema operacional, padrões de uso e comportamento, elementos que, ainda que não identifiquem diretamente o titular, são considerados dados pessoais nos termos do artigo 5º, I e II, da LGPD, por permitirem a criação de perfis individualizados (ANPD, 2024).

Diante da gravidade das infrações e da ausência de mecanismos eficazes de mitigação de riscos, a ANPD determinou à empresa ByteDance, controladora do *TikTok*, a desativação da funcionalidade “*feed* sem cadastro” e a apresentação de plano de conformidade (Brasil, 2024b). Reforçou, ainda, que “essa prática pode acarretar danos irreparáveis a um público altamente vulnerável” (ANPD, 2024, p. 8), reafirmando o papel do Estado na contenção de práticas lesivas e na regulação de ambientes digitais que impactam diretamente o desenvolvimento físico, psíquico e moral de crianças e adolescentes.

De forma similar, em dezembro de 2024, a ANPD ordenou à empresa *X. Corp* a interrupção imediata do uso de dados de crianças e adolescentes no treinamento de sistemas de inteligência artificial generativa. Por meio do Despacho Decisório nº 29/2024/FIS/CGF, a ANPD determinou que a empresa excluísse dos Termos de Uso a expressão “para qualquer finalidade”, por entender que tal formulação é genérica e viola o princípio da especificidade da finalidade previsto na LGPD. Além disso, ordenou a interrupção do tratamento de dados pessoais de usuários menores de 18 anos no Brasil para fins de treinamento de sistemas de inteligência artificial generativa pela empresa *X* (Brasil, 2024c).

Além disso, a coleta de dados de crianças e adolescentes pode ocorrer por diversas vias, extrapolando os meios digitais tradicionais, inclusive por meio de brinquedos inteligentes conectados à internet, em que os dados pessoais coletados assumem o papel de contrapartida implícita na relação entre o usuário e o serviço.

Os chamados “brinquedos conectados” também representam pontos críticos. Leal (2017, p. 180) observa que falhas técnicas nestes produtos permitem a coleta invisível de dados sensíveis, colocando a criança sob risco dentro do próprio ambiente familiar. Nas palavras da autora:

Há riscos de que o brinquedo conectado via bluetooth ou wi-fi possa se transformar em um espião dentro do quarto da criança [...], enviando seus dados sem o consentimento dos pais. [...] Questiona-se, assim, a segurança dos dados coletados pelas empresas por intermédio desse tipo de produto, sobretudo pela falta de transparência associada à vulnerabilidade fática e técnica do próprio usuário (Leal, 2017, p. 180).



Verifica-se, portanto, a existência de um ecossistema digital em que crianças e adolescentes interagem continuamente por meio de dispositivos conectados à internet, nos quais o tratamento de dados ocorre de forma permanente e, muitas vezes, invisível.

As informações são utilizadas para fins mercadológicos, em uma lógica que opera sob a dinâmica da gratuidade aparente. Conforme destaca Bioni (2025), diversos serviços digitais, embora disponibilizados sem cobrança direta aos usuários, exemplificadamente as redes sociais, baseiam-se na coleta de dados pessoais como forma de contraprestação. Esses dados alimentam mecanismos de personalização e direcionamento publicitário, cuja monetização sustenta financeiramente a manutenção e o crescimento das plataformas.

Tal cenário acentua a condição de hipervulnerabilidade desses sujeitos, que se intensifica diante da consolidação e expansão progressiva das tecnologias de captação e análise de informações.

4 Ferramentas legais para efetivar a minimização de dados: uma análise dos mecanismos de proteção infantojuvenil na LGPD e legislação correlata

Os princípios jurídicos são norteadores fundamentais do ordenamento, servindo como alicerces para interpretação e aplicação das normas. Como define Mello (2015 p. 54):

Princípio é, pois, por definição, mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas, compondo-lhes o espírito e servindo de critério para exata compreensão e inteligência delas, exatamente porque define a lógica e a racionalidade do sistema normativo, conferindo-lhe a tônica que lhe dá sentido harmônico.

Em outras palavras, princípios expressam os valores e fins maiores que permeiam o ordenamento e orientam todas as etapas de aplicação da lei. No contexto da proteção de dados pessoais, os princípios adquirem papel ainda mais crucial, pois atuam como instrumentos de tutela fundamentais, diante de rápidas evoluções tecnológicas e eventuais lacunas ou defasagens legislativas.

