CONTRIBUIÇÕES DA DATA PRIVACY BRASIL PARA A TOMADA DE SUBSÍDIOS SOBRE O GUIA ORIENTATIVO “FORNECEDORES DE PRODUTOS OU SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO, NO ÂMBITO DO ECA DIGITAL”

2026

DataPrivacyBR

DataPrivacyBR Research

Sobre a Data

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo. Fundada em 2018, a Data Privacy Brasil Ensino surgiu como um espaço para difundir e inovar no conhecimento sobre privacidade e proteção de dados no país. Com conteúdo adaptado para uma linguagem mais prática, com exercícios e estudos de caso, trata-se de uma escola para todos aqueles que se interessam e querem se aprofundar na temática da privacidade, proteção de dados e novas tecnologias.

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos e suprapartidária, que promove a proteção de dados pessoais e outros direitos fundamentais a partir de uma perspectiva de justiça social e das assimetrias de poder.

A partir de 2023, as duas instituições se uniram para formar uma única organização, man tendo os mesmos princípios e atividades. Com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para a promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, buscamos uma sociedade democrática em que as tecnologias estejam a serviço da autonomia e dignidade das pessoas.

Ficha técnica

A Data Privacy Brasil é uma organização de ensino, pesquisa e incidência que produz conhecimento e forma pessoas para um ecossistema informacional justo. Por meio da educação, construção de saberes e mobilização da sociedade, buscamos uma sociedade democrática na qual as tecnologias estejam a serviço da autonomia, dignidade das pessoas e redução de assimetrias de poder.

Direção

Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe

Ana Luiza Serafini, Bárbara Yamasaki, Bianca Marques, Eduardo Mendonça, Gabriela Vergili, Gabriel Franco, Giovanna Amaral, Giovana Andrade, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luize Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Paula Uematsu, Pedro Henrique Santos, Rafael Guimarães, Rodolfo Rodrigues e Vanessa Nobre.

Imprensa

Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacy.br.org

Como citar esse documento

NÓVOA, Natasha; Mendonça, Eduardo; RODRIGUES, Carla; ZANATTA, Rafael. **Contribuições da Data Privacy Brasil para a Tomada de Subsídios sobre o Guia Orientativo "Fornecedores de Produtos ou Serviços de Tecnologia da Informação, no âmbito do ECA Digital.** São Paulo: Data Privacy Brasil, 2026.

INTRODUÇÃO

A Data Privacy Brasil apresenta suas contribuições à Tomada de Subsídios sobre o Guia Orientativo "Fornecedores de Produtos ou Serviços de Tecnologia da Informação", no âmbito do ECA Digital, aberta pela Autoridade Nacional de Proteção de Dados. A Tomada de Subsídios constitui etapa relevante de participação social para o aperfeiçoamento do documento que busca delimitar conceitos essenciais da Lei nº 15.211/2025, especialmente no que diz respeito ao seu escopo de aplicação e ao significado dos deveres de prevenção, proteção, informação e segurança. Em nossa visão, a regulamentação do ECA Digital deve ser construída de forma transparente, tecnicamente consistente e orientada pela proteção integral de crianças e adolescentes, sem perder de vista a necessidade de segurança jurídica, previsibilidade regulatória e responsabilização efetiva dos fornecedores.

A contribuição parte da compreensão de que o ECA Digital inaugura um marco relevante para a proteção de crianças e adolescentes em ambientes digitais. A lei desloca o debate de uma lógica centrada apenas em conteúdo, consentimento ou direcionamento declarado para uma abordagem mais ampla, voltada ao desenho dos serviços, às suas funcionalidades, aos modelos de negócio, às práticas de tratamento de dados, às arquiteturas de recomendação e às condições concretas de uso por crianças e adolescentes. Por essa razão, entendemos que o Guia deve evitar interpretações excessivamente abertas que permitam aos próprios fornecedores definir, por autodeclaração, se estão ou não sujeitos à incidência da lei.

Este documento se concentra especialmente na categoria de acesso provável por crianças e adolescentes, prevista no art. 1º, parágrafo único, da Lei nº 15.211/2025. Trata-se de conceito central para a efetividade do ECA Digital, pois impede que serviços digitais generalistas, amplamente utilizados por crianças e adolescentes, escapem dos deveres legais apenas porque não se apresentam como produtos voltados a esse público. Em nossa visão, a noção de acesso provável deve ser compreendida como critério material, preventivo e *ex ante*, capaz de considerar a realidade concreta de uso, a atratividade, a facilidade de acesso e a existência de riscos presumidos em determinadas arquiteturas digitais.

A análise aqui apresentada dialoga com pesquisas, documentos de posição e acúmulos institucionais da Data Privacy Brasil sobre proteção de dados, direitos de crianças e adolescentes, governança de plataformas, design de serviços digitais, riscos algorítmicos e modelos de negócio baseados em dados. A partir desse percurso, reiteramos que a proteção de crianças e adolescentes não pode depender exclusivamente de mecanismos formais, como termos de uso, avisos genéricos, autodeclarações etárias ou classificações internas de público-alvo. O desafio regulatório está em construir parâmetros capazes de avaliar como os serviços digitais funcionam, como atraem e retêm usuários em desenvolvimento, quais fricções efetivas impõem e quais riscos decorrem de suas escolhas de design, arquitetura e monetização.

Também entendemos que a interpretação do Guia deve preservar o equilíbrio entre proteção e participação. O objetivo do ECA Digital não é excluir crianças e adolescentes da vida digital, mas assegurar que sua presença previsível em ambientes digitais seja acompanhada de deveres proporcionais de prevenção, segurança, transparência, proteção por padrão e governança documentada. Assim, a contribuição busca fortalecer uma leitura do acesso provável que não transforme a proteção em bloqueio generalizado, vigilância excessiva ou coleta adicional de dados, mas que imponha aos fornecedores o dever de construir ambientes digitais compatíveis com a condição peculiar de desenvolvimento de crianças e adolescentes.

Contribuições da Data Privacy Brasil na Tomada de Subsídios

O texto abaixo corresponde à versão extensa da contribuição apresentada pela Data Privacy Brasil à Tomada de Subsídios sobre o Guia Orientativo "Fornecedores de Produtos ou Serviços de Tecnologia da Informação", no âmbito do ECA Digital. A submissão realizada na plataforma da Tomada de Subsídios precisou observar os limites formais do procedimento participativo. Por esse motivo, esta versão desenvolve, de forma mais detida, a fundamentação jurídica, regulatória, empírica e bibliográfica que orientou a contribuição institucional. O objetivo é registrar com maior precisão os pressupostos, argumentos e recomendações que sustentam a posição da Data Privacy Brasil.

A contribuição está organizada em três blocos analíticos sobre a categoria de acesso provável por crianças e adolescentes. O primeiro bloco trata da probabilidade de uso e da atratividade, com foco na realidade concreta de circulação de crianças e adolescentes em ambientes digitais e nos elementos de design, linguagem, sociabilidade, reputação, entretenimento e personalização que tornam determinados serviços previsivelmente utilizados por esse público. O segundo bloco aborda a facilidade de acesso e utilização, compreendida como critério material relacionado às condições de entrada, permanência, retorno, navegação, compartilhamento, controle, proteção e saída. O terceiro bloco examina o significativo grau de risco, defendendo que esse elemento não deve ser tratado como requisito autônomo e excludente da incidência do ECA Digital, mas como vetor de calibração das obrigações de cuidado, prevenção e governança.

Essa organização busca responder a um ponto central da minuta do Guia. Embora seja importante conferir previsibilidade à aplicação da Lei nº 15.211/2025, a interpretação do acesso provável não pode abrir espaço para que fornecedores disputem semanticamente os critérios de incidência da lei, minimizem sinais de presença infantojuvenil ou transfiram à ANPD, às famílias e aos próprios usuários em desenvolvimento o ônus de comprovar riscos que decorrem do modo ordinário de funcionamento de certos serviços digitais. Em nossa visão, o Guia deve afirmar com maior clareza que a análise do acesso provável depende de uma leitura objetiva do ecossistema sociotécnico, considerando design, funcionalidades, arquitetura da informação, modelo de negócio, práticas de tratamento de dados, recomendação, personalização, monetização e fricções efetivas de acesso.

a. Acesso Provável por crianças e adolescentes
ii. Probabilidade de uso e atratividade
iii. Facilidade de acesso e utilização
iv. Significativo grau de risco

De início, entendemos que o Guia deve densificar a interpretação do conceito de acesso provável previsto no art. 1º, parágrafo único, da Lei nº 15.211/2025 ("ECA Digital"), de modo a impedir que fornecedores controlem a incidência do ECA Digital por meio de declarações formais de público-alvo, termos de uso adultocêntricos, autodeclarações etárias ou classificações internas de mercado. Trata-se de um ponto sensível para a Data Privacy Brasil, pois a forma como o Guia delimita o acesso provável terá efeitos sobre a efetividade dos deveres de prevenção, proteção, informação e segurança previstos no ECA Digital. Em nossa visão, essa interpretação deve ser orientada pelo art. 227 da Constituição Federal, pelo art. 70 do Estatuto da Criança e do Adolescente, pelo art. 14 da Lei Geral de Proteção de Dados e pelo art. 8º do Código de Defesa do Consumidor. Lidos em conjunto, esses dispositivos exigem uma abordagem preventiva, material e orientada à proteção integral, e não uma análise limitada à intenção declarada do fornecedor ou à classificação formal que a própria empresa atribui ao seu produto ou serviço.

