

Tomada de Subsídios conceitos previstos no ECA Digital

Conheça mais sobre a [Tomada de Subsídios](#).

39 respostas totais

Resposta #1

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
216272520507473716664650	Registrado	314038638259115145093461	50%	28/11/2025 12:41

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Teste teste teste teste

Envio de arquivo.

- [Download attachment pdf 13 KB](#)

Resposta #2

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
369432513541654335860731	Registrado	314038638259115145093461	50%	29/11/2025 20:58

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Os próprios conceitos de "criança" e "adolescente". É preciso deixar claro que se tratam de pessoas físicas, ou seja seres humanos reais, para que a lei não seja usada para criminalizar trabalhos artísticos, promovendo censura.

Envio de arquivo.

-

Resposta #3

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
226017071123743365550752	Registrado	314038638259115145093461	50%	01/12/2025 14:45
Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos? Acesso provável. Em que circunstâncias será aplicada a proibição de atividades. Envio de arquivo. -				

Resposta #4				
Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
260866158233133586136302	Registrado	314038638259115145093461	50%	01/12/2025 22:45
Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos? Principais conceitos que demandam esclarecimentos no ECA Digital (Lei nº 15.211/2025) 1. Produto ou serviço de tecnologia da informação (art. 2º, I) O conceito é amplo e pode incluir desde plataformas comerciais até ferramentas educacionais comunitárias. É necessário delimitar se abrange apenas serviços ofertados com finalidade econômica ou também iniciativas públicas/comunitárias. Parâmetros: finalidade, modelo de negócio e grau de interação com dados pessoais. 2. Acesso provável (art. 1º, parágrafo único) A expressão é vaga e pode gerar insegurança sobre quais serviços devem aplicar medidas protetivas. Parâmetros: métricas de probabilidade (percentual de usuários menores de 18 anos, classificação indicativa, atratividade do conteúdo). Deve considerar contextos coletivos, como povos e comunidades tradicionais. 3. Provedores de conteúdos com controle editorial (art. 39, §1º) A distinção entre curadoria humana e algoritmos automatizados não está clara. Parâmetros: definir controle editorial como intervenção humana direta na seleção ou organização de conteúdos, diferenciando de sistemas de recomendação algorítmica. 4. Provedores de conteúdos protegidos por direitos autorais (art. 39, §1º) Há dúvida sobre plataformas que hospedam conteúdos mistos (autorais e não autorais). Parâmetros: indicar se a obrigação recai sobre todo o serviço ou apenas sobre a parte que disponibiliza conteúdo protegido. Prever salvaguardas específicas para expressões culturais coletivas, como saberes tradicionais. 5. Deveres de prevenção, proteção, informação e segurança (art. 5º, caput) O texto desloca a responsabilidade para uma postura preventiva, mas não define parâmetros mínimos. Parâmetros: detalhar requisitos de due diligence (relatórios de impacto, mecanismos de supervisão parental, classificação de riscos). Prever adaptações culturais e linguísticas para garantir efetividade junto a diferentes comunidades. Envio de arquivo. -				

Resposta #5				
Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
190776499908430720050222	Registrado	314038638259115145093461	50%	11/12/2025 10:14

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Associação Brasileira de Medicina e Diagnóstica ("ABRAMED") encaminha no documento anexo, sua proposta e contribuições para a Tomada de Subsídio. Em tempo, se coloca a total disposição para esclarecimento ou alinhamento sobre o tema, considerando o impacto para a população e a cadeia de saúde como um todo. Agradecemos a possibilidade de participação da sociedade civil e do setor empresarial em um assunto tão sensível e necessário.

Envio de arquivo.

- [Download attachment.pdf 377 KB](#)

Resposta #6

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
256006792690104779207397	Registrado	314038638259115145093461	50%	11/12/2025 10:14

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Capítulo IV: Mecanismos de Aferição de Idade; Capítulo V: Controles Parentais; Capítulo XI: Reportes de Violação aos Direitos de Crianças e Adolescentes; Capítulo XII: Relatórios de Transparência; Documento completo em anexo.

Envio de arquivo.

- [Download attachment.pdf 105 KB](#)

Resposta #7

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
141693632959326419259032	Registrado	314038638259115145093461	50%	11/12/2025 10:53

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

1. "Design manipulativo": requer definição precisa porque é um termo amplo. Sem critérios técnicos, práticas que explorem vulnerabilidades de crianças podem ser tratadas como neutras, dificultando fiscalização e responsabilização. 2. "Configurações que evitem uso compulsivo": a expressão é vaga e depende de parâmetros objetivos. Mecanismos como autoplay, rolagem infinita e notificações excessivas induzem uso prolongado; por isso, é necessário definir limites mensuráveis para tornar a regra aplicável. 3. "Comprometer a autonomia": a autonomia infantil é facilmente afetada por estímulos persuasivos. Sem clareza, fornecedores podem alegar que certas escolhas de interface não reduzem autonomia, mesmo quando manipulam comportamento. 4. "Manipular interfaces": interfaces podem ser manipuladas ao ocultar opções, dificultar configurações ("fricção") ou criar fluxos pouco intuitivos. A definição evita que práticas nocivas sejam justificadas como simples decisões de design. 5. "Exposição vexatória ou constrangedora": a expressão deve abranger humilhação, desafios arriscados, "pegadinhas", deepfakes e monetização do sofrimento infantil, impedindo que conteúdos danosos sejam tratados como humor ou entretenimento.

Envio de arquivo.

- [Download attachment pdf 224 KB](#)

Resposta #8

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
707281327254867769465530	Registrado	314038638259115145093461	50%	11/12/2025 17:16

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

As contribuições da Samsung Eletrônica da Amazônia LTDA. estão no arquivo em anexo.

Envio de arquivo.

- [Download attachment pdf 285 KB](#)

Resposta #9

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
429756204428317045354282	Registrado	314038638259115145093461	50%	11/12/2025 17:41

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Mecanismos confiáveis de verificação de idade: conforme art. 9º, §1º, é dever dos fornecedores de produtos ou serviços de tecnologia da informação não veicularem conteúdo impróprio, inadequado ou proibido para menores, adotar mecanismos confiáveis de verificação de idade a cada acesso. Já o art. 11 prevê que o Poder Público poderá atuar como regulador, certificador ou promotor de soluções de verificação de idade. Nesse sentido, o conceito de “mecanismo confiável de verificação de idade” é o maior desafio da Lei 15.211/25. Segundo o radar tecnológico nº 5 da ANPD, existem 4 gerações de soluções para aferição de idade online: (i) autodeclaração (vedada pelo §1º do art. 9º); (ii) verificação documental e biometria; (iii) estimativas ou inferências biométricas ou comportamentais e; (iv) tokens e provas criptográficas. O papel do Poder Público, especialmente na promoção de soluções de verificação de idade embarcadas por tecnologias da quarta geração será essencial para não prejudicar pequenas e microempresas especialmente, haja vista o dispêndio de recursos necessários para implementar tais soluções. As provas de conhecimento zero (ZKP) são importantes nesse debate, mas não são imbatíveis ou à prova de falha, dependendo sempre da correta implementação com as aplicações de internet. Por fim, as soluções de segunda e terceira geração podem ser manipuláveis com IA, além de criarem um desequilíbrio quanto à proteção de dados pessoais. Conteúdo impróprio ou inadequado; conforme o §2º do art. 9º, “conteúdos impróprios ou inadequados” são aqueles que contêm material pornográfico ou outros vedados pela legislação. Destacamos que o art. 81 do ECA já prevê uma lista de itens cuja venda é proibida a crianças e adolescentes. Do mesmo modo, o art. 16, II da Lei 14.790/23 prevê a proibição da participação de menores de 18 anos em produtos e serviços de apostas de quota fixa. Logo, é imprescindível a preexistência de normativos públicos para fixar o conceito e evitar seu alargamento.

Envio de arquivo.