Nesse sentido, a LGPD se ancora em uma base principiológica que articula liberdade, privacidade e transparência, aliada a fundamentos e diretrizes técnicas voltadas à regulamentação concreta do tratamento de dados. Entre os princípios consagrados no artigo 6º, destaca-se o princípio da minimização dos dados, previsto no inciso III, que determina que o tratamento deve se restringir “[...] ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (Brasil, 2018).

Quanto à nomenclatura adotada, Iuri Pinheiro e Vólia Bomfim (2022, p.40) esclarecem que “embora denominado pela LGPD como Princípio da Necessidade, essa última premissa também vem sendo denominada de Princípio da Minimização”.



O caráter estruturante e normativo desse princípio foi explicitamente reconhecido pelo Supremo Tribunal Federal (STF) ao julgar conjuntamente a Ação Direta de Inconstitucionalidade (ADI) 6649, ocasião em que validou o compartilhamento de dados entre entes públicos desde que observados os parâmetros estabelecidos pela LGPD, especialmente o princípio da minimização, reforçando requisitos como finalidade legítima, transparência, controle de acesso, justificativa formal e responsabilização em casos de uso abusivo, conforme assentado expressamente pela Corte na manifestação jurisprudencial (STF, 2024), cujos termos são esclarecedores:

Ementa: DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS. 1. A Ação Direta de Inconstitucionalidade é cabível para impugnação do Decreto 10.046/2019, uma vez que o ato normativo não se esgota na simples regulamentação da Lei de Acesso à Informação e da Lei Geral de Proteção de Dados Pessoais, mas inova na ordem jurídica com a criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados. [...] O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); **c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.** [...] 8. O tratamento de dados pessoais promovido por órgãos públicos que viole parâmetros legais e constitucionais, inclusive o dever de publicidade fora das hipóteses constitucionais de sigilo, importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa. 9. Declaração de inconstitucionalidade, com efeitos pro futuro, do art. 22 do Decreto 10.046/2019. O Comitê Central de Governança de Dados deve ter composição independente, plural e aberta à participação efetiva de representantes de outras instituições democráticas, não apenas dos representantes da Administração Pública federal. Ademais, seus integrantes devem gozar de garantias mínimas contra influências indevidas. (ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15-09-2022, PROCESSO ELETRÔNICO DJe-s/n DIVULG 16-06-2023 PUBLIC 19-06-2023) (Brasil, 2022) (Grifo nosso).

No contexto infantojuvenil, a aplicação do princípio da minimização de dados exige atenção redobrada por parte dos controladores, que devem adotar práticas restritivas e orientadas por normas claras, considerando que as crianças estão “submetidas de maneira desigual à coleta precoce, expostas ao risco associado e subtraídas da possibilidade de desenvolver autodeterminação informacional em razão de sua vulnerabilidade” (Instituto Alana; Internetlab, 2020, p. 180).

Sob a mesma inteligência, o § 4º do art. 14 da LGPD proíbe expressamente os controladores de condicionar a participação de crianças e adolescentes em jogos, aplicativos de internet



ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à finalidade daquela atividade (Brasil, 2018).

Ademais, a Resolução nº 245/2024 do CONANDA consolida tal princípio no parágrafo único do art. 12, ao estabelecer que “será recolhida apenas a quantidade mínima de dados pessoais para os fins de uso do serviço, cujo armazenamento deverá durar apenas o tempo necessário para a finalidade da coleta” (Brasil, 2024a).

Impõe-se, conseqüentemente, uma tutela sob o olhar do melhor interesse da criança, tendo em vista que a coleta de dados não pode ser guiada apenas por interesses econômicos do serviço, mas deve priorizar a condição de vulnerabilidade da criança e a sensibilidade de seus dados pessoais. Nessa direção, Fernandes e Medon (2021, p. 18) sustentam que:

Se essa vedação já é importante para pessoas adultas sujeitas a contratos de adesão em que fornecem seus dados em troca do acesso a funcionalidades, mais ainda deve ser a proteção conferida a essas pessoas em desenvolvimento, haja vista a ínsita vulnerabilidade e a gravidade dos danos que podem advir do tratamento de seus dados [...]

Não obstante o elevado grau de abstração que permeia o princípio da minimização, sua concretização se ampara em arcabouço legal específico na medida em que a LGPD confere aos controladores e operadores margem de discricionariedade para instituir políticas públicas voltadas à proteção desse público (Oliveira, 2021). Destaca-se, nesse contexto, o art. 50, que autoriza e estimula a adoção dessas medidas de governança, oferecendo instrumentos normativos capazes de converter o princípio em práticas efetivas no tratamento de dados pessoais, aos dispor sobre a possibilidade de:

[...] formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Brasil, 2018).