O ponto de partida deve ser a superação da oposição rígida entre serviços direcionados e serviços generalistas. Como afirmam Rodrigues, Mendonça e Zanatta (2026, p. 5), "a distinção entre serviços 'direcionados' e serviços efetivamente utilizados por crianças revela-se insuficiente para assegurar a proteção integral desse público". O acesso provável representa, ainda nas palavras dos autores, uma "inflexão deliberada em relação a abordagens restritivas", pois desloca o eixo da responsabilização da intenção declarada dos fornecedores para a "realidade concreta de uso, atratividade e facilidade de acesso dos serviços digitais por crianças e adolescentes"[1]. Essa formulação é essencial para evitar que a autoavaliação empresarial seja transformada em escudo contra deveres de proteção. Ao reconhecer o acesso provável como critério material de incidência, o ECA Digital impede que fornecedores se beneficiem de uma espécie de desconhecimento conveniente sobre a presença de crianças e adolescentes em seus ecossistemas digitais.

Nesse sentido, entendemos que a categoria de acesso provável deve ser compreendida como uma tecnologia regulatória de fechamento de lacunas. Rodrigues, Mendonça e Zanatta (2026, p. 9-10) afirmam que "o critério de incidência deixa de depender apenas da autodeclaração empresarial sobre o público-alvo e passa a considerar a realidade do uso social do serviço". Também observam que, quando a incidência depende de o serviço ser dirigido a crianças, "a proteção pode falhar justamente nos ambientes generalistas onde crianças e adolescentes circulam de fato"[2]. Essa é uma preocupação central para a implementação do ECA Digital. O Guia não deve reproduzir uma lógica em que serviços generalistas, amplamente utilizados por crianças e adolescentes, possam afastar deveres protetivos apenas porque se apresentam como voltados a adultos ou porque incluem uma idade mínima contratual em seus termos de uso. Por isso, recomenda-se que a ANPD evite formulações que permitam a fornecedores alegar público adulto, ausência de intenção de direcionamento ou simples desconhecimento da presença infantojuvenil para afastar a incidência da lei.

1 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

2 *Idem.*

A análise do acesso provável deve observar probabilidade de uso, atratividade, facilidade de acesso e risco significativo como dimensões integradas de um mesmo teste material. Rodrigues, Mendonça e Zanatta (2026, p. 14) afirmam que os incisos I e II operam como "gatilhos de realidade", voltados à observação concreta do funcionamento dos serviços digitais. Também sustentam que "a lei desloca o foco da intenção declarada do fornecedor para os efeitos reais do design, das funcionalidades, da linguagem visual e do apelo cultural do serviço". Assim, a pergunta não deve ser apenas se o serviço se declara voltado a crianças e adolescentes, mas se, por sua arquitetura, linguagem, estética, funcionalidades, circulação social, modelo de negócio e dinâmica de engajamento, tende a ser utilizado por esse público. Essa formulação é mais compatível com a função preventiva do ECA Digital, pois permite olhar para o modo como os serviços efetivamente operam, atraem, retêm, classificam, recomendam e monetizam a presença de crianças e adolescentes.

Quanto à probabilidade de uso e à atratividade, entendemos que o Guia deve partir da experiência concreta de crianças e adolescentes, e não apenas da intenção comercial declarada pelo fornecedor. A atratividade não se limita a cores, personagens, mascotes ou anúncios explicitamente infantis. Em crianças, pode aparecer em elementos lúdicos, sensoriais, narrativos e colecionáveis. Em adolescentes, pode aparecer em funcionalidades que mobilizam pertencimento, identidade, reputação, visibilidade, autoexpressão, competição e reconhecimento. Montgomery e Chester (2009, p. S18, tradução própria) registram que "mídias digitais ressoam particularmente bem com muitas das tarefas desenvolvimentais fundamentais da adolescência"[3]. boyd (2008, p. 119, tradução própria) afirma que "a participação em redes sociais tornou-se parte importante da vida social adolescente"[4], enquanto Livingstone (2008, p. 407, tradução própria) lembra que "os *selfs* são constituídos por meio da interação com outros"[5]. A atratividade pode ser relacional, social e arquitetural, e não apenas visual ou publicitária.

A atratividade, portanto, pode decorrer menos do conteúdo ostensivo e mais da forma como o serviço organiza presença social, perfis, comentários, métricas de reputação, comunidades, influenciadores, criação de conteúdo e fluxos personalizados. boyd (2008, p. 124, tradução própria) observa que "amigos são articulados publicamente, perfis são visualizados publicamente e comentários são visíveis publicamente" e que persistência, buscabilidade, replicabilidade e audiências invisíveis alteram dinâmicas sociais.[6] Risco e

3 MONTGOMERY, Kathryn C.; CHESTER, Jeff. **Interactive food and beverage marketing: targeting adolescents in the digital age.** Journal of Adolescent Health, [s. l.], v. 45, n. 3, supl., p. S18-S29, 2009. DOI: https://doi.org/10.1016/j.jadohealth.2009.04.006. Disponível em: https://doi.org/10.1016/j.jadohealth.2009.04.006. Acesso em: 9 jun. 2026.

4 BOYD, danah. **Why Youth Social Network Sites: The Role of Networked Publics in Teenage Social Life.** In: BUCKINGHAM, David (ed.). Youth, Identity, and Digital Media. Cambridge, MA: The MIT Press, 2008. p. 119-142. DOI: https://doi.org/10.1162/dmal.9780262524834.119. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1345415. Acesso em: 9 jun. 2026.

5 LIVINGSTONE, Sonia. **Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression.** New Media & Society, London, v. 10, n. 3, p. 393-411, 2008. DOI: https://doi.org/10.1177/1461444808089415. Disponível em: https://doi.org/10.1177/1461444808089415. Acesso em: 9 jun. 2026.

6 BOYD, danah. **Why Youth Social Network Sites: The Role of Networked Publics in Teenage Social Life.**

atratividade não nascem apenas de conteúdo infantilizado, mas de uma arquitetura que organiza identidade, reputação, exposição e pertencimento em públicos em rede. Em outras palavras, um serviço pode ser atrativo para crianças e adolescentes mesmo sem linguagem infantil explícita, caso ofereça mecanismos de reconhecimento, competição, visibilidade e interação social que dialoguem com suas práticas de sociabilidade e formação identitária.

No Brasil, a probabilidade de uso deve ser lida a partir de uma presença infantojuvenil já consolidada em plataformas de comunicação, sociabilidade e circulação de conteúdo. A TIC Kids Online Brasil 2024 registra que 83% dos usuários de Internet de 9 a 17 anos possuem perfil próprio em plataformas digitais, percentual que chega a 93% entre adolescentes de 13 a 14 anos e a 99% entre adolescentes de 15 a 17 anos. Entre crianças e adolescentes com perfil próprio e uso semanal, há presença expressiva em plataformas centrais de comunicação e sociabilidade.[7] Esses dados não tornam automática a incidência do ECA Digital sobre qualquer serviço, mas afastam a premissa de que a presença infantojuvenil em ambientes digitais seria marginal, eventual ou excepcional. Em nossa visão, eles reforçam que a análise do acesso provável deve partir de uma realidade social em que crianças e adolescentes já circulam ordinariamente por serviços digitais estruturados por interação, personalização, recomendação e engajamento.

Por isso, recomendamos que o Guia transforme a atratividade em critério operacional. Devem ser considerados, entre outros elementos, estética gamer ou lúdica, avatares, filtros, mascotes, símbolos reconhecíveis, colecionáveis, perfis, comentários, curtidas, lives, comunidades abertas, mundos virtuais, rankings, desafios, missões, streaks, pontuação, recompensas variáveis, recomendação algorítmica persistente, notificações, fluxos contínuos de conteúdo, influenciadores e recursos de IA generativa narrativa ou relacional. Esses elementos não devem ser avaliados isoladamente. A incidência do acesso provável deve observar sua confluência com design, funcionalidade, circulação social, facilidade de acesso e modelo de negócio. Como afirmam Rodrigues, Mendonça e Zanatta (2026, p. 18), o teste não depende da intenção declarada, mas da "leitura objetiva do ecossistema sociotécnico no qual ele opera".[8] É essa leitura impede que fornecedores fragmentem a análise em elementos isolados e sustentem que nenhum deles, sozinho, seria suficiente para caracterizar o acesso provável.

A facilidade de acesso e utilização também deve ser lida como critério material. O art. 1º, parágrafo único, II, da Lei nº 15.211/2025 não autoriza uma verificação meramente formal da existência de idade mínima contratual, aviso etário, botão genérico ou autode-

---

In: BUCKINGHAM, David (ed.). Youth, Identity, and Digital Media. Cambridge, MA: The MIT Press, 2008. p. 119-142. DOI: https://doi.org/10.1162/dmal.9780262524834.119. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1345415. Acesso em: 9 jun. 2026.

7 NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024 [tabelas]**. São Paulo: NIC.br, 2024. Disponível em: https://cetic.br/pt/tics/kidsonline/2024/criancas/C9/. Acesso em: 9 jun. 2026.