-

Resposta #10

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
824921825621226884268545	Registrado	314038638259115145093461	50%	12/12/2025 10:06

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Federação das Indústrias do Estado de São Paulo (FIESP) reconhece a importância de um marco legal para a proteção de crianças e adolescentes no ambiente digital e entende que sua eficácia depende da elucidação de conceitos que ainda apresentam elevado grau de indeterminação jurídica. Sinteticamente, apontam-se os seguintes termos, com detalhamento anexo: 1) “acesso provável” (art. 1º, p.u.) baseado em qualificadores vagos, deve ser aferido por evidências objetivas, como perfil etário real de usuários e direcionamento de conteúdo; 2) “acesso possível” deve ser distinguido de “acesso provável”, pois o primeiro é universal, enquanto o segundo exige previsibilidade de uso por crianças e adolescentes; 3) “atratividade” (art. 1º, p.u., I) não pode decorrer de elementos estéticos isolados, devendo considerar intenção do fornecedor, conteúdo infantil e marketing direcionado; 4) “medidas razoáveis” (art. 6º) exigem padrão mínimo de diligência, escalonado por porte da empresa e nível de risco; 5) “medidas adequadas” (art. 3º) devem ser traduzidas em controles técnicos e organizacionais mínimos, proporcionais ao risco; 6) “exploração comercial” (art. 4º, VI) necessita delimitação para abranger apenas práticas abusivas, não modelos legítimos de monetização; 7) “uso compulsivo” (art. 8º, IV) é conceito clínico, devendo a obrigação limitar-se à oferta de ferramentas de bem-estar digital; 8) “desenvolvimento progressivo” (art. 7º) demanda parâmetros etários objetivos, com regimes graduais de autonomia e proteção; 9) “mecanismos confiáveis de verificação de idade” (art. 9º) devem seguir abordagem baseada em risco e preservação da privacidade; 10) a expressão “a cada acesso” (art. 9º, §1º) deve ser interpretada de forma material, restrita a momentos relevantes da jornada do usuário; e 11) a vedação à “autodeclaração” (art. 9º, §1º) deve ser entendida como proibição da declaração unilateral não validada, admitindo mecanismos verificáveis.

Envio de arquivo.

- [Download attachment pdf 209 KB](#)

Resposta #11

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
565993141115243102486609	Registrado	314038638259115145093461	50%	12/12/2025 10:24

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

O ECA DIGITAL é uma resposta normativa à necessidade de enfrentar de modo estruturado e preventivo as ameaças que se projetam sobre crianças e adolescentes no ambiente virtual. Logo, o conceito de “acesso provável” deverá ser direcionado a situações que envolvam ameaças concretas a crianças e adolescentes no ambiente virtual. Este foi o intuito da legislação. Logo, tal conceito deverá considerar os serviços que usualmente são acessados diretamente por crianças e adolescentes como, por exemplo, as redes sociais e plataformas de jogos, afastando outros ambientes. Por exemplo, no âmbito da saúde suplementar, não faz sentido considerar como de “acesso provável” a utilização de áreas restritas para beneficiários de planos de saúde, tendo em vista que tais ambientes são utilizados por maiores de idade para a verificação de extratos de utilização, mensalidades, solicitações de procedimentos, alterações cadastrais, dentre outras atividades (RN 509 da ANS). Expandir os cuidados do ECA Digital para todo e qualquer serviço digital, ainda que não usualmente acessado por menores, apenas por conta da “facilidade de uso e utilização” poderá causar uma sobrecarga inadequada de obrigações para os agentes que não atendem menores em suas plataformas, causando um ônus desnecessário. A nossa sugestão, portanto, seria considerar os incisos I, II e III do art. 1º do ECA Digital como cumulativos. Sendo assim, entendemos que o conceito de “acesso provável” deverá considerar aquelas situações que, pelas regras de experiência, são usualmente usufruídas por menores.

Envio de arquivo.

Resposta #12

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
1081351885653428054943553	Registrado	314038638259115145093461	50%	12/12/2025 10:54

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Um dos conceitos que demandam esclarecimento na Lei nº 15.211/2025 é a definição de “produto ou serviço de tecnologia da informação” prevista no art. 2º, inciso I. A redação atual estabelece que tais produtos devem ser “fornecidos a distância, por meio eletrônico e providos em virtude de requisição individual”, exemplificando aplicações de internet, softwares, sistemas operacionais, lojas de aplicativos e jogos eletrônicos conectados à internet. Essa formulação, porém, pode gerar um alcance restritivo da lei. Ao condicionar o enquadramento ao modo de fornecimento (remoto, por exemplo) a definição acaba deixando de fora produtos digitais utilizados por crianças e adolescentes que podem ser adquiridos fisicamente e executados em consoles domésticos (por exemplo, no Nintendo Switch, The Legend of Zelda: Tears of the Kingdom, Mario Kart 8 Deluxe, ou ainda no PlayStation, tanto o 4 quanto o 5, o jogo Minecraft), experiências digitais locais e aplicações de realidade virtual ou aumentada que operam sem conexão contínua à internet (como o jogo Astrobot, por exemplo). Embora tais produtos envolvam interação digital, coleta ou exposição a dados, possibilidade de acesso a conteúdo sensível e riscos associados ao uso infantil, eles não se enquadram tecnicamente no modelo de fornecimento descrito pelo inciso I. É importante destacar que nenhum outro dispositivo do artigo mencionado corrige essa limitação. Os demais incisos herdam a mesma restrição. Assim, produtos digitais utilizados, mas não fornecidos “a distância”, ficariam fora do âmbito protetivo da lei, o que criaria um vazio regulatório incompatível com o objetivo central do Estatuto de garantir ambiente digital seguro e adequado ao melhor interesse da criança e do adolescente. Por esse motivo, seria interessante que o conceito fosse complementado para abranger, produto ou serviço digital independentemente do modo de aquisição, forma de distribuição comercial ou da necessidade de conectividade permanente.

Envio de arquivo.

Resposta #13

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
676456813871376785141018	Registrado	314038638259115145093461	50%	12/12/2025 13:15

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Fornecedores de produtos ou serviços de tecnologia da informação com “acesso provável” Art. 1º, parágrafo único 2. “Perfilamento” para publicidade comercial Art. 2º, V c/c art. 22 e 26 3. Tratamento dos dados pessoais de crianças e de adolescentes de forma que “cause, facilite ou contribua” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei Arts. 2º, V, 22 e 26 4. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser “utilizados unicamente para essa finalidade” Art. 13 5. Mecanismos de Supervisão Parental Arts. 2º, VIII, art. 12, III e art. 16 e ss 6. Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais Art. 16, parágrafo único, II 7. Verificação de idade “a cada acesso” do usuário ao conteúdo, produto ou serviço Art. 9, §1º

Envio de arquivo.

-

Resposta #14

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
140930235596888332503346	Registrado	314038638259115145093461	50%	12/12/2025 15:03

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Resposta consta do arquivo anexo.

Envio de arquivo.

- [Download attachment pdf 212 KB](#)

Resposta #15

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
679727591617393798947446	Registrado	314038638259115145093461	50%	12/12/2025 15:51

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Em atenção à Consulta Pública aberta em 28 de novembro de 2025, o escritório de advocacia Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados (SBSA Advogados), especializado em Direito do Terceiro Setor, vem apresentar recomendações e sugestões para esclarecimento de conceitos da Lei nº 15.211/2025 (“ECA Digital”). Nesta contribuição, buscaremos responder à pergunta formulada pela ANPD. Nossa análise, que consta do arquivo em anexo, prioriza conceitos que impactam diretamente organizações da sociedade civil que atuam na proteção de crianças e adolescentes, bem como aqueles cuja interpretação demanda harmonização com a Lei Geral de Proteção de Dados Pessoais (LGPD), buscando inspiração em padrões internacionais consolidados.

Envio de arquivo.

-

Resposta #16

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
941112910891725559174177	Registrado	314038638259115145093461	50%	12/12/2025 15:56

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

-Fornecedores de produtos ou serviços de tecnologia da informação com “acesso provável”. Art. 1º, parágrafo único 2. -“Perfilamento” para publicidade comercial. Art. 2º, V c/c art. 22 e 26 3. -Tratamento dos dados pessoais de crianças e de adolescentes de forma que “cause, facilite ou contribua” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei. Arts. 2º, V, 22 e 26 4. -Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser “utilizados unicamente para essa finalidade”. Art. 13 5. - Mecanismos de Supervisão Parental. Arts. 2º, VIII, art. 12, III e art. 16 e ss 6. -Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais. Art. 16, parágrafo único, II 7. -Verificação de idade “a cada acesso” do usuário ao conteúdo, produto ou serviço. Art. 9º, §1º 8. -Autonomia progressiva. Art. 10 9. - Mecanismos de notificações acerca de violações aos direitos de crianças e adolescentes. Art. 28, caput e art. 29, §3º 10. -Ofício às autoridades competentes. Art. 28, parágrafo único e 29, §2º.