Ademais, o § 1º do dispositivo em comento determina que:

[...] Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular (Brasil, 2018).

Além das diretrizes de boas práticas previstas no art. 50, a própria LGPD institui instrumentos operacionais que reforçam a tutela infantojuvenil. Nesse sentido, faz-se presente o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), cujo conceito figura no art. 5º, XVII, como “[...] documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (Brasil, 2018).



Ao exigir avaliação prévia de riscos e salvaguardas proporcionais, o Relatório de Impacto à Proteção de Dados (RIPD) e as regras de boas práticas e de governança previstas no art. 50 da LGPD operam como instrumentos complementares que, sob a ótica do princípio da minimização, transformam diretrizes abstratas em obrigações verificáveis voltadas à coleta de informações de crianças e adolescentes.

Segundo Angelini et al. (2023), o Estado deve implementar políticas públicas educativas que promovam o uso seguro da internet por crianças e adolescentes, incluindo a inserção de conteúdos sobre privacidade e proteção de dados nos currículos escolares.

Tal exigência concretiza, em chave digital, a vedação já imposta pelo Código de Defesa do Consumidor, que considera abusiva a publicidade dirigida à criança quando dela se aproveita para induzir comportamentos prejudiciais e, ainda, proíbe práticas que explorem sua vulnerabilidade etária para fins mercadológicos, nos termos dos arts. 37, §2º, e 39, IV, respectivamente:

§ 2º É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeite valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança. [...] IV - prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços (Brasil, 1990).

Além disso, o Projeto de Lei nº 4.474/2024 promove uma transição crucial ao converter o princípio abstrato da minimização de dados em protocolos técnicos concretos voltados à proteção digital infantojuvenil. Seu núcleo inovador reside na instituição de ambientes digitais certificados, os quais impõem:

[...] § 2º Os ambientes certificados mencionados no caput devem, ao menos: I – ser certificados por entidades independentes; II – oferecer classificação etária indicativa dos conteúdos que podem ser acessados; III – ser seguros em relação a interação entre usuários e em relação a eventual publicidade de produtos ou serviços; IV – oferecer controle parental das atividades das crianças e adolescentes; e V – estabelecer mecanismos de registro e supervisão de comunicação entre os usuários (Brasil, 2024d).

Além disso, o art. 10-A do mesmo projeto estabelece presunção protetiva infantil, exigindo verificação de idade e salvaguardas imediatas ao determinar que,

[...] Até que seja confirmada a idade do titular dos dados, o controlador deve assumir que os dados coletados são de criança e adolescente. Parágrafo único. A confirmação mencionada no caput pode ser realizada uma única vez e refeita periodicamente caso haja indícios de que o titular dos dados seja criança ou adolescente (Brasil, 2024d).

Essa limitação intencional é fundamental para garantir um ambiente digital livre de manipulação algorítmica, preservando a autonomia de crianças e adolescentes frente às dinâmicas mercadológicas. Assim, neutraliza-se a pressão econômica por captura massiva de dados, assegurando desenvolvimento livre de perfis preditivos que limitam escolhas futuras e



proporcionando, dessa forma, a “[...] proteção e a garantia de direitos básicos e fundamentais, como o livre desenvolvimento da personalidade, a autodeterminação informativa, a privacidade e intimidade, não devem ser preteridos ou ignorados em prol do avanço tecnológico” (Duarte; Nascimento, 2023, p. 238).

Evita-se, outrossim, que os dados do público infantojuvenil “[...] sejam mapeados e tenham suas preferências e escolhas pregressas utilizadas e manipuladas, preservando, dessa forma, sua liberdade na construção da própria identidade e o livre desenvolvimento da personalidade” (Teixeira; Rettore, 2021, p. 277).

Assim, a concretização do princípio atua como ponte entre os dispositivos legais gerais e a efetiva proteção da privacidade infantojuvenil, desempenhando não apenas uma função restritiva formal, mas, sobretudo, configurando-se como instrumento essencial à salvaguarda da autonomia e da privacidade de crianças e adolescentes no ambiente digital.