8 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

claração simples.[9] Facilidade não significa ausência absoluta de barreiras, mas redução concreta de obstáculos práticos de ingresso, navegação, permanência, retorno, compartilhamento, fornecimento de dados e exercício de direitos. Por isso, a pergunta não é se o fornecedor inseriu alguma barreira documental, mas se essa barreira funciona como fricção efetiva, proporcional e verificável diante da experiência concreta de crianças e adolescentes. A existência de um obstáculo formal não deve ser confundida com a existência de uma medida materialmente eficaz de proteção.

Rodrigues, Mendonça e Zanatta (2026, p. 11) advertem que "os elementos críticos do acesso provável não podem ser tratados como adendos" e que a probabilidade é construída por indicadores, métricas e inferências frequentemente controladas pelas próprias plataformas. Por essa razão, o acesso provável exige "critérios verificáveis e expectativas claras sobre quais evidências contam", sob pena de transformar "um teste material num formalismo administrável pela autorreferência empresarial".[10] Essa advertência é central para evitar que fornecedores selecionem métricas convenientes, minimizem sinais de presença infantil ou transfiram o ônus probatório para a ANPD, para famílias e para usuários em desenvolvimento. O Guia deve, portanto, explicitar que a autoavaliação do fornecedor não vincula a autoridade e que os dados usados para afastar o acesso provável devem ser auditáveis, consistentes e compatíveis com a realidade de uso do serviço.

A facilidade deve ser aferida a partir do funcionamento do produto ou serviço. O Guia deve considerar gratuidade ou modelo freemium, download simplificado, disponibilidade em lojas de aplicações de amplo acesso, funcionamento em celulares, tablets ou dispositivos compartilhados, login por contas de terceiros, navegação sem autenticação robusta, linguagem operacional simples, comandos gestuais intuitivos, redução de etapas de cadastro, comunidades abertas e compartilhamento rápido. A minuta do Guia registra que o celular é o principal dispositivo de acesso à Internet entre crianças e adolescentes, com 96% dos usuários de 9 a 17 anos conectados pelo aparelho em 2025 e uso diário pelo celular de 90%, chegando a 98% entre adolescentes de 15 a 17 anos. Nesse cenário, compatibilidade móvel e baixa complexidade operacional são indicadores materiais de facilidade, pois aproximam o serviço do cotidiano efetivo de crianças e adolescentes.

A facilidade também abrange a continuidade de uso. Em ambientes digitais, ela não se limita ao ingresso inicial. Ela se manifesta quando a arquitetura reduz fricções para permanecer, retornar, publicar, reagir, consumir conteúdo, compartilhar informações ou realizar pagamentos. Quando fluxos de retorno, notificações, recomendações, recompensas e atalhos de interação reduzem o esforço necessário para continuar usando o serviço, a facilidade pode operar como mecanismo de captura de atenção. Segundo a TIC Kids Online Brasil 2024, entre usuários de 11 a 17 anos, 24% tentaram passar menos tempo na

9 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: seção 1, edição extra A, Brasília, DF, p. 1, 17 set. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 11 jun. 2026.

10 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

Internet e não conseguiram, 22% passaram menos tempo do que deveriam com família, amigos ou tarefas escolares e 15% deixaram de comer ou dormir por causa da Internet.[11] Esse dado reforça que a facilidade não deve ser examinada apenas no momento da entrada, mas também nas condições de permanência, retorno, pausa, limite e saída.

Essa leitura permite diferenciar barreiras formais de fricções. Barreiras formais deslocam responsabilidade para o usuário, como termos extensos, avisos genéricos, caixas de confirmação e autodeclarações de idade sem capacidade real de impedir ou modular o uso por crianças e adolescentes. Fricções efetivas reduzem materialmente o acesso indevido, configuram o serviço de forma protetiva por padrão e tornam compreensíveis os caminhos de controle, pausa, limitação, denúncia, bloqueio e saída. Rodrigues, Mendonça e Zanatta (2026, p. 6) defendem que cabe às empresas demonstrar "fricções suficientes para tornar o acesso difícil para crianças e adolescentes".[12] O Guia deve evitar que obstáculos simbólicos sejam apresentados como prova de ausência de facilidade. Em nossa visão, a questão central é a demonstração de que a barreira produz efeito protetivo real sem recorrer a vigilância excessiva, coleta desnecessária de dados ou exclusão generalizada.

Ainda, não basta observar se é fácil entrar, navegar, compartilhar ou fornecer dados. É necessário verificar se é igualmente fácil compreender configurações, restringir perfilamento, limitar recomendações, alterar privacidade, retirar consentimento, excluir conta, apagar dados, bloquear interações indesejadas, denunciar abusos e reduzir exposição. A jurisprudência europeia sobre cookies ajuda a tornar esse ponto operacional. No caso Planet49, o Tribunal de Justiça da União Europeia afirmou que caixas pré-selecionadas não constituem consentimento válido para armazenamento de cookies.[13] O art. 7º, item 3, do Regulamento Geral de Proteção de Dados da União Europeia reforça a mesma lógica ao exigir que a retirada do consentimento seja tão fácil quanto sua concessão.[14] Embora se trate de norma estrangeira e voltada especificamente ao consentimento, o critério é útil como parâmetro de desenho regulatório, pois evidencia que a interface não deve ser eficiente apenas para adesão, engajamento e extração de dados, mas também para controle, proteção e saída.

Essa simetria também aparece em decisões e sanções recentes sobre desenho de

11 NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024 [tabelas].** São Paulo: NIC.br, 2024. Disponível em: https://cetic.br/pt/tics/kidsonline/2024/criancas/C9/. Acesso em: 9 jun. 2026.

12 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

13 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **Acórdão do Tribunal de Justiça, Grande Secção, de 1º de outubro de 2019.** Processo C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV contra Planet49 GmbH. ECLI:EU:C:2019:801. Luxemburgo: Tribunal de Justiça da União Europeia, 2019. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=218467&doclang=PT. Acesso em: 11 jun. 2026.

14 UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. **Regulamento (UE) 2016/679, de 27 de abril de 2016.** Jornal Oficial da União Europeia, Luxemburgo, L 119, p. 1-88, 4 maio 2016, art. 7º, item 3. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/por. Acesso em: 11 jun. 2026.

fluxos. O caso Amazon Prime, conduzido pela Federal Trade Commission, evidenciou a relevância jurídica de interfaces que facilitam assinatura e dificultam o cancelamento.[15] As sanções da autoridade francesa contra Google e Shein por problemas relacionados a cookies e consentimento indicam que facilidade de aceitar, seguir navegando ou permanecer logado não pode ser confundida com escolha informada.[16] A atuação do Information Commissioner's Office contra o Reddit[17] e do Ofcom em relação à Fenix International[18], responsável pelo OnlyFans, reforça que mecanismos de idade não podem ser apenas declarados, pois precisam ser proporcionais, documentados, verificáveis e capazes de reduzir acesso indevido sem produzir vigilância excessiva. Esses exemplos demonstram que a arquitetura dos fluxos importa para fins regulatórios e que a facilidade deve ser analisada ao longo de toda a jornada de uso.

Quanto ao significativo grau de risco, entendemos que a principal contribuição deve ser impedir que o inciso III seja interpretado como requisito autônomo e excludente da incidência do ECA Digital. A minuta do Guia reconhece presunções legais de acesso provável para algumas categorias de fornecedores e serviços, mas, ao afirmar a necessidade de presença concomitante dos três requisitos, pode abrir espaço para que fornecedores aleguem ausência de risco comprovado mesmo diante de serviços prováveis, atrativos e facilmente acessíveis por crianças e adolescentes. Rodrigues, Mendonça e Zanatta (2026, p. 5) afirmam que o "significativo grau de risco" não se apresenta como requisito autônomo ou excludente, mas como "consequência presumida do próprio acesso provável em contextos marcados por assimetrias estruturais e práticas intensivas de tratamento de dados"[19]. Essa formulação deve orientar a revisão do Guia, para que o risco não se converta em barreira probatória adicional imposta à autoridade ou aos titulares em desenvolvimento.

Essa leitura precisa ser ajustada para não deslocar o ônus regulatório para a ANPD, para as famílias ou para usuários em desenvolvimento. O ECA Digital não foi estruturado como regime repressivo, dependente da demonstração posterior de dano consumado. Como afirmam Rodrigues, Mendonça e Zanatta (2026, p. 6), "exigir uma prova empírica de dano, como se fosse equivalente de 'grau significativo de risco', esvaziaria a função pre-

15 UNITED STATES OF AMERICA. **Federal Trade Commission. Amazon.com, Inc. (ROSCA), FTC v. Case No. 2:23-cv-0932-JHC. Washington, DC: Federal Trade Commission, 2023-2025.** Disponível em: https://www.ftc.gov/legal-library/browse/cases-proceedings/2123050-amazoncom-inc-rosca-ftc-v. Acesso em: 11 jun. 2026.

16 FRANCE. **Commission Nationale de l'Informatique et des Libertés. Cookie regulation: the CNIL is continuing the action plan initiated in 2019 and has imposed two fines on SHEIN and GOOGLE.** Paris: CNIL, 3 Sept. 2025. Disponível em: https://www.cnil.fr/en/cookie-regulation-cnil-continuing -action-plan-initiated-2019-and-has-imposed-two-fines-shein-and. Acesso em: 11 jun. 2026.