Envio de arquivo.

- [Download attachment pdf 372 KB](#)

Resposta #17

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
163115184333880334802231	Registrado	314038638259115145093461	50%	12/12/2025 15:57

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Contribuição do Idec - Instituto de Defesa de Consumidores Os principais conceitos, termos e expressões que demandam esclarecimentos são: de acesso provável (art. 1º e ss.), medidas razoáveis (art. 6, caput e §2º), experiências adequadas à idade (art. 10), funcionamento básico (art. 17, VIII), publicidade comercial (art. 22) e fundados indícios de operação por crianças e adolescentes (art. 24, §3º e §4º). Em anexo enviamos as justificativas para cada um desses itens.

Envio de arquivo.

- [Download attachment pdf 84,7 KB](#)

Resposta #18

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
699896665234520291146784	Registrado	314038638259115145093461	50%	12/12/2025 16:04

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Prezados/as, Encontra-se em anexo o PDF com a minha contribuição. Cordialmente, Elora

Envio de arquivo.

- [Download attachment pdf 137 KB](#)

Resposta #19

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
355967093034017368076123	Registrado	314038638259115145093461	50%	12/12/2025 16:20

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Seguem no documento anexo as contribuições elaboradas pela ABRADÉE.

Envio de arquivo.

- [Download attachment pdf 157 KB](#)

Resposta #20

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
34841993199711691514667	Registrado	314038638259115145093461	50%	12/12/2025 16:22

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Em atenção à Consulta Pública aberta em 28 de novembro de 2025, o escritório de advocacia Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados (SBSA Advogados) vem apresentar recomendações e sugestões para esclarecimento de conceitos da Lei nº 15.211/2025 (“ECA Digital”). Nossa análise priorizará conceitos que impactam diretamente organizações da sociedade civil que atuam na proteção de crianças e adolescentes, bem como aqueles cuja interpretação demanda harmonização com a Lei Geral de Proteção de Dados Pessoais (LGPD), buscando inspiração em padrões internacionais consolidados.

Envio de arquivo.

- [Download attachment pdf 170 KB](#)

Resposta #21

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
549726852359762241841763	Registrado	314038638259115145093461	50%	12/12/2025 16:33

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

BRASSCOM - Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais

Conceitos que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei: De acesso provável; Suficiente probabilidade de uso e atratividade; Considerável facilidade ao acesso; Significativo grau de risco; Larga escala; O grau mais elevado de proteção da privacidade e dos dados pessoais; Disponibilização de informações claras, acessíveis e adequadas; No momento/a cada acesso do usuário; Conteúdo impróprio ou inadequado para menores; Fornecimento de sinal de idade; Vedado seu tratamento para qualquer outro propósito; Responsabilidade solidária; Mais alto nível de proteção disponível; Sistemas de recomendação personalizados; Inteligência Artificial; Técnicas de perfilamento para direcionamento de publicidade comercial. Devido a limitação de caracteres, as justificativas se encontram no documento em anexo.

Envio de arquivo.

- [Download attachment.pdf 380 KB](#)

Resposta #22

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
185301061706477548990909	Registrado	314038638259115145093461	50%	12/12/2025 16:49

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Contribuição constante no anexo.

Envio de arquivo.

- [Download attachment.pdf 407 KB](#)

Resposta #23

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
228467541299791797119113	Registrado	314038638259115145093461	50%	12/12/2025 17:13

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A STRIMA, associação civil sem fins lucrativos que representa serviços de streaming de conteúdo audiovisual que atuam no Brasil, reunindo Disney+ , Globoplay, HBO Max, Netflix, Prime Video e Bandplay, inscrita no CNPJ nº 59.131.178/0001-14, com sede na cidade de Brasília/DF na Quadra SHCS CR 516, Bloco B, Número 66 - 1º Pavimento - Parte C0463/Parte 146, vem, respeitosamente, apresentar contribuições à Tomada de Subsídios Disponibilizada pela ANPD para esclarecer conceitos do ECA Digital. Conforme publicado na Nota Técnica nº 10/2025/CON2/CGN/ANPD1 (Nota Técnica), essa r. Agência identificou de forma precisa, sobre a necessidade de “esclarecimento de conceitos, termos e expressões previsto no ECA Digital, de modo a assegurar a plena eficácia da Lei 15.211 de 17/09/2025, no ordenamento jurídico brasileiro” (p.1). Dessa forma, a STRIMA vem, respeitosamente apresentar - em anexo - sua colaboração junto a essa r. Agência, trazendo sugestões e referências na tentativa de contribuir com o processo de regulamentação do ECA Digital

Envio de arquivo.

-

Resposta #24

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
71329057217989307833616	Registrado	314038638259115145093461	50%	12/12/2025 17:16

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Contribuição conjunta entre Abecs (Associação Brasileira das Empresas de Cartões de Crédito e Serviços) e Febraban (Federação Brasileira de Bancos). Diante da extensão das contribuições das entidades, enviamos mediante o documento anexo.

Envio de arquivo.

- [Download attachment pdf 1.61 MB](#)

Resposta #25

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
663392248532550992425420	Registrado	314038638259115145093461	50%	12/12/2025 17:21

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

As contribuições da Telefônica Brasil S.A. se encontram no arquivo anexo.

Envio de arquivo.

- [Download attachment pdf 134 KB](#)

Resposta #26

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
386803612601461613542193	Registrado	314038638259115145093461	50%	12/12/2025 17:27

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Em nome do b/luz, encaminhamos anexa a nossa contribuição para o tema.

Envio de arquivo.

- [Download attachment pdf 227 KB](#)

Resposta #27

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
1100656749776973619595930	Registrado	314038638259115145093461	50%	12/12/2025 17:29

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Associação Brasileira de Mobilidade e Tecnologia (“AMOBITEC”) vem, respeitosamente, expor seu posicionamento na Tomada de Subsídios voltada ao esclarecimento de conceitos críticos do recém-sancionado Estatuto Digital da Criança e do Adolescente (ECA Digital). No documento em anexo apresentamos quadro consolidado com os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que, em nossa avaliação, demandam esclarecimentos adicionais para assegurar sua adequada compreensão e aplicação. O referido quadro demonstra que diversos conceitos centrais da Lei nº 15.211/2025 – tais como “de acesso provável”, “suficiente probabilidade de uso e atratividade”, “considerável facilidade de acesso e utilização”, “significativo grau de risco”, “grau mais elevado de proteção da privacidade e dos dados pessoais”, “informações claras, acessíveis e adequadas”, “a cada acesso”, “vedada a autodeclaração”, “conteúdo impróprio, inadequado ou proibido”, “sinal de idade”, “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”, bem como as noções de responsabilidade solidária e de sistemas de recomendação personalizados, inteligência artificial e publicidade comercial – carecem de maior densificação normativa e interpretativa para viabilizar sua aplicação coerente, proporcional e tecnicamente exequível. As respostas ao questionário da Tomada de Subsídios buscam justamente suprir essa lacuna, ao identificar, para cada expressão, parâmetros objetivos de interpretação (finalidade do serviço, natureza do conteúdo, funcionalidades, público-alvo, perfil de risco, contexto de uso, tipo de dado tratado, modelo de negócio, presença de barreiras de acesso, critérios de aferição e verificação de idade, entre outros), em alinhamento com a LGPD, o CDC, o princípio da proteção integral e as melhores práticas internacionais de regulação baseada em risco.

Envio de arquivo.

- [Download attachment pdf 418 KB](#)

Resposta #28

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
181518592875390763377612	Registrado	314038638259115145093461	50%	12/12/2025 17:42

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

O Conselho Digital apresenta suas contribuições com relação a aspectos dos arts. 1º, 7º, 9º, 13, 17, 31 e 39 do ECA Digital, incluindo-se seus parágrafos e incisos, na forma do documento anexo.

Envio de arquivo.