Considerações finais

A análise empreendida ao longo deste artigo evidenciou que o princípio da minimização de dados, embora formalmente consagrado no art. 6º, III, da LGPD, ainda carece de efetivação plena quando se trata da proteção de informações pessoais de crianças e adolescentes no ambiente digital, a despeito da robusta arquitetura normativa – que abrange a Constituição Federal, o Estatuto da Criança e do Adolescente, a LGPD e resoluções específicas.

Ficou demonstrado que as crianças e adolescentes, em razão de sua condição peculiar de desenvolvimento, encontram-se em situação de hipervulnerabilidade diante de práticas digitais que priorizam modelos econômicos baseados na extração massiva de dados. Casos como os que envolveram o *TikTok* e a *X. Corp* exemplificam a dificuldade de se impor limites concretos à atuação de plataformas digitais quando o controle estatal ainda é fragmentado, reativo e, por vezes, desprovido de instrumentos coercitivos eficazes.

Nesse contexto, o princípio da minimização de dados antecede a própria coleta, ultrapassando a mera conformidade com finalidades técnicas. Ele se configura como um instrumento de proteção que desloca a perspectiva: a criança e o adolescente não devem ser concebidos como repositórios de dados exploráveis, mas como sujeitos hipervulneráveis cuja proteção demanda coleta estritamente necessária e tratamento proporcional.

Essa diretriz, fundada na condição peculiar de desenvolvimento, concretiza-se por meio de instrumentos normativos e políticas públicas que operacionalizam o princípio em ações concretas. Assim, a minimização de dados não se impõe apenas como limitação técnica, mas como exigência ética essencial à salvaguarda da dignidade infantojuvenil frente às dinâmicas mercadológicas exploratórias.



Em última análise, a proteção de dados de crianças e adolescentes não pode ser compreendida apenas como resposta jurídica à evolução tecnológica, mas como expressão de compromisso civilizatório com o futuro. Garantir que esses sujeitos se desenvolvam em ambientes digitais seguros, livres de manipulação e orientados pela ética da contenção, é assegurar as condições materiais para que a infância não apenas exista, mas floresça sob o amparo da dignidade da pessoa humana.

Referências

- AMIN, Andréa Rodrigues et al. **Curso de direito da criança e do adolescente: aspectos teóricos e práticos**. Coordenação de Kátia Regina Ferreira Lobo Andrade Maciel. 12. ed. São Paulo: Saraiva Educação, 2019.
- ANGELINI, Kelli; et al. Privacidade e proteção aos dados pessoais de crianças e adolescentes na Internet: marco legal e ações estratégicas para prover direitos na era digital. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio. **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2021, p. 15-28.
- ALANA; SÃO PAULO. Ministério Público. **Comentário Geral N° 25 sobre os direitos das crianças em relação ao ambiente digital**: Versão Comentada. Autores: João Francisco de Aguiar Coelho et al. São Paulo: Instituto Alana, 2022. 152 p. Disponível em: <https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf>. Acesso em: 6 jul. 2025.
- BASAN, Arthur Pinheiro. **Publicidade digital e proteção de dados pessoais: o direito ao sossego**. 1. ed. Indaiatuba: Foco, 2021.
- BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. 1. ed. Rio de Janeiro: Zahar, 16 jan. 2014.
- BESSA, Leonardo Roscoe. A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa. **Consultor Jurídico**, 26 out. 2020. Disponível em: <https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa/>. Acesso em: 7 jul. 2025.
- BIONI, Bruno Ricardo (Org.). **Proteção de dados: contexto, narrativas e elementos fundantes**. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.
- BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados Pessoais. **Argumenta Journal Law**, Jacarezinho, n. 32, p. 191-207, jan./jun. 2020. DOI: 10.35356/argumenta.v0i32.1840. Disponível em: <https://periodicos.uenp.edu.br/index.php/argumenta/article/view/312>. Acesso em: 7 jul. 2025.
- BRASIL. Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD). Enunciado CD/ANPD nº 1, de 22 de maio de 2023. Dispõe acerca do tratamento de dados pessoais de crianças e adolescentes. **Diário Oficial da União**, Brasília, DF, ed. 98, seção 1, p. 129, 24 maio 2023. Disponível em: <https://www.in.gov.br/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934>. Acesso em: 7 jul. 2025.



BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **ANPD abre processo sancionador e emite determinações ao TikTok**, 2024b. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-processo-sancionador-e-emite-determinacoes-ao-tiktok>. Acesso em: 26 jun. 2025.