17 UNITED KINGDOM. **Information Commissioner's Office. Reddit, Inc.** Wilmslow: ICO, 23 Feb. 2026. Disponível em: https://ico.org.uk/action-weve-taken/enforcement/2026/02/reddit-inc/. Acesso em: 11 jun. 2026.

18 UNITED KINGDOM. Office of Communications. **Final Decision CW.01283.04.24: Fenix International Limited.** London: Ofcom, 26 Mar. 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/enforcement/final-decision-cw.01283.04.24-fenix-international-limited.pdf. Acesso em: 11 jun. 2026.

19 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

ventiva da norma jurídica, violando o princípio da proteção integral". O risco deve funcionar como vetor de calibração regulatória.[20] Probabilidade de uso, atratividade e facilidade de acesso operam como gatilhos materiais de incidência. O risco significativo orienta o nível de rigor das salvaguardas, dos relatórios de impacto, das configurações protetivas por padrão, das auditorias, da mitigação de práticas manipulativas, da transparência, da prestação de contas e do monitoramento contínuo. Essa distinção entre aplicabilidade e modulação é essencial para preservar a função preventiva do ECA Digital.

Rodrigues, Mendonça e Zanatta (2026, p. 20) advertem que o inciso III pode ser mobilizado como cláusula de escape interpretativa por empresas que, mesmo diante de probabilidade de acesso, atratividade e facilidade, sustentem ausência de risco significativo para se colocar fora do alcance da lei. Em resposta, os autores afirmam que o "significativo grau de risco" não pode ser compreendido como filtro excludente da incidência do ECA Digital, mas como "vetor de calibração regulatória que organiza a aplicação proporcional e responsiva da lei".[21] Em outras palavras, o risco não atua no plano da aplicabilidade da norma, mas no plano de sua concretização. Em nossa visão, o Guia deve afirmar expressamente essa distinção, sob pena de permitir que fornecedores disputem semanticamente o que seria risco significativo e, com isso, esvaziem o âmbito de incidência da lei.

Essa interpretação é coerente com a compreensão de que ambientes digitais podem produzir riscos pela própria arquitetura. Rodrigues, Mendonça e Zanatta (2026, p. 10-11) afirmam que o ECA Digital desloca o debate "do marketing para o desenho do serviço e para os riscos previsíveis que esse desenho produz". Também sustentam que "o eixo substantivo da inovação é a migração do debate de coleta de dados para arquiteturas de risco" e que o dano potencial passa a incluir "manipulação comportamental, engajamento compulsivo e desenho viciante". Assim, o risco não deve ser visto como evento excepcional externo ao serviço, mas como possibilidade produzida por padrões de interface, monetização, recomendação, perfilamento e incentivos de permanência. Dessa forma, o Guia deve tratar o design como categoria material de responsabilidade, e não apenas como detalhe instrumental da experiência do usuário.

A experiência regulatória comparada confirma que o risco significativo tem sido associado ao desenho dos sistemas, e não apenas a conteúdos específicos. O Regulamento Europeu de Inteligência Artificial proíbe práticas de IA que explorem vulnerabilidades associadas à idade, deficiência ou situação social e econômica quando capazes de distorcer substancialmente o comportamento e causar dano significativo.[22] Leis recentes sobre re-

20 *Idem.*

21 *Idem.*

22 UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).** Jornal Oficial da União Europeia, Luxemburgo, L, 2024/1689, 12 jul. 2024. Art. 5º. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=pt. Acesso em: 11 jun. 2026.

des sociais, como a SAFE for Kids Act de Nova York[23] e a Protecting Our Kids from Social Media Addiction Act da Califórnia[24], tratam feeds algorítmicos, notificações e configurações de conta como objetos regulatórios autônomos. Esses exemplos mostram que o risco de crianças e adolescentes em ambientes digitais pode decorrer de sistemas de entrega personalizada, retenção, notificação e arquitetura de escolha, e não apenas de conteúdos isolados. Eles também indicam que a regulação contemporânea tem deslocado sua atenção para mecanismos de recomendação, personalização, retenção e exploração de vulnerabilidades.

Casos recentes reforçam essa virada. O acordo da Federal Trade Commission e do Ministério Público de Los Angeles com a NGL Labs envolveu aplicativo de mensagens anônimas utilizado por adolescentes, alegações de marketing direcionado aos mais jovens, riscos de cyberbullying e práticas enganosas.[25] As decisões no caso K.G.M. contra Meta e Google e na ação do Estado de Massachusetts contra a Meta demonstram que alegações centradas em escolhas de design não se confundem com responsabilidade por conteúdo de terceiros.[26] O veredicto do Novo México contra a Meta, relacionado à segurança de crianças em plataformas, reforça que riscos de aliciamento, exploração, contato indesejado e comunicação predatória podem decorrer de escolhas sobre moderação, denúncia, recomendação, comunicação privada, configuração de contas e incentivos econômicos.[27] A relevância desses exemplos, para o Guia, está em mostrar que riscos à segurança, à privacidade e ao desenvolvimento podem decorrer do modo ordinário de organização do serviço.

O Guia também deve evitar reduzir o risco significativo à saúde mental em sentido estrito. O inciso III menciona privacidade, segurança e desenvolvimento biopsicossocial. Isso inclui exposição indevida de dados, perfilamento, inferência sensível, exploração comercial, contato indesejado, assédio, aliciamento, fraude, manipulação, compulsão de

23 NEW YORK. Senate. Senate Bill S7694A, 2023-2024 Legislative Session. **Stop Addictive Feeds Exploitation (SAFE) for Kids Act.** Albany: New York State Senate, 2024. Signed by Governor, Chap. 120, 20 June 2024. Disponível em: https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A. Acesso em: 11 jun. 2026.

24 CALIFORNIA. Legislature. Senate Bill No. 976, Chapter 321. **Protecting Our Kids from Social Media Addiction Act. Sacramento: California Legislative Information, 2024.** Approved by Governor and filed with Secretary of State, 20 Sept. 2024. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB976. Acesso em: 11 jun. 2026.

25 UNITED STATES OF AMERICA. Federal Trade Commission; THE PEOPLE OF THE STATE OF CALIFORNIA. **Federal Trade Commission and The People of the State of California v. NGL Labs, LLC; Raj Vir; Joao Figueiredo. Case No. 2:24-cv-05753-JLS-PVC. Stipulated Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief.** United States District Court, Central District of California, 14 July 2024. Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/DN008StipulatedOrderforPermanentInjunction.pdf. Acesso em: 11 jun. 2026.

26 UNITED STATES OF AMERICA. **Superior Court of California, County of Los Angeles. P.F., et al. (K.G.M.) v. Meta Platforms, Inc., et al. Case No. 23SMCV03371; Lead Case No. 22STCV21355. Verdict Form — Meta.** Los Angeles: Superior Court of California, County of Los Angeles, 25 Mar. 2026. Disponível em: https://www.crowell.com/a/web/b3HgCKaRwDn5JSu1FVt4Vg/verdict-form-meta.pdf. Acesso em: 11 jun. 2026.

27 NEW MEXICO. **First Judicial District Court, County of Santa Fe. State of New Mexico, ex rel. Raúl Torrez, Attorney General v. Meta Platforms, Inc.; Instagram, LLC; Meta Payments, Inc.; Meta Platforms Technologies, LLC; and Mark Zuckerberg. Case No. D-101-CV-2023-02838. Plaintiff's Complaint for Abatement and Civil Penalties and Demand for Jury Trial.** Santa Fe: First Judicial District Court, 5 Dec. 2023. Disponível em: https://nmag.gov/wp-content/uploads/2024/01/2023-12-05-NM-v.-Meta-et-al.-COMPLAINT-REDACTED.pdf. Acesso em: 11 jun. 2026.

uso, perda de autonomia e restrições ao exercício de direitos. O'Keeffe, Clarke-Pearson e o Council on Communications and Media (2011, p. 800, tradução própria) observam que "uma grande parte do desenvolvimento social e emocional desta geração está ocorrendo na Internet e em telefones celulares" e que, por sua "capacidade limitada de autorregulação e suscetibilidade à pressão dos pares", crianças e adolescentes estão sob risco ao experimentar mídias sociais.[28] Odgers e Jensen (2020) recomendam cautela contra pânicos morais e leituras lineares sobre tecnologia e saúde mental, mas essa cautela reforça a necessidade de uma abordagem estrutural sobre arquiteturas, incentivos e modelos de negócio.[29] O risco não deve ser tratado como causalidade simples e individual, mas como fenômeno situado em ecossistemas sociotécnicos opacos e assimétricos.

Dados nacionais reforçam essa leitura sem tratar crianças e adolescentes como grupo homogêneo. A TIC Kids Online Brasil 2024 registra situações relacionadas à privacidade, segurança e autonomia informacional, como publicação seguida de arrependimento e apagamento, tentativa de terceiros se passarem pelo usuário, uso indesejado de informações e perda de dinheiro por engano. Também registra situações ofensivas ou desagradáveis e compras em jogos online.[30] Rodrigues, Mendonça e Zanatta (2026, p. 12) lembram que "crianças e adolescentes não formam um grupo homogêneo" e que raça, gênero, classe e território modulam exposição a assédio, exploração, perfis indevidos e dinâmicas de dependência.[31] Frota (2007) também reforça que infância e adolescência são categorias históricas, sociais e jurídicas.[32] Assim, o risco deve considerar condições concretas de conectividade, dispositivo compartilhado, literacia digital, mediação familiar, território, raça, gênero, deficiência e vulnerabilidades acumuladas.