-

Resposta #29

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
1185706779514354854836834	Registrado	314038638259115145093461	50%	12/12/2025 17:45

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

CNseg: Acesso provável: Necessário esclarecer que os critérios do art. 1º, p. u. são cumulativos, pois a conjunção “e” entre os inc. II e III indica a intenção do legislador de estabelecer critérios cumulativos e não alternativos. Entendimento diverso importaria novas regras a qualquer provedor, ainda que seu serviço não represente risco concreto a menores. A expressão “acesso provável” visa restringir os agentes alcançados, com abordagem baseada em risco. No setor segurador, não há direcionamento de oferta, nem conteúdo atrativo a menores, como em redes sociais/mensageria. Serviços estritamente contratuais, de suporte ao cliente e gestão de apólices, sem coleta/uso de dados para perfilamento infantil, não devem ser enquadrados como de “acesso provável”. Também é preciso definir o que seria “suficiente probabilidade de uso” e “considerável facilidade de acesso” (incisos I e II), que parecem ter o mesmo sentido. Perfilamento e publicidade: Necessário esclarecer o que passa a ser vedado com o ECA Digital, detalhando as práticas vedadas na publicidade comercial para menores. O setor segurador não direciona publicidade a menores, nem utiliza seus dados pessoais para perfilamento, segmentação mercadológica ou análise emocional. Propõe-se que a regulamentação esclareça que rotinas de comunicação obrigatória (ex. avisos de vencimento, esclarecimentos contratuais, comunicações assistenciais) não se enquadram como publicidade dirigida, por terem natureza informativa e serem endereçadas ao responsável legal. Aferição de idade: Necessária definição quanto ao método e momento. No setor segurador, a identificação e verificação de idade do proponente e dos beneficiários ocorre na fase de contratação (proposta), com dados mínimos necessários. Revalidações de idade a cada acesso geraria ônus desproporcional, sem qualquer ganho. Propõe-se considerar suficiente a aferição de idade na contratação e em eventos civis relevantes, como alterações de beneficiários, resgates e portabilidades.

Envio de arquivo.

- [Download attachment pdf 150 KB](#)

Resposta #30

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
196446930832207911524989	Registrado	314038638259115145093461	50%	12/12/2025 18:04

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

[CONTRIBUIÇÃO FEITA EM NOME DO CGI.BR] O Comitê Gestor da Internet no Brasil – CGI.br vem, por meio desta Tomada de Subsídios, oferecer contribuições para o esclarecimento adicional de termos, conceitos e expressões previstas no ECA digital. As contribuições concentram-se nos termos adiante indicados que demandam maior precisão para sua adequada interpretação e aplicação: 1. Acesso provável aos produtos e serviços (Art. 1º); 2. Produtos e serviços de tecnologia da informação (Art. 2º); e 3. Modulação de obrigações de acordo com o grau de interferência sobre o conteúdo (Art. 39). As contribuições completas, com justificativas e recomendações para as definições dos termos apontados podem ser encontradas no documento enviado em anexo. O CGI.br agradece a oportunidade de contribuir para o aprimoramento e esclarecimento de termos, conceitos e expressões previstos e permanece à disposição para o diálogo e novas contribuições.

Envio de arquivo.

- [Download attachment pdf 613 KB](#)

Resposta #31

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
1133727041521107142404469	Registrado	314038638259115145093461	50%	12/12/2025 18:10

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A aplicação da Lei nº 15.211/2025 demanda o esclarecimento de conceitos centrais cuja redação aberta pode comprometer a previsibilidade regulatória, dentre os quais se destacam “acesso provável”, “perfilamento”, “análise emocional”, “uso compulsivo”, “configuração padrão mais protetiva”, “verificação confiável de idade”, “serviço com controle editorial” e “riscos psicossociais”. A precisão desses termos deve se basear em parâmetros técnicos, objetivos e mensuráveis, calibrados pelo risco de dano à criança e pela viabilidade tecnológica das soluções adotadas. Nesse sentido, a regulamentação pode considerar, de forma cumulativa ou graduada, critérios como: número de usuários ativos mensais no Brasil; percentual estimado de crianças e adolescentes na base de usuários; tipo e sensibilidade dos dados tratados; grau de automação e de inferência comportamental ou emocional; existência de funcionalidades de interação social, recomendação personalizada ou monetização; grau de intervenção do fornecedor sobre a curadoria, priorização ou moderação de conteúdos; natureza do modelo de negócio; porte econômico do fornecedor; e extensão territorial da operação. Também devem ser considerados, como fator de modulação regulatória, o nível de maturidade em proteção já implementado, incluindo a adoção de classificação indicativa, ferramentas de supervisão parental, controles de tempo de uso e de funcionalidades potencialmente aditivas, mecanismos proporcionais de verificação etária, políticas de moderação e avaliações internas de risco. A incorporação desses parâmetros permite uma aplicação proporcional e responsiva da lei, em consonância com o art. 39, assegurando proteção efetiva às crianças e adolescentes sem inviabilizar a inovação tecnológica nem restringir indevidamente a liberdade de expressão.

Envio de arquivo.

- [Download attachment.pdf 3.93 MB](#)

Resposta #32

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
921697785027544934748176	Registrado	314038638259115145093461	50%	12/12/2025 18:30

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Associação Latino-Americana de Internet (ALAI) considera que as diretrizes gerais do ECA Digital são pertinentes diante do atual contexto, marcado por rápidas transformações tecnológicas, pela ampliação do acesso digital por grupos vulneráveis e pelos riscos inerentes às fases específicas de desenvolvimento de crianças e adolescentes. Reconhecemos como legítimo o propósito de garantir a proteção integral e prevenir danos. Por essa razão, ressaltamos a necessidade de esclarecimentos técnicos e normativos que permitam a plena efetividade do objetivo protetivo da lei. Essa necessidade se evidencia diante da persistência de conceitos indefinidos, de obrigações que demandam elevado esforço interpretativo e de situações que requerem regulamentação complementar para assegurar a correta aplicação da norma, bem como segurança jurídica e proporcionalidade regulatória. Torna-se, portanto, imprescindível que a regulamentação posterior estabeleça critérios técnicos e objetivos para suprir as definições em aberto, levando em consideração as particularidades de cada setor e os diferentes níveis de risco associados a cada modelo de serviço. Esse é um requisito fundamental para garantir que a implementação do ECA Digital seja efetiva, proporcional, alinhada aos princípios da proteção integral e harmonizada com o ordenamento jurídico brasileiro e com os atos normativos da Agência Nacional de Proteção de Dados (ANPD). Ressaltamos, ainda, a importância de evitar a imposição de obrigações uniformes a serviços que apresentam características e graus de risco substancialmente distintos. Por fim, em razão da limitação de caracteres deste formulário, apresentamos em anexo as necessidades específicas de esclarecimento sobre conceitos, termos e expressões do texto legislativo, objeto desta Tomada de Subsídios. A ALAI permanece à disposição para contribuir com o avanço do escopo regulatório aplicável ao ambiente digital.

Envio de arquivo.

Resposta #33

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
428158917097516190923554	Registrado	314038638259115145093461	50%	12/12/2025 19:42

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Zetta, associação que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, inscrita no CNPJ sob o nº 37.253.906/0001-28, vem, através da manifestação anexa no campo abaixo, apresentar contribuições à Tomada de Subsídios referente aos conceitos previstos no ECA Digital, publicada por essa Autoridade Nacional de Proteção de Dados (“ANPD”), e submetida à sociedade em 28 de novembro de 2025.

Envio de arquivo.

- [Download attachment pdf 212 KB](#)

Resposta #34

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
275308236049305861224868	Registrado	314038638259115145093461	50%	12/12/2025 19:47

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Câmara Brasileira da Economia Digital, entidade multissetorial que representa diversos provedores de serviços digitais em atuação no Brasil, reconhece a relevância de que sejam esclarecidos os principais conceitos e termos previstos na Lei nº 15.211/2025 e coloca-se à disposição para colaborar com um diálogo produtivo, transparente e embasado em evidências. Trata-se de um marco regulatório recente, que inaugura um conjunto significativo de obrigações e que exigirá, de todos os atores - reguladores, empresas e sociedade civil - um processo de construção interpretativa incremental, cuidadoso e coerente com a complexidade do ecossistema digital. A regulamentação do Estatuto Digital da Criança e do Adolescente exige uma hermenêutica que reconheça que o direito, especialmente em matérias tecnológicas, opera com conceitos cuja concretização não é automática, mas depende da articulação entre estabilidade semântica, coerência sistêmica e sensibilidade ao contexto. A tradição interpretativa indica que normas jurídicas não são instruções mecânicas: elas integram um sistema de princípios que precisam ser compreendidos à luz de seu propósito normativo, evitando tanto arbitrariedades quanto rigidez excessiva. Assim, ao densificar termos como “acesso provável”, “medidas eficazes”, “funcionalidades não essenciais” ou “modelo mais protetivo”, o regulador deve buscar sentidos que sejam publicamente justificáveis, operacionais e compatíveis com a integridade do sistema jurídico, sem reduzir conceitos complexos a propriedades contingentes de tecnologias específicas ou a suposições generalistas sobre modelos de negócio. Uma abordagem baseada em princípios, que não seja excessivamente restritiva, oferece a maior flexibilidade para acomodar tecnologias em desenvolvimento e conceitos relacionados. Por isso, a camara-e.net envia em anexo contribuição na íntegra indicando conceitos específicos que carecem de esclarecimentos.