BRASIL. Resolução nº 245, de 5 de abril de 2024. Dispõe sobre os direitos das crianças e adolescentes em ambiente digital. **Diário Oficial da União**, Brasília, DF, ed. 68, seção 1, p. 42, 9 abr. 2024a. Disponível em: <https://in.gov.br/en/web/dou/-/resolucao-n-245-de-5-de-abril-de-2024-552695799>. Acesso em: 26 jun. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 jun. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **ANPD determina adoção de medidas preventivas à X. Corp**. Brasília, DF: ANPD, 2024c. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-adoacao-de-medidas-preventivas-a-x-corp>. Acesso em: 26 jun. 2025.

BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Institui a política de governança no compartilhamento de dados da administração pública federal. **Diário Oficial da União**: seção 1, Brasília, DF, 10 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 26 jun. 2025.

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**: seção 1, Brasília, DF, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 26 jun. 2025.

BRASIL. Decreto nº 99.710, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. **Diário Oficial da União**, Brasília, DF, 22 nov. 1990. Seção 1, p. 22255. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm. Acesso em: 05 jul. 2025.

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 (Lei Geral de Proteção de Dados Pessoais – LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 26 jun. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente – ECA. **Diário Oficial da União**: seção 1, Brasília, DF, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 26 jun. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4474, de 2024**. Altera as Leis nº 8.069/1990, nº 12.965/2014 e nº 13.709/2018 para instituir medidas de proteção a crianças e adolescentes na internet. Autoria: Antonio Carlos Rodrigues. Apresentação: 21 nov. 2024d. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2470873>. Acesso em: 26 jun. 2025.



bdtd.uerj.br:8443/bitstream/1/21519/2/Disserta%C3%A7%C3%A3o%20-%20Felipe%20Magno%20Silva%20Fonseca%20-%202023%20-%20Completa.pdf. Acesso em: 6 jun. 2025.

FRAZÃO, Ana. Proteção de dados, inteligência artificial e crianças. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio. **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2021, p. 84-106.

INSTITUTO ALANA; INTERNETLAB. **O direito das crianças à privacidade**: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020.

LEAL, Livia Teixeira. Internet of toys: os brinquedos conectados à internet e o direito da criança e do adolescente. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 12, p. 175–187, abr./jun. 2017. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/38/32>. Acesso em: 26 jun. 2025.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**. 32. ed., revista e atualizada até a Emenda Constitucional n. 84, de 2 dez. 2014. São Paulo: Malheiros, 2015.

OLIVEIRA, Deborah Siqueira de. Capítulo 23. Desdobramentos Práticos da Minimização de Dados. In: PALHARES, Felipe. **Estudos Sobre Privacidade e Proteção de Dados**. 1. ed. São Paulo: Editora Revista dos Tribunais, 2021. Disponível em: <https://www.jusbrasil.com.br/doutrina/estudos-sobre-privacidade-e-protecao-de-dados/1353726854>. Acesso em: 7 jul. 2025.

ÖZKUL, Didem; VOSLOO, Steven; BAGHDASARYAN, Bella. **Best interests of the child in relation to the digital environment**. Florença: UNICEF Innocenti, fev. 2025. Disponível em: <https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf>. Acesso em: 26 jun. 2025.

PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins (Org.). **Estudos sobre LGPD – Lei Geral de Proteção de Dados – Lei nº 13.709/2018**: doutrina e aplicabilidade no âmbito laboral. Porto Alegre: Escola Judicial do TRT4, 2022. Disponível em: <https://www.trt4.jus.br/portais/media/1063693/E-book-EstudosLGPD-Edjud4.pdf>. Acesso em: 7 jul. 2025.

TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. O princípio do melhor interesse no ambiente digital. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio. **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2021, p. 255-286.

TIC KIDS ONLINE BRASIL. **Pesquisa Sobre O Uso Da Internet Por Crianças E Adolescentes No Brasil**. Livro Eletrônico, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Acesso em: 7 jul. 2025.



UNICEF. **Children and digital marketing**: industry toolkit. [S.l.]: UNICEF, 2022. Disponível em: https://www.unicef.dk/wp-content/uploads/2022/09/industry-toolkit-children-digital-marketing_07.pdf. Acesso em: 26 jun. 2025.

WRIGHT, Verrion. Conformidade com a COPPA: Lei de Proteção à Privacidade Online de Crianças. **BigID**, [s. d.]. Disponível em: <https://bigid.com/pt/blog/coppa-compliance/>. Acesso em: 7 jul. 2025.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. In: BRUNO, Fernanda et al. (Orgs.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018.