A interpretação proposta preserva o equilíbrio entre proteção e participação. O art. 7º do Marco Civil da Internet reconhece o acesso à Internet como essencial ao exercício da cidadania. Livingstone e Third (2017, p. 662, tradução própria) afirmam que "a proteção tende a prevalecer sobre a participação" e perguntam como promover a proteção contra danos online e, simultaneamente, capacitar crianças a maximizar oportunidades da era

28 O'KEEFFE, Gwenn Schurgin; CLARKE-PEARSON, Kathleen; COUNCIL ON COMMUNICATIONS AND MEDIA. **The impact of social media on children, adolescents, and families.** Pediatrics, [s. l.], v. 127, n. 4, p. 800-804, abr. 2011. DOI: https://doi.org/10.1542/peds.2011-0054. Disponível em: https://pediatrics.aappublications.org/content/127/4/800. Acesso em: 9 jun. 2026.

29 ODGERS, Candice L.; JENSEN, Michaeline R. **Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions.** Journal of Child Psychology and Psychiatry, [s. l.], v. 61, n. 3, p. 336-348, 2020. DOI: https://doi.org/10.1111/jcpp.13190. Disponível em: https://doi.org/10.1111/jcpp.13190. Acesso em: 9 jun. 2026.

30 NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024 [tabelas].** São Paulo: NIC.br, 2024. Disponível em: https://cetic.br/pt/tics/kidsonline/2024/criancas/C9/. Acesso em: 9 jun. 2026.

31 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

32 FROTA, Ana Maria Monte Coelho. **Diferentes concepções da infância e adolescência: a importância da historicidade para sua construção.** Estudos e Pesquisas em Psicologia, Rio de Janeiro, v. 7, n. 1, p. 147-160, abr. 2007. Disponível em: http://www.redalyc.org/articulo.oa?id=451844613015. Acesso em: 9 jun. 2026.

digital.[33] Essa tensão deve orientar o Guia. O reconhecimento do acesso provável não deve conduzir a bloqueios generalizados, exclusão de crianças e adolescentes ou ampliação indiscriminada de verificação etária. A resposta adequada é design seguro, proteção por padrão, minimização de dados, limitação de perfilamento, avaliação de impactos, governança documentada e mecanismos de controle adequados à idade. Em outras palavras, o objetivo não é retirar crianças e adolescentes dos ambientes digitais, mas exigir que tais ambientes sejam construídos de forma compatível com sua condição peculiar de desenvolvimento.

Essa preocupação é ainda mais relevante porque a Internet foi, como afirmam Livingstone e Third (2017, p. 663-658, tradução própria), "amplamente concebida, implícita ou explicitamente, como um recurso adulto em termos de provisão, regulação e ideologia". As autoras também afirmam que a Internet é "um espaço amplamente cego à idade ou implicitamente adulto".[34] Por isso, a regulação não deve aceitar que fornecedores desenhem serviços para um usuário abstrato adulto e depois tratem crianças e adolescentes como exceção indesejada. O acesso provável exige inverter essa lógica, incorporando a presença infantojuvenil previsível desde o desenho, a governança e a avaliação de riscos. Essa é a forma mais adequada de responder à assimetria estrutural entre fornecedores e usuários em desenvolvimento.

O Guia deve reconhecer, ainda, que plataformas digitais não apenas hospedam interações, mas organizam possibilidades de identidade, privacidade, sociabilidade e exposição. Livingstone e Third (2017, p. 664, tradução própria) afirmam que "plataformas digitais redefinem identidade, privacidade, sociabilidade e necessidade segundo os interesses de seus proprietários" e que crianças são configuradas como "assemblages algorítmicos".[35] Essa formulação é especialmente importante para sistemas de recomendação, IA generativa, perfilamento e publicidade comportamental. Ela demonstra que crianças e adolescentes não são apenas usuários finais de uma interface, mas também objetos de cálculo, inferência, ranqueamento, segmentação e monetização. Em nossa visão, esse é um dos motivos pelos quais o Guia deve tratar modelos de negócio, design, recomendação e governança de dados como dimensões centrais do acesso provável.

Recomendamos, portanto, que a ANPD substitua uma leitura centrada na intenção declarada dos mercados por uma leitura centrada no ecossistema sociotécnico. O acesso provável deve ser aferido a partir da confluência entre uso efetivo ou previsível, atratividade, facilidade de acesso e risco presumido em arquiteturas de dados, interação, recomendação, personalização, monetização, IA generativa e circulação em larga escala. Como afirmam Rodrigues, Mendonça e Zanatta (2026, p. 10), uma vez identificada a presença previsível de crianças e adolescentes no ecossistema, "a organização deve justificar escolhas de design, configurar proteções por padrão e governar riscos de forma *ex an-*

33 LIVINGSTONE, Sonia; THIRD, Amanda. **Children and young people's rights in the digital age: an emerging agenda.** New Media & Society, [s. l.], v. 19, n. 5, p. 657-670, 2017. DOI: https://doi.org/10.1177/1461444816686318. Disponível em: https://doi.org/10.1177/1461444816686318. Acesso em: 9 jun. 2026.

34 *Idem.*

35 *Idem.*

te".[36] Essa orientação deve ser incorporada ao Guia de modo expresso, para que o acesso provável não se torne uma categoria aberta à disputa semântica dos fornecedores, mas um critério operacional de responsabilização, prevenção e governança.

Em síntese, o acesso provável deve ser compreendido como tecnologia regulatória de fechamento de lacunas. Ele impede que serviços generalistas amplamente utilizados por crianças e adolescentes escapem de deveres de proteção por meio de autodeclarações de público adulto, barreiras formais ou disputa semântica sobre risco significativo. Probabilidade, atratividade e facilidade são critérios materiais de realidade. O risco significativo não é cláusula de escape, mas vetor de calibração das obrigações. Quanto maior a intensidade da coleta de dados, da personalização, do perfilamento, da recomendação, da interação social, da monetização, da exposição e da exploração de vulnerabilidades, maior deve ser o rigor das salvaguardas exigidas. Essa interpretação preserva a função preventiva do ECA Digital e aproxima o Guia de uma governança de riscos orientada à proteção integral, à justiça de dados e ao desenvolvimento seguro de crianças e adolescentes em ambientes digitais.

b. Dever de prevenção
i. Dever de prevenção em sentido estrito
ii. Dever de proteção
iii. Dever de informação
iv. Dever de segurança

De início, entendemos que o Guia estrutura o dever de prevenção em quatro dimensões: prevenção em sentido estrito, proteção, informação e segurança. Todas essas dimensões estão ancoradas, direta ou indiretamente, no princípio do melhor interesse da criança e do adolescente. Esse princípio opera como critério material para orientar a interpretação e a aplicação de cada dever, exigindo que fornecedores demonstrem, concretamente, que suas escolhas são compatíveis com a proteção integral desse público. As contribuições abaixo se organizam em torno dessas quatro dimensões e apontam caminhos para torná-las mais robustas. Há, porém, uma ausência que merece atenção: o design como dimensão autônoma do dever de prevenção. Como observa Monteiro (2026), as escolhas de interface e arquitetura de um serviço não são detalhes técnicos, na medida em que criam obrigações jurídicas, moldam comportamentos e definem, na prática, o nível de proteção que crianças e adolescentes efetivamente recebem.

Quanto ao dever de prevenção em sentido estrito, o Guia o descreve como obrigação proativa e transversal, exigível desde a concepção do produto ou serviço até sua operação contínua. Essa caracterização está alinhada com os arts. 7º e 8º do ECA Digital e

36 RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

representa avanço interpretativo relevante, pois deixa claro que o cumprimento do dever não se esgota em respostas pontuais a danos já ocorridos. Contudo, o Guia não enfrenta uma questão que decorre diretamente desse modelo: a quem incumbe demonstrar que as medidas adotadas são adequadas e suficientes.

O texto descreve o conteúdo do dever, mas silencia sobre o ônus probatório. Como argumentam Rodrigues, Mendonça e Zanatta (2026)[37], o ECA Digital deliberadamente escolheu um padrão regulatório ex ante, no qual o ônus argumentativo de não incidência recai sobre os fornecedores, e não sobre o regulador ou sobre as próprias crianças e adolescentes afetados. Essa lógica deve ser transposta para o dever de prevenção. Não basta ao fornecedor listar medidas adotadas; cabe a ele demonstrar ativamente que essas medidas são proporcionais aos riscos concretos do seu serviço.

Nesse sentido, sugerimos que o Guia explicite essa inversão do ônus e oriente como os fornecedores devem documentar e evidenciar a adequação das medidas preventivas, inclusive por meio de avaliações de impacto periódicas, tal como já previsto no art. 47 do Decreto nº 12.880/2026.