Envio de arquivo.

- [Download attachment pdf 544 KB](#)

Resposta #35

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
3734190851463390499903	Registrado	314038638259115145093461	50%	12/12/2025 20:08

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

A Meta parabeniza a ANPD pela iniciativa e agradece a oportunidade de contribuir para o diálogo com diversos atores da sociedade, visando uma regulamentação eficaz e proporcional do ECA Digital, baseada em soluções técnicas que promovem privacidade, segurança e proteção dos usuários. As principais contribuições são: 1. Sistemas de recomendação personalizados (Art. 17, §4, V): Defendemos controles parentais direcionados e proporcionais, priorizando riscos demonstráveis para menores, especialmente quanto a conteúdos inadequados à idade. 2. Funcionalidades não essenciais (Art. 17, §4, VIII): A IA é fundamental nos serviços digitais; desativá-la pode inviabilizar o serviço. Apenas recursos que possam ser desativados sem prejuízo funcional e que representem riscos a menores devem ser abrangidos. 3. Sinal de Idade (Art. 12): A verificação de idade via lojas de aplicativos e sistemas operacionais permite coleta mínima de dados e garante salvaguardas de privacidade. 4. Alcance do Art. 9: O conceito deve focar em plataformas voltadas a adultos ou que não adotem medidas efetivas para combater conteúdos inadequados, considerando apenas serviços classificados como "18+" pelo Ministério da Justiça. 5. Escopo do Art. 1: Solicitamos esclarecimento sobre "probabilidade suficiente de uso e atratividade" e "considerável facilidade de acesso e uso". 6. Uso de dados pessoais para verificação de idade (Art. 13): Defendemos que dados coletados para verificação de idade sejam usados para fins compatíveis (ex.: prevenção de fraudes, experiências apropriadas à idade), sempre com salvaguardas robustas e em conformidade com a LGPD. 7. Publicidade Comercial (Art. 22): O Art. 22 não proíbe publicidade comercial nem perfilamento em geral, apenas restringe o direcionamento de anúncios a crianças e adolescentes.

Envio de arquivo.

- [Download attachment pdf 3.21 MB](#)

Resposta #36

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
181739911143469152821068	Registrado	314038638259115145093461	50%	12/12/2025 20:32

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

O Instituto Alana encaminhou documento com contribuições, devidamente anexado, ao e-mail da Coordenação de Normatização.

Envio de arquivo.

-

Resposta #37

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
827280434293406132253137	Registrado	314038638259115145093461	50%	12/12/2025 20:56

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Contribuição em anexo.

Envio de arquivo.

- [Download attachment pdf 114 KB](#)

Resposta #38

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
406678647889654776758494	Registrado	314038638259115145093461	50%	12/12/2025 21:31

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Vedação de acesso a conteúdo impróprio: É preciso esclarecer o que se entende pelo conceito "medidas eficazes" para o impedimento de acesso de crianças e adolescentes ao conteúdo impróprio, inadequado ou proibido para menores de 18 anos, nos termos do art. 9º, haja vista sua amplitude e genericidade. Identificação inequívoca de conteúdos: Delimite-se o conceito de "identificação técnica específica do conteúdo", previsto no art. 29, §2º, bem como os requisitos que permitirão que se conclua, com segurança, pela possibilidade técnica de identificação de conteúdo específico na internet. Garantia de vinculação de conta ao responsável legal: Se explique qual seria o conceito de "garantia", para que o setor privado possa se preparar de forma efetiva para o cumprimento da lei. Na definição, deve-se levar em consideração se a vinculação será obrigatória quando os responsáveis legais não tiverem acesso, por vontade própria, às plataformas, bem como quando não for tecnicamente viável, e, ainda, o contexto sociocultural brasileiro, para que essas disposições não excluam o acesso dos usuários menores. Publicidade: Se esclareça se as recomendações algorítmicas (como conteúdo recomendado com base nas preferências do usuário) não publicitárias entram na proibição da utilização de perfilamento para direcionamento de publicidade comercial, prevista no art. 22, já que isso pode alterar significativamente a experiência de usuários em plataformas digitais. Esclarecer, também, como será tratada a base de dados crianças e adolescentes que já está cadastrada nas plataformas. Sanções: Necessário esclarecer como será a compatibilização e estrutura de sanções para se evitar sanção em duplicidade Vacatio legis: Se esclareça se a ANPD emitirá regulamentação ou orientação sobre a lei com previsão de período maior de adaptação ou transição que aquele previsto no art. 41-A, em especial para micro e pequenas empresas, que têm tratamento diferenciado pelo ordenamento brasileiro.

Envio de arquivo.

-

Resposta #39

Identificador de Usuário	Status do usuário	Hash IP	Conclusão	Respondido em
866176563633687499294004	Registrado	314038638259115145093461	50%	12/12/2025 23:25

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Em nome da Associação de Software de Entretenimento (ESA)

Envio de arquivo.

-

ANDP

Tomada de Subsídios conceitos previstos no ECA Digital

DEZEMBRO / 2025



Sobre o Conselho Digital

O Conselho Digital é uma entidade brasileira, sem fins lucrativos ou afiliações políticas, que coordena, estuda e representa o ecossistema dos aplicativos de internet e toda a diversidade dos seus modelos de negócios.

Nossa organização acredita que a tecnologia, quando bem construída e utilizada, é uma porta para o futuro. Ela nos mantém conectados, potencializa habilidades, desenvolve novas oportunidades e pode mudar a vida das pessoas para melhor.

Partindo dessa premissa, atuamos através de estudos, eventos e atividades de advocacy em favor de políticas públicas e setoriais que fortaleçam uma internet livre, segura e responsável no Brasil e no mundo.

Defendemos políticas que respeitem a neutralidade tecnológica, a inovação e a diversidade de modelos de negócios; e que tenham como consequência:

- Usuários conscientes e com poder de escolha;
- Uma sociedade plural e próspera;
- Ambientes de negócio juridicamente seguros;
- Mercados abertos e dinâmicos; e
- Empresas responsáveis e lucrativas.

Por fim, assumimos o compromisso de construir um ambiente harmonioso e produtivo entre nossos associados, assim como uma relação transparente e colaborativa com a sociedade e governo.



Diretor-Executivo





Tomada de Subsídios

Conceitos

ECA Digital

DESTINATÁRIO: ANPD

Data: Dezembro de 2025

O Conselho Digital cumprimenta a iniciativa da Tomada de Subsídios da ANPD e, através de sua contribuição, traz considerações sobre conceitos e parâmetros que podem ser tratados no âmbito da regulamentação do ECA Digital, para maior efetividade da Lei, mitigação de insegurança jurídica e o risco de obrigações excessivas ou desproporcionais, que podem aumentar o risco na experiência online dos usuários ao invés de proteger, e reduzir a funcionalidade e utilidade dos sistemas dos provedores.

Sugere-se como importante o reconhecimento de que o risco está associado a um conjunto de configurações, salvaguardas e limites aplicados por faixa etária, e não à mera existência de funcionalidades. Em linha com o ECA Digital e com os princípios da LGPD, recomenda-se que a regulamentação considere as medidas de bem-estar digital e de design apropriados por idade disponíveis pelos provedores, considerando as melhores práticas, modelos de negócios e tecnologias distintas.