Quanto ao dever de proteção, o Guia o enquadra sobretudo como obrigação de resposta a conteúdos danosos produzidos por terceiros e a condutas abusivas de outros usuários, como moderação ativa, remoção de conteúdo e comunicação a autoridades. Esse enquadramento é fundamental, mas poderia ressaltar a dimensão estrutural da responsabilidade do fornecedor por escolhas arquitetônicas do seu serviço como vetor autônomo de dano a crianças e adolescentes.

O art. 22 do ECA Digital veda o perfilamento para fins de publicidade comercial direcionada a crianças e adolescentes. O art. 8º, IV, exige que configurações que evitem o uso compulsivo sejam adotadas por padrão desde a concepção. Esses dispositivos revelam que o legislador reconhece o design do serviço como fonte de risco independente de qualquer conduta de terceiro. Como destacaram Zanatta, Valente e Mendonça (2021) [38]no âmbito da LGPD, o tratamento de dados de crianças e adolescentes exige avaliação do que é "abusivo" e "excessivo" a partir do melhor interesse, critério que vai além do consentimento formal e alcança a arquitetura do serviço. Nesse sentido, o Guia poderia esclarecer de forma mais clara que o dever de proteção também abrange as escolhas de design do fornecedor, incluindo mecanismos de recomendação algorítmica, funcionalidades de engajamento e modelos de monetização que possam prejudicar o desenvolvimento biopsicossocial de crianças e adolescentes. Funcionalidades de risco devem ser desabilitadas por padrão como condição de cumprimento desse dever, e não disponibilizadas como opção *opt-in*.

Quanto ao dever de informação, o Guia acerta ao caracterizá-lo como obrigação subs-

37 RODRIGUES, Carla; MENDONÇA, Eduardo; ZANATTA, Rafael. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. P. 6.

38 ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Júlia. **Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD.** In: COSTA, Ana Cláudia et al. (org.). LGPD e Crianças e Adolescentes. São Paulo: Thomson Reuters Revista dos Tribunais, 2021. P.14.

tantiva, que não se satisfaz com a mera disponibilização de textos extensos ou tecnicamente opacos. Também acerta ao destacar que informar significa empregar esforços efetivos de comunicação voltados à compreensão real pelo público destinatário. Essa orientação é correta e merece ser preservada na versão definitiva. Contudo, o Guia não diferencia as exigências informacionais conforme o destinatário. Crianças, adolescentes e responsáveis legais têm posições jurídicas e capacidades de compreensão distintas. O texto também não aborda a transparência sobre sistemas automatizados de recomendação e engajamento, justamente onde a assimetria entre fornecedores e usuários se torna mais aguda.

O art. 7º, § 1º, do ECA Digital já exige que informações sobre configurações menos protetivas sejam fornecidas de forma "clara, acessível e adequada" para que crianças, adolescentes e seus responsáveis possam exercer escolhas informadas. Essa exigência pressupõe calibração por público. O que é adequado para um responsável legal não é necessariamente adequado para uma criança de oito anos ou para um adolescente de quinze. O Guia poderia densificar esse ponto à luz do art. 4º, V, do ECA Digital, que consagra o respeito à autonomia progressiva como fundamento do regime protetivo.

Essa preocupação se torna ainda mais urgente em plataformas voltadas ao público infantojuvenil. Como apontam Rodrigues, Mendonça e Nóvoa (2026)[39], sistemas que produzem enunciados plausíveis a partir de padrões probabilísticos, e não de uma compreensão situada do desenvolvimento da criança, podem induzir à aceitação acrítica de conteúdos e reduzir capacidades fundamentais como atenção sustentada, elaboração narrativa e julgamento reflexivo. Esse risco está diretamente relacionado à opacidade. Quando o funcionamento desses sistemas não é transparente para crianças, adolescentes e seus responsáveis, o dever de informação deixa de cumprir sua função protetiva. Desse modo, deve-se pensar em formas de incentivar que fornecedores que se utilizam de algoritmos com impacto relevante sobre a experiência de crianças e adolescentes divulguem, em linguagem acessível, os critérios gerais de funcionamento desses sistemas, bem como os mecanismos disponíveis para contestá-los ou limitá-los.

Neste ponto, entendemos que há um desafio em não deixar que o dever de informação permaneça incompleto nos serviços em que o risco ao desenvolvimento biopsicossocial é mais significativo, como aqueles que organizam fluxos personalizados de conteúdo, recompensas, notificações e recomendações contínuas. Portanto, desincentivar o fornecedor a adotar modelos comunicacionais que ocultem riscos, dispersem informações essenciais ou dificultem a reversão de escolhas torna o dever de informação mais palpável. Seguindo a lógica do privacy by design, isso inclui ser transparente desde a concepção do desenho do serviço, tornando acessíveis as informações sobre ferramentas de mobilização de atenção, permanência e retorno. Essas informações são condições indispensáveis para que crianças, adolescentes e seus responsáveis possam, de fato, exercer as escolhas que o Guia descreve como finalidade deste dever.

Quanto ao dever de segurança, o Guia o conceitua de forma mais ampla do que a

39 MENDONÇA, Eduardo; NÓVOA, Natasha; RODRIGUES, Carla. **Contribuições da Data Privacy Brasil à Embaixada da França: questionário sobre inteligência artificial e crianças.** São Paulo: Data Privacy Brasil, 2026. P. 3.

proteção técnica de dados pessoais, alcançando vetores de dano típicos do ambiente digital, como exploração sexual, assédio e indução a comportamentos nocivos. Essa leitura dialoga com o art. 6º do ECA Digital, que elenca condutas específicas que os fornecedores devem prevenir. O Guia também acerta ao vincular a intensidade do dever ao grau de interferência do agente sobre conteúdos e interações.

Um ponto que pode ser aprofundado é a ausência de orientação sobre como o dever de segurança se articula com a responsabilidade solidária prevista no art. 15 do ECA Digital. O Guia menciona a proporcionalidade conforme o porte e a natureza do fornecedor, mas não orienta como os deveres de segurança se distribuem na cadeia digital, especialmente entre sistemas operacionais, lojas de aplicações e aplicações de internet, nem o que se espera de cada agente para que a proteção solidária seja efetiva. Por isso, recomendamos complementar essa seção com orientações sobre a coordenação de medidas entre os diferentes agentes da cadeia, incluindo obrigações mínimas de governança interna, como designação de responsáveis, revisões periódicas e planos de resposta a incidentes que contemplem especificamente a proteção de crianças e adolescentes, articulando esse dever com os princípios de segurança, prevenção e responsabilização previstos no art. 6º da LGPD.

Dentro do escopo delimitado no Guia Orientativo, há interesse em incluir novos temas? Em caso afirmativo, quais seriam e qual a justificativa para essa inclusão?

A Data Privacy Brasil identifica ao menos seis temas que, embora estejam relacionados ao escopo atual do Guia, ainda não receberam tratamento analítico suficiente para assegurar a efetividade do ECA Digital. A inclusão desses temas não amplia indevidamente o objeto do Guia. Ao contrário, densifica categorias já presentes na minuta, como acesso provável, dever de prevenção, dever de proteção, dever de informação, dever de segurança e design seguro. Também contribui para reduzir zonas de silêncio que podem ser instrumentalizadas por fornecedores para limitar obrigações, fragmentar responsabilidades ou sustentar interpretações excessivamente formais da Lei nº 15.211/2025.

Em nossa visão, o Guia deve avançar de uma descrição geral dos deveres para uma orientação mais operacional sobre como esses deveres se aplicam em ecossistemas digitais marcados por múltiplos fornecedores, interfaces persuasivas, sistemas de recomendação, monetização indireta, inteligência artificial generativa, serviços híbridos e intensa circulação de crianças e adolescentes. Esse aprofundamento é compatível com o próprio objetivo do Guia, que pretende esclarecer o escopo de aplicação do ECA Digital e o significado dos deveres de prevenção, proteção, informação e segurança. A seguir, apresentamos os temas que deveriam ser incluídos ou aprofundados, sua justificativa e uma proposta de tratamento.

Ademais, sugerimos que o Guia incorpore o design como quinta dimensão autônoma do dever de prevenção, ao lado da prevenção em sentido estrito, da proteção, da informação e da segurança. Os arts. 7º e 8º, IV, da Lei já reconhecem que escolhas arquiteturais - configurações por padrão, mecanismos de engajamento, interfaces de consentimento

- produzem efeitos jurídicos independentes da conduta de terceiros. Como observa Monteiro (2026), as decisões regulatórias mais relevantes sobre plataformas digitais não são tomadas em tribunais, mas em reuniões internas de produto, por equipes que muitas vezes não percebem que estão assumindo compromissos com consequências jurídicas diretas.

Reconhecer o design como dimensão expressa do dever de prevenção teria três consequências práticas. Primeiro, orientaria fornecedores a tratar obrigações legais como restrições de projeto desde a concepção - e não como camadas de conformidade adicionadas ao final do desenvolvimento -, em linha com a lógica do *privacy and safety by default* já consagrada nos arts. 7º e 8º da Lei. Segundo, permitiria à ANPD avaliar não apenas se o fornecedor adotou medidas pontuais, mas se a arquitetura do serviço, em sua totalidade, é compatível com a proteção integral de crianças e adolescentes. Terceiro, deslocaria o ônus de justificação: funcionalidades que promovem engajamento compulsivo, que reduzem fricções para permanecer e aumentam fricções para sair, ou que organizam fluxos de recomendação sem transparência deveriam ser justificadas pelo fornecedor como proporcionais - e não presumidas como neutras até prova em contrário.

Novo tema	Justificativa	Proposta de inclusão
Design abusivo como vício ou defeito de concepção	O Guia trata o design de forma dispersa, como elemento de atratividade ou como referência ao design protetivo, mas não reconhece suficientemente que certas arquiteturas, como rolagem infinita, autoplay, ocultação de pontos de parada, notificações manipulativas, recompensas variáveis e fluxos que dificultam a saída, podem constituir vício ou defeito de concepção do produto ou serviço. Essa leitura é importante porque tais escolhas não são meramente estéticas ou periféricas. Elas integram o próprio serviço ofertado e podem explorar a vulnerabilidade e a imaturidade decisória de crianças e adolescentes. A literatura sobre padrões obs-	Incluir subseção no dever de prevenção, ou uma quinta dimensão autônoma, intitulada "Do design abusivo como defeito de concepção". A seção deve orientar que, nos termos do CDC e do ECA Digital, interfaces que induzem uso compulsivo, dificultam a saída, ocultam escolhas protetivas ou exploram vulnerabilidades de crianças e adolescentes devem ser tratadas como defeituosas em sua concepção, atraindo deveres de prevenção, correção, mitigação e responsabilização dos fornecedores que as estruturaram.

	curos de design reforça que o design é um ato persuasivo e que determinadas escolhas deinterface podem subverter princípios de centralidade no usuário em favor dos interesses do fornecedor.	
Responsabilidade objetiva e solidária na cadeia digital	O Guia define lojas de aplicações, sistemas operacionais e aplicações de internet como fornecedores, mas ainda não esclarece suficientemente como se distribui a responsabilidade quando o risco ou o dano decorre da interação entre diferentes agentes da cadeia digital. Isso é relevante em situações como loja de aplicações que distribui aplicativo com design abusivo, sistema operacional que não implementa controles protetivos eficazes ou aplicação que depende de configurações padrão permissivas para ampliar retenção, coleta de dados ou exposição.	Incluir orientação específica sobre "Responsabilidade solidária na cadeia de fornecimento digital", com remissão à lógica do CDC e ao art. 15 do ECA Digital. O Guia deve explicitar que a existência de múltiplos agentes técnicos não pode diluir a responsabilidade pela proteção de crianças e adolescentes. Lojas de aplicações, sistemas operacionais e aplicações devem demonstrar quais medidas adotaram para prevenir riscos previsíveis, especialmente quando controlam pontos de entrada, distribuição, configuração, interoperabilidade, sinal de idade, controles parentais ou padrões de segurança.
Limites ao argumento do risco do desenvolvimento	O Guia menciona a avaliação prospectiva de risco, mas não enfrenta suficientemente a possibilidade de fornecedores alegarem que determinados danos seriam imprevisíveis por estarem associados à inovação tecnológica. Esse argumento, próximo à ideia de risco do desenvolvi-	Incluir subseção no dever de segurança intitulada "Limites ao argumento do risco do desenvolvimento". O Guia deve afirmar que inovação, complexidade técnica ou caráter emergente de determinada tecnologia não afastam o dever de prevenir riscos conhecidos ou

	mento, não deve funcionar como salvo-conduto para arquiteturas digitais que já apresentam riscos conhecidos ou previsíveis, especialmente quando envolvem crianças e adolescentes. A prioridade absoluta prevista no art. 227 da Constituição Federal e a lógica preventiva do ECA Digital exigem que a novidade tecnológica não seja utilizada para neutralizar deveres de cuidado.	previsíveis segundo o estado da arte. O ônus de demonstrar a imprevisibilidade concreta do risco deve recair sobre o fornecedor, que deverá apresentar documentação técnica, avaliação de impacto, testes de segurança, histórico de incidentes, medidas de mitigação e justificativas para as escolhas adotadas. A regulação baseada em risco não deve ser tratada como método técnico autônomo capaz de deslocar a prioridade normativa da proteção integral.
Inteligência artificial generativa e riscos específicos para crianças e adolescentes	O Guia menciona sistemas de inteligência artificial generativa como fornecedores com presunção de acesso provável, mas ainda não desenvolve os riscos qualitativamente distintos desses sistemas. Ferramentas generativas podem produzir conteúdo inadequado sob demanda, simular relações afetivas, personalizar respostas a partir de perfis comportamentais, induzir confiança excessiva, gerar *deepfakes* envolvendo adolescentes, produzir alucinações com aparência de autoridade e explorar vulnerabilidades por meio de personalização preditiva. A análise deve ser calibrada ao desenvolvimento, considerando a relação entre *affordan-*	Incluir subseção autônoma sobre “Inteligência artificial generativa e riscos específicos para crianças e adolescentes”. O Guia deve orientar que fornecedores de IA generativa realizem avaliações de impacto centradas em alucinações, conteúdo gerado sem supervisão adequada, simulação de afeto, antropomorfização, personalização, treinamento ou ajuste com dados de crianças e adolescentes, transparência sobre limitações do sistema e mecanismos de denúncia, bloqueio, contestação e escalonamento humano.

	ces tecnológicas, restrições, tarefas, competências e vulnerabilidades adolescentes.	
Serviços de mensageria e aplicabilidade do ECA Digital	O Guia exclui serviços de mensageria privada da definição de rede social, o que é tecnicamente adequado. No entanto, não esclarece suficientemente quais obrigações lhes são aplicáveis quando forem fornecedores de produto ou serviço de tecnologia da informação de acesso provável por crianças e adolescentes. Essa omissão pode criar zona de desresponsabilização, especialmente diante do uso intenso de serviços	Incluir orientação interpretativa sobre "Serviços de mensageria e aplicabilidade do ECA Digital". O Guia deve explicitar que, embora não sejam redes sociais, serviços de mensageria de acesso provável estão sujeitos aos deveres gerais de prevenção, informação e segurança, especialmente quanto a mecanismos de bloqueio de contatos indesejados, denúncia de abuso, configurações protetivas por padrão, controles adequados à idade, gestão de grupos, limitação de encaminhamento e canais acessíveis a crianças, adolescentes e responsáveis.
Participação de crianças e adolescentes na elaboração de políticas e avaliação de impacto	O Guia ainda é pouco desenvolvido quanto ao direito de crianças e adolescentes de participar das decisões que afetam seus direitos digitais. A ausência de diretrizes sobre escuta adaptada, consultas com linguagem acessível, metodologias participativas e avaliação da compreensão por esse público reproduz uma lógica adultocêntrica de regulação.	Incluir seção final sobre "Participação de crianças e adolescentes nos processos regulatórios e nas avaliações de impacto". O Guia deve recomendar que a ANPD, em futuras atualizações ou instrumentos complementares, incorpore mecanismos de consulta a crianças e adolescentes, como grupos focais, materiais em linguagem adaptada, parcerias com escolas, organizações da sociedade civil e especialistas em infância. Também deve orientar fornecedores, quando

		proporcional ao risco e à escala do serviço, a realizar testes de compreensão e processos éticos de escuta para avaliar a efetividade de informações, controles e salvaguardas.

A Data Privacy Brasil sugere que o Guia incorpore o design como quinta dimensão autônoma do dever de prevenção, ao lado da prevenção em sentido estrito, da proteção, da informação e da segurança. Os arts. 7º e 8º, IV, da Lei já reconhecem que escolhas arquiteturais - configurações por padrão, mecanismos de engajamento, interfaces de consentimento - produzem efeitos jurídicos independentes da conduta de terceiros. Como observa Monteiro (2026), as decisões regulatórias mais relevantes sobre plataformas digitais não são tomadas em tribunais, mas em reuniões internas de produto, por equipes que muitas vezes não percebem que estão assumindo compromissos com consequências jurídicas diretas.

Reconhecer o design como dimensão expressa do dever de prevenção teria três consequências práticas. Primeiro, orientaria fornecedores a tratar obrigações legais como restrições de projeto desde a concepção - e não como camadas de conformidade adicionadas ao final do desenvolvimento -, em linha com a lógica do privacy and safety by default já consagrada nos arts. 7º e 8º da Lei. Segundo, permitiria à ANPD avaliar não apenas se o fornecedor adotou medidas pontuais, mas se a arquitetura do serviço, em sua totalidade, é compatível com a proteção integral de crianças e adolescentes. Terceiro, deslocaria o ônus de justificação: funcionalidades que promovem engajamento compulsivo, que reduzem fricções para permanecer e aumentam fricções para sair, ou que organizam fluxos de recomendação sem transparência deveriam ser justificadas pelo fornecedor como proporcionais - e não presumidas como neutras até prova em contrário.

A inclusão desses temas confere ao Guia maior operacionalidade e reduz o risco de que zonas de silêncio sejam instrumentalizadas por fornecedores para limitar seus deveres de proteção. Em particular, a qualificação do design abusivo como defeito de concepção e a explicitação da responsabilidade solidária na cadeia digital respondem diretamente à necessidade de superar uma lógica reativa, insuficiente para enfrentar riscos estruturais decorrentes de escolhas arquiteturais das plataformas. O Guia deve deixar claro que o ECA Digital não se limita a reagir a danos já consumados. Sua função é orientar a concepção, a operação e a governança de produtos e serviços digitais para que sejam compatíveis, desde a origem, com a proteção integral de crianças e adolescentes.