Com relação à tomada de subsídios, consideram-se merecedores de atenção os termos relacionados aos:

- sistemas de recomendação;
- sistemas de geolocalização;
- serviços impróprios/inadequados;
- funcionalidades essenciais de IA;
- probabilidade de uso/atratividade de serviços e produtos;
- finalidade exclusiva de tratamento dos dados de age assurance.

Ainda, propõem-se alguns parâmetros em nossas sugestões:

- Finalidade do emprego de funcionalidades: distinções claras entre segurança Vs. engajamento ou aspecto comercial;
- critérios objetivos de classificação dos conceitos;
- uso de dados baseado no melhor interesse da criança;

- Exemplos de funcionalidades essenciais para adoção pelos operadores, segundo o juízo de proporcionalidade.

A seguir, melhor detalhamos:

1. “suficiente probabilidade de uso e atratividade” e “considerável facilidade ao acesso e utilização”

“Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.

Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações:

I - **suficiente probabilidade de uso e atratividade** do produto ou serviço de tecnologia da informação por crianças e adolescentes;

II - **considerável facilidade ao acesso e utilização** do produto ou serviço de tecnologia da informação por crianças e adolescentes;

(...)”

Problema: não há compreensão sobre a forma em que se dará o enquadramento dos serviços e produtos no meio digital, para aplicação da Lei.

O conceito amplo de **“suficiente probabilidade de uso e atratividade”** e **“considerável facilidade ao acesso e utilização”** pode ser usado em função das **suas características gerais**, como: público-alvo, marketing, finalidade de uso; ou em função das **camadas de proteção** disponibilizadas, avaliadas conforme seu design, capacidade de moderação e restrição etária aplicadas por cada plataforma.

Sugestão: sem critérios objetivos, qualquer plataforma pode ser interpretada como “facilmente acessível”. A sugestão é que este conceito leve em consideração a finalidade e o público-alvo do serviço/ produto ou da parcela do serviço que está sendo direcionada às crianças, em conjunto com as ferramentas disponíveis por padrão e/ou controle parental para restrição do acesso do produto ou serviço por menores.

Os conceitos devem centrar-se na obtenção de resultados de proteção, em vez de prescrever abordagens técnicas específicas, permitindo que os serviços implementem soluções que se alinhem com os seus casos de utilização reais e perfis de risco.

Portanto, seria importante ter claro que obrigações decorrentes da Lei não incidam sobre serviços ou produtos que não ofereçam conteúdo inadequado para menores de idade, ou que já considerem as salvaguardas adotadas para impedir o contato não solicitado de indivíduos desconhecidos com menores, os conteúdos sujeitos à classificação indicativa brasileira ou autoclassificação baseada em sistema internacional, ou cujos termos e condições já proíbam conteúdo impróprio e a plataforma ofereça medidas reativas adequadas e proporcionais, em face do conteúdo nocivo reportado ou identificado.

2. “o grau mais elevado de proteção da privacidade e dos dados pessoais” e “disponibilização de informações claras, acessíveis e adequadas”

“Art. 7º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo **mais protetivo disponível em relação à privacidade e à proteção de dados pessoais**, considerados a autonomia e o desenvolvimento progressivo do indivíduo e justificado o melhor interesse da criança e do adolescente.

§ 1º O produto ou serviço referido no caput deste artigo deverá, por padrão, operar com o **grau mais elevado de proteção da privacidade e dos dados pessoais**, observado que será obrigatória a **disponibilização de informações claras, acessíveis e adequadas** para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à eventual adoção de configurações menos protetivas.

O Artigo 7 e outros artigos semelhantes exigem que as empresas operem com “o grau mais elevado de proteção da privacidade e dos dados pessoais”. No entanto, o que constitui “o grau mais elevado de proteção da privacidade e dos dados pessoais” não está definido, deixando as empresas com muita incerteza sobre como operar seus serviços e produtos. Recomendamos que as orientações regulatórias definam explicitamente o que constitui “o grau mais elevado de proteção da privacidade e dos dados pessoais”, indicando principalmente os controles em mente (ou seja, publicidade, marketing, compartilhamento de dados com terceiros) e como esses controles devem ser definidos por padrão para menores de idade. Recomendamos, ainda, que seja considerada flexibilidade aos provedores de serviços para determinar o grau mais elevado de proteção, considerados também o oferecimento de proteções por padrão e ferramentas de controle parental, que conjuntamente entregam uma experiência adequada à idade.

O Artigo 7 e outros artigos semelhantes exigem que as empresas forneçam informações claras, acessíveis e adequadas para que os menores e seus responsáveis possam fazer escolhas informadas. No entanto, o que constitui informação “clara, acessível e adequada” não está definido, deixando as empresas com muita incerteza sobre como calibrar adequadamente suas divulgações. Recomendamos uma orientação regulatória que estabeleça que ter uma seção sobre menores na política de privacidade da empresa é suficiente para constituir informação “clara, acessível e adequada”, conforme exigido pelo Artigo 7.

O Artigo 7 também exige que os provedores de produtos ou serviços destinados a crianças e adolescentes, ou com grande probabilidade de serem acessados por eles, adotem configurações padrão que sejam proporcionalmente protetivas em termos de privacidade e proteção de dados, considerando a autonomia, o desenvolvimento progressivo e o melhor interesse dos usuários. Destacamos que esse requisito não deve impedir a prestação de serviços essenciais, especialmente quando as funcionalidades centrais dependem do processamento de dados pessoais. Sem essa salvaguarda, a lei poderia comprometer o próprio propósito desses serviços.

Considera-se que alguns serviços devem processar dados para personalização, a fim de oferecer uma experiência no melhor interesse do menor, como, por exemplo, para suportar experiências mais apropriadas para a faixa etária. As configurações padrão não devem ser interpretadas de forma a restringir esses serviços. Além disso, essa clarificação estaria em conformidade com o Artigo 28.2 do Regulamento Europeu de Serviços Digitais.

3. Produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 anos

“Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que **disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes** para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos.

(...) § 2º Para os fins desta Lei, consideram-se impróprios ou inadequados para crianças e adolescentes os **produtos, serviços ou conteúdos de tecnologia da informação que contenham material pornográfico, ou quaisquer outros vedados pela legislação vigente**”.

Problema: Entendemos que falta precisão sobre a definição do escopo do art. 9º. O caput do artigo referido faz menção às **“medidas eficazes para impedir o acesso”**, no entanto, a redação do parágrafo 2º não distingue os provedores, cujos serviços sejam exclusivos para adultos, a exemplo de plataformas de relacionamento adulto e apostas, que devem dispor de “adult-only” por design; dos provedores que contenham conteúdo diversificado, dotados de aparato substancial de tecnologia para evitar que o acesso ao conteúdo ocorra por usuário de idade incompatível com a natureza do conteúdo.

O termo amplo gera insegurança jurídica para o ecossistema digital e pode gerar obrigações desproporcionais para os provedores que cumprem a legislação oferecendo camadas de proteção à experiência inadequada à idade do usuário. Sem limites de definição claros, esses descritores subjetivos poderiam abranger praticamente qualquer tema adulto na literatura, incluindo obras com significado educacional, histórico ou cultural significativo.

É importante destacar que nem todos os serviços são iguais. Assim como ocorre no Reino Unido, a orientação da Ofcom sobre mecanismos altamente eficazes de verificação etária no âmbito do Online Safety Act (“HEAA Guidance”) estabelece critérios específicos que os processos de verificação etária devem cumprir para serem considerados altamente eficazes — e tais critérios variam conforme o tipo de serviço (serviços regulados de interação entre usuários são diferentes de serviços de busca, que por sua vez são diferentes de lojas de aplicativos). O guia apresenta exemplos de métodos de verificação etária que são, ou não são, capazes de alcançar um alto nível de eficácia (ver seção 4, página 18). Importante notar que esses requisitos se aplicam exclusivamente a serviços regulados de interação entre usuários e não se estendem a serviços de busca ou lojas de aplicativos.

Sugestão: Para evitar obrigações excessivas a todos os agentes de forma indiscriminada, mesmo quando é utilizada tecnologia para o cumprimento da Lei, sugere-se que a regulamentação, ao tratar dos conceitos de aplicação das normas, considere a importância da melhor definição do escopo, que deve focar nos serviços cujas ofertas predominantes são para adultos e que **não ofereçam** ferramentas por padrão e/ou controle parental para restrição do acesso do produto ou serviço por menores.

Além disso, no que diz respeito ao Artigo 9 §2, a orientação deve ser precisa na definição de conteúdo “pornográfico” para distinguir entre material explícito destinado principalmente à excitação sexual e obras literárias que incluem temas sexuais adultos como parte de contextos jornalísticos, narrativos, educacionais, históricos ou culturais mais amplos. Sem esse esclarecimento, existe o risco de que obras literárias legítimas e valiosas possam ser indevidamente classificadas como materiais pornográficos.

4. Vedação ao uso de dados de verificação de idade para qualquer outra finalidade

“Art. 13. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados **unicamente** para essa finalidade, **vedado seu tratamento para qualquer outro propósito**”.

Problema: A lógica de proteção da privacidade do menor ao prever a vedação do tratamento dos dados de verificação etária (age assurance) para outras finalidades pode, contudo, prejudicar a própria finalidade da Lei, de modo que a regulamentação deve preservar o interesse do legislador e evitar interpretações literais que venham a conflitar com outros interesses intrínsecos ao melhor interesse do menor, como:

- prevenção de fraude;
- auditorias internas;
- segurança;
- fornecimento de experiências adequadas à idade.

Sugestão: O tratamento de dados coletados para verificação de idade de crianças e adolescentes deve considerar o seu melhor interesse. A segurança do sistema de verificação em múltiplas camadas ocorre de maneira contínua e se baseia no oferecimento de “experiências adequadas à idade”, o que é justamente proporcionado com os dados coletados para a verificação de idade.

5. validação de controle parental

Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão:

(...)

§ 1º A autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital **estabelecerá, por regulamento, diretrizes e padrões mínimos sobre mecanismos de supervisão parental** a serem observados pelos fornecedores.

(...)

§ 4º: As **configurações-padrão das ferramentas de supervisão parental** deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo:

Problema: Tratando-se do art. 17, faz-se necessária maior clareza, por parte do regulador, sobre quais mecanismos deverão ser adotados para a validação do controle parental. A vinculação a uma conta 18+ já seria suficiente? Haverá alguma base pública de dados disponível via API que permita a verificação das informações acerca do responsável legal do menor?

Sugestão: Ao se considerar a viabilidade de uma base de dados pública com informações sobre responsáveis, sugerimos a adoção de um período de testes para a validação dessa base e sua integração com os sistemas de controle parental de cada produto ou serviço.

Além disso, considera-se bem-vinda a orientação do regulador quanto aos padrões mínimos para a execução de relatórios de impacto, monitoramento e avaliação da proteção de dados pessoais, listados no art. 16, parágrafo único, inciso II.

6. Controle sobre sistemas de recomendação personalizados

Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão:

(...)

§ 4º: As configurações-padrão das ferramentas de supervisão parental deverão adotar **o mais alto nível de proteção disponível, assegurados, no mínimo:**

(...)

V – controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação;

Problema: O uso do poder normativo e coercitivo pela ANPD, caso venha a se lastrear em interpretação literal da Lei, incorre no risco de desconsiderar o melhor interesse da criança e do adolescente na experiência digital. Nota-se que a Lei, ao dispor sobre a possibilidade de desativação do controle de sistemas de recomendação personalizadas, não diferencia a situação finalística do funcionamento do sistema para segurança, prevenção a fraudes, e à adequada experiência digital, segundo conteúdos pré-delimitados por seus pais e responsáveis, com o uso do mesmo para finalidades comerciais ou de engajamento.

Ao criar uma obrigação absoluta sobre os sistemas de recomendação, criando a possibilidade do controle total ou da desativação completa dos sistemas essenciais para manter crianças em ambientes adequados à idade, a regulamentação estaria exigindo das plataformas que funcionalidades essenciais do sistema possam ser esvaziadas, prejudicando a efetividade da proteção, usabilidade dos sistemas e da aderência aos parâmetros de conteúdo configurados pelos supervisores através das ferramentas de controle parental.

Portanto, ao invés de acautelar os interesses da família e dos menores, tal previsão passaria a expor o usuário a conteúdos aleatórios, inadequados ou irrelevantes aos seus interesses.

Sugestão: O “controle sobre sistemas de recomendação personalizada” deve ser limitada à proteção de menores contra a exposição a experiências e conteúdos indesejados.

7. “Restrição ao compartilhamento da geolocalização”

Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão:

(...)

§ 4º As configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo:

(...)

VI – restrição ao compartilhamento da geolocalização e fornecimento de aviso prévio e claro sobre seu rastreamento;

Problema: A possibilidade de restringir compartilhamento da geolocalização de maneira absoluta inviabiliza modelos legítimos que baseiam o compartilhamento de tais informações com supervisores de menores de idade, como medida de segurança. A finalidade da ferramenta deve ser levada em consideração, porque sua previsão ampla passaria a inviabilizar usos legítimos do georreferenciamento como medida de segurança, como no caso do “Uber Teens”. Tais recursos, dotados de salvaguardas, não se confundem, por exemplo, com rastreamento de dados sensíveis para uma finalidade comercial, quando abusiva.

Sugestão: As configurações-padrão devem sempre considerar o melhor interesse do menor e a autonomia dos pais e responsáveis de tutelar pelos interesses e pela adequação dos serviços dispostos pelo provedor, de acordo com a autonomia individual de cada um e o aviso prévio sobre a finalidade da ferramenta.

O mais alto nível de proteção disponível não deve ser interpretado como as configurações mais restritivas, mas sim deve considerar as funcionalidades essenciais intrínsecas ao produto e ao serviço relacionadas às funções de segurança e de verificação etária, além dos riscos apresentados pelo serviço e da autonomia dos responsáveis sobre o que é ou não considerado adequado para o seu filho ou tutorado, diante de informações necessárias (transparência qualificada) sobre o funcionamento dos sistemas.

8. “Inteligência Artificial” e “Funcionalidades não essenciais ao funcionamento básico dos sistemas”

Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão:

(...)

§ 4º As configurações-padrão das ferramentas de supervisão parental **deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo:**

(...)

VIII – revisão regular das **ferramentas de inteligência artificial**, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a **possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas;**

Problema: Não há definição sobre o conceito de “essencial” para determinar quais funções são ou não essenciais para serem desabilitadas, o que traz o risco de obrigar a inserção de meios de desativação de componentes importantes para proteção ou adequação etária e de funcionamento de sistemas de IA integrados ao produto. Estes mecanismos são necessários para a segurança, classificação e recomendação de conteúdos de acordo com a concepção de safety by design.

Os sistemas de inteligência artificial são parte integral do desenho de produto ou serviço, assim como de todas as ferramentas que operam para oferecer experiências apropriadas à idade, segurança, integridade, etc, que são essenciais para o cumprimento da Lei. Temos preocupações quanto à inclusão de requisitos específicos de inteligência artificial nesta lei, pois essa abordagem interpreta erroneamente, tanto a natureza onipresente da tecnologia de IA, quanto suas diversas aplicações na segurança online. A IA não é inerentemente prejudicial; é uma tecnologia usada para muitos fins legítimos, incluindo a moderação eficaz de conteúdo em grande escala. As ferramentas de IA podem ser usadas para identificar e remover conteúdo prejudicial de forma rápida e consistente em grandes volumes de interações de usuários. Muitos recursos de segurança que protegem as crianças online, desde a filtragem de conteúdo até a detecção de possíveis comportamentos predatórios, dependem da tecnologia de IA. Além disso, adicionar requisitos específicos de IA não melhora significativamente os objetivos de proteção da lei. Conteúdos inadequados para crianças se enquadram no âmbito das medidas de segurança exigidas, independentemente de serem gerados por IA ou criados por humanos. O método de criação de conteúdo não altera a forma como um serviço deve ser moderado e regulamentado. Além disso, exigir uma revisão externa dos sistemas de IA pode comprometer a segurança, expondo informações confidenciais sobre os sistemas de moderação de conteúdo a terceiros.

Sugestão: As “funcionalidades não essenciais ao funcionamento básico dos sistemas” devem ser interpretadas como todas aquelas que o provedor, que dispõe de ferramentas por padrão e/ou controle parental para restrição do acesso do produto ou serviço por menores, disponibilize para desabilitação. Este juízo deve ser exercido de forma proporcional a uma relação exemplificativa de “funcionalidades essenciais” consideradas pelo regulador.

Com isso, cumpre-se a Lei e, ao mesmo tempo, garante-se a autonomia do provedor do serviço e produto a dispor de maneira apropriada da tecnologia disponível ao seu modelo, sem criar riscos, engessamentos incompatíveis ou inviabilizar mudanças de posicionamento sobre as melhores práticas no ambiente digital, considerando as constantes transformações no uso da tecnologia e na conclusão dos especialistas.

Sugere-se que as orientações regulatórias se concentrem no resultado e não no mecanismo em si, regulamentando a tecnologia de IA como um todo. Importante reconhecer que as ferramentas de IA podem aumentar a segurança online quando implementadas adequadamente e que os serviços devem ter flexibilidade para desenvolver e revisar sistemas de IA internamente, desde que incorporem princípios adequados de segurança desde a concepção. Essa abordagem atenderia melhor aos objetivos de proteção da lei, evitando consequências indesejadas para aplicações benéficas de IA que ajudam a manter as crianças seguras online.

9. Acesso gratuito a informações por pesquisadores

Art. 31. Os provedores de aplicações de internet direcionadas a crianças e a adolescentes ou de acesso provável por eles que possuam mais de 1.000.000 (um milhão) de usuários nessa faixa etária registrados, com conexão de internet no território nacional, deverão elaborar relatórios semestrais, em língua portuguesa, a serem publicados no sítio eletrônico do provedor, que contenham:

Parágrafo único. Os provedores de aplicações de internet deverão viabilizar, de forma gratuita, o acesso a dados necessários à realização de pesquisas sobre os impactos de seus produtos e serviços nos direitos de crianças e de adolescentes e no melhor interesse deles, por parte de instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas, conforme critérios e requisitos definidos em regulamento, vedada a utilização desses dados para quaisquer finalidades comerciais e assegurado o cumprimento dos princípios da finalidade, da necessidade, da segurança e da confidencialidade das informações.

O artigo 31, parágrafo único, do ECA Digital estabelece que os provedores de aplicações de internet devem conceder a pesquisadores acesso aos dados necessários para a realização de pesquisas sobre temas relacionados à proteção de crianças e adolescentes no ambiente digital. No entanto, a norma não especifica (i) quais dados podem ser acessados; (ii) os critérios para a concessão desse acesso; ou (iii) quem se qualifica como pesquisador elegível para fins dessa obrigação.

A ausência de parâmetros claros expõe os provedores a solicitações excessivas ou potencialmente inadequadas, inclusive por indivíduos possivelmente não qualificados. Considerando que o próprio texto legal remete à regulamentação para a definição desses critérios e requisitos, é essencial que tal regulamentação estabeleça (i) os procedimentos para apresentação e avaliação dos pedidos de acesso; (ii) as qualificações exigidas dos pesquisadores; (iii) o escopo e as limitações dos dados que podem ser disponibilizados; e (iv) as salvaguardas necessárias para proteger dados pessoais, informações confidenciais e segredos comerciais.

Sugestão: Para enfrentar essas preocupações, recomendamos tomar como referência o regime europeu previsto no artigo 40 do DSA, que oferece uma abordagem equilibrada para o acesso de pesquisadores, assegurando proporcionalidade regulatória e a proteção da segurança da informação, dos dados pessoais e dos segredos comerciais. Nesse sentido, propomos que os seguintes parâmetros sejam aplicados ao Digital ECA, adaptados do modelo do DSA ao contexto jurídico brasileiro:

- O acesso aos dados deverá ser condicionado à solicitação fundamentada de um Pesquisador Autorizado ao respectivo provedor de aplicação e à ANPD, indicando o tipo de pesquisa, a justificativa para as informações solicitadas em relação ao objeto da pesquisa e os benefícios que dela advirão para a sociedade civil. Somente poderão ser requisitadas as informações estritamente necessárias ao tema da pesquisa.

- O provedor de aplicação deverá responder em prazo razoável e apresentar justificativa fundamentada. A resposta poderá incluir a concessão de acesso aos dados solicitados ou a submissão do caso à ANPD para revisão, caso o provedor entenda que: (a) não possui acesso aos dados requisitados; (b) a concessão do acesso possa representar risco significativo à segurança do serviço ou à proteção de informações confidenciais ou segredos comerciais; ou (c) o Pesquisador Autorizado não esteja devidamente qualificado, as informações solicitadas não guardem relação com o propósito da pesquisa, ou o pedido seja insuficientemente fundamentado.
- A análise de qualquer pedido de revisão caberá à ANPD, que deverá avaliar a solicitação do Pesquisador Autorizado e os argumentos apresentados pelo provedor de aplicação. A ANPD deverá emitir decisão em até 15 (quinze) dias, notificar as partes envolvidas e, se necessário, estabelecer novo prazo para manifestações adicionais.

10. Modulação de Obrigações

Art. 39. As obrigações previstas nos arts. 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 desta Lei aplicar-se-ão conforme as características e as funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o grau de interferência do fornecedor do produto ou serviço sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor.

O artigo 39 do ECA Digital estabelece que as obrigações previstas nos artigos 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 (conjuntamente, as “Obrigações Moduláveis”) deverão ser aplicadas conforme as características e funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o grau de interferência do provedor do produto ou serviço sobre o conteúdo disponibilizado, o número de usuários e o porte do provedor.

Embora o artigo 39 do ECA Digital reconheça a necessidade de calibrar a aplicabilidade de determinadas obrigações às especificidades dos diversos tipos de produtos ou serviços de tecnologia da informação, é importante prever expressamente que as limitações técnicas desses produtos e serviços devam ser consideradas como parâmetro para avaliar a pertinência de cada obrigação.

Por exemplo, a obrigação de remoção de conteúdo mediante notificação (notice and take down), prevista no artigo 29 do ECA Digital, apresenta desafios conceituais e técnicos significativos para diferentes tipos de serviços online que não são redes sociais com conteúdo gerado por usuários, incluindo, sem limitação, provedores de IA generativa. Nesses sistemas:

- (i) o conteúdo é dinâmico, pois cada prompt pode gerar infinitas variações;
- (ii) não há URL fixa ou hash associado às saídas;
- (iii) o conteúdo identificável existe apenas no momento da geração;
- (iv) as saídas dependem da forma como o usuário formula sua solicitação, tornando-as imprevisíveis e infinitamente variáveis; e

(v) a singularidade das saídas pode resultar em um alto volume de reclamações distintas, cada uma exigindo tratamento individualizado.

Além disso, embora os critérios para avaliação do grau de intervenção para a aplicação proporcional das Obrigações Moduláveis dependam de regulamentação específica (nos termos do §3º do artigo 39), é pertinente que a definição de “grau de interferência” estabeleça que o Conteúdo Gerado pelo Usuário — ainda que criado por meio de um produto ou serviço de tecnologia da informação — não pode ser imputado ao provedor desses produtos ou serviços.

Sugestão: Diante do exposto, é importante a inclusão das seguintes definições:

“Grau de interferência: a capacidade do fornecedor de influenciar, moderar ou intervir na disponibilidade, circulação ou alcance de conteúdo acessível a crianças e adolescentes, exceto quanto ao conteúdo gerado pelos próprios usuários em suas interações com o produto ou serviço de tecnologia da informação, inclusive no contexto de IA generativa, hipótese em que inexistente interferência do provedor.”

“Características e funcionalidades: propriedades técnicas, consistentes em capacidades e limitações operacionais e tecnológicas inerentes ao produto ou serviço de tecnologia da informação, que condicionam a aplicabilidade, a forma e a extensão dos requisitos previstos nesta Lei.”

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Tomada de Subsídios – Conceitos Previstos no ECA Digital

ASSOCIAÇÃO DE SOFTWARE DE ENTRETENIMENTO (ESA)

12 de dezembro de 2025

Prezados(as),

A Associação de Software de Entretenimento (“*Entertainment Software Association*”, ESA) apresenta estas contribuições no âmbito da consulta pública da ANPD relativa à Lei nº 15.211/2025 (“ECA Digital”). Os membros da ESA são os inovadores, criadores, publicadores e líderes empresariais que transformam o entretenimento e a forma como as pessoas jogam jogos eletrônicos em consoles, dispositivos portáteis e computadores pessoais. A indústria