REFERÊNCIAS

BOYD, danah. **Why Youth Social Network Sites: The Role of Networked Publics in Teenage Social Life. In: BUCKINGHAM, David (ed.). Youth, Identity, and Digital Media.** Cambridge, MA: The MIT Press, 2008. p. 119-142. DOI: https://doi.org/10.1162/dmal.9780262524834.119. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1345415. Acesso em: 9 jun. 2026.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 11 jun. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.** Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jun. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 11 jun. 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: seção 1, edição extra A, Brasília, DF, p. 1, 17 set. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm. Acesso em: 11 jun. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 11 jun. 2026.

CALIFORNIA. Legislature. Senate Bill No. 976, Chapter 321. **Protecting Our Kids from Social Media Addiction Act. Sacramento: California Legislative Information, 2024.** Approved by Governor and filed with Secretary of State, 20 Sept. 2024. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB976. Acesso em: 11 jun. 2026.

FRANCE. Commission Nationale de l'Informatique et des Libertés. **Cookie regulation: the CNIL is continuing the action plan initiated in 2019 and has imposed two fines on SHEIN and GOOGLE.** Paris: CNIL, 3 Sept. 2025. Disponível em: https://www.cnil.fr/en/cookie-regulation-cnil-continuing-action-plan -initiated-2019-and-has-imposed-two-fines-shein-and. Acesso em: 11 jun. 2026.

FROTA, Ana Maria Monte Coelho. **Diferentes concepções da infância e adolescência: a importância da historicidade para sua construção.** Estudos e Pesquisas em Psicologia, Rio de Janeiro, v. 7, n. 1, p. 147-160, abr. 2007. Disponível em: http://www.redalyc.org/articulo.oa?id=451844613015. Acesso em: 9 jun. 2026.

LIVINGSTONE, Sonia. **Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression.** New Media & Society, London, v. 10, n. 3, p. 393-411, 2008. DOI: https://doi.org/10.1177/1461444808089415. Disponível em: https://doi.org/10.1177/1461444808089415. Acesso em: 9 jun. 2026.

LIVINGSTONE, Sonia; THIRD, Amanda. **Children and young people's rights in the digital age: an emerging agenda.** New Media & Society, [s. l.], v. 19, n. 5, p. 657-670, 2017. DOI: https://doi.org/10.1177/1461444816686318. Disponível em: https://doi.org/10.1177/1461444816686318. Acesso em: 9 jun. 2026.

MENDONÇA, Eduardo; NÓVOA, Natasha; RODRIGUES, Carla. **Contribuições da Data Privacy Brasil à Embaixada da França: questionário sobre inteligência artificial e crianças.** São Paulo: Data Privacy Brasil, 2026. p. 3.

MONTEIRO, Renato Leite. **Design is law: regulatory consequences of interface choices in AI systems.** Interactions, Nova York, v. 33, n. 2, p. 39-43, mar./abr. 2026.

MONTGOMERY, Kathryn C.; CHESTER, Jeff. **Interactive food and beverage marketing: targeting adolescents in the digital age.** Journal of Adolescent Health, [s. l.], v. 45, n. 3, supl., p. S18-S29, 2009. DOI: https://doi.org/10.1016/j.jadohealth.2009.04.006. Disponível em: https://doi.org/10.1016/j.jadohealth.2009.04.006. Acesso em: 9 jun. 2026.

NEW MEXICO. **First Judicial District Court, County of Santa Fe. State of New Mexico, ex rel. Raúl Torrez, Attorney General v. Meta Platforms, Inc.; Instagram, LLC; Meta Payments, Inc.; Meta Platforms Technologies, LLC; and Mark Zuckerberg.** Case No. D-101-CV-2023-02838. Plaintiff's Complaint for Abatement and Civil Penalties and Demand for Jury Trial. Santa Fe: First Judicial District Court, 5 Dec. 2023. Disponível em: https://nmag.gov/wp-content/uploads/2024/01/2023-12-05-NM-v.-Meta-et-al.-COMPLAINT-REDACTED.pdf. Acesso em: 11 jun. 2026.

NEW YORK. Senate. **Senate Bill S7694A, 2023-2024 Legislative Session. Stop Addictive Feeds Exploitation (SAFE) for Kids Act.** Albany: New York State Senate, 2024. Signed by Governor, Chap. 120, 20 June 2024. Disponível em: https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A. Acesso em: 11 jun. 2026.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024 [tabelas].** São Paulo: NIC.br, 2024. Disponível em: https://cetic.br/pt/tics/kidsonline/2024/criancas/C9/. Acesso em: 9 jun. 2026.

O'KEEFFE, Gwenn Schurgin; CLARKE-PEARSON, Kathleen; COUNCIL ON COMMUNICATIONS AND MEDIA. **The impact of social media on children, adolescents, and families.** Pediatrics, [s. l.], v. 127, n. 4, p. 800-804, abr. 2011. DOI: https://doi.org/10.1542/peds.2011-0054. Disponível em: https://pediatrics.aappublications.org/content/127/4/800. Acesso em: 9 jun. 2026.

ODGERS, Candice L.; JENSEN, Michaeline R. **Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions.** Journal of Child Psychology and Psychiatry, [s. l.], v. 61, n. 3, p. 336-348, 2020. DOI: https://doi.

org/10.1111/jcpp.13190. Disponível em: https://doi.org/10.1111/jcpp.13190. Acesso em: 9 jun. 2026.

RODRIGUES, Carla; MENDONÇA, Eduardo Gomes; ZANATTA, Rafael A. F. **O conceito jurídico de acesso provável no ECA Digital.** São Paulo: Data Privacy Brasil, 2026. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2026/01/20250119_acesso-provavel-Eca-Digital.pdf. Acesso em: 9 jun. 2026.

UNIÃO EUROPEIA. **Parlamento Europeu; Conselho da União Europeia. Regulamento (UE) 2016/679, de 27 de abril de 2016.** Jornal Oficial da União Europeia, Luxemburgo, L 119, p. 1-88, 4 maio 2016, art. 7º, item 3. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj/por. Acesso em: 11 jun. 2026.

UNIÃO EUROPEIA. **Parlamento Europeu; Conselho da União Europeia. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).** Jornal Oficial da União Europeia, Luxemburgo, L, 2024/1689, 12 jul. 2024. Art. 5º. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?eliuri=eli%3Areg%3A2024%3A1689%3Aoj&locale=pt. Acesso em: 11 jun. 2026.

UNIÃO EUROPEIA. **Tribunal de Justiça da União Europeia. Acórdão do Tribunal de Justiça, Grande Secção, de 1º de outubro de 2019. Processo C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV contra Planet49 GmbH. ECLI:EU:C:2019:801.** Luxemburgo: Tribunal de Justiça da União Europeia, 2019. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=218467&doclang=PT. Acesso em: 11 jun. 2026.

UNITED KINGDOM. **Information Commissioner's Office. Reddit, Inc.** Wilmslow: ICO, 23 Feb. 2026. Disponível em: https://ico.org.uk/action-weve-taken/enforcement/2026/02/reddit-inc/. Acesso em: 11 jun. 2026.

UNITED KINGDOM. **Office of Communications. Final Decision CW.01283.04.24: Fenix International Limited.** London: Ofcom, 26 Mar. 2025. Disponível em: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/enforcement/final-decision-cw.01283.04.24-fenix-international-limited.pdf. Acesso em: 11 jun. 2026.

UNITED STATES OF AMERICA. **Federal Trade Commission. Amazon.com, Inc. (ROSCA), FTC v. Case No. 2:23-cv-0932-JHC.** Washington, DC: Federal Trade Commission, 2023-2025. Disponível em: https://www.ftc.gov/legal-library/browse/cases-proceedings/2123050-amazoncom-inc-rosca-ftc-v. Acesso em: 11 jun. 2026.

UNITED STATES OF AMERICA. **Federal Trade Commission; THE PEOPLE OF THE STATE OF CALIFORNIA. Federal Trade Commission and The People of the State of California v. NGL Labs, LLC; Raj Vir; Joao Figueiredo. Case No. 2:24-cv-05753-JLS-PVC. Stipulated Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief.** United States District Court, Central District of California, 14 July 2024. Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/DN008Stipu-

latedOrderforPermanentInjunction.pdf. Acesso em: 11 jun. 2026.

UNITED STATES OF AMERICA. **Superior Court of California, County of Los Angeles. P.F., et al. (K.G.M.) v. Meta Platforms, Inc., et al. Case No. 23SMCV03371; Lead Case No. 22STCV21355. Verdict Form — Meta.** Los Angeles: Superior Court of California, County of Los Angeles, 25 Mar. 2026. Disponível em: https://www.crowell.com/a/web/b3HgCKaRwDn5JSu1FVt4Vg/verdict-form-meta.pdf. Acesso em: 11 jun. 2026.

ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Júlia. **Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. In: COSTA, Ana Cláudia et al. (org.). LGPD e Crianças e Adolescentes.** São Paulo: Thomson Reuters Revista dos Tribunais, 2021. p. 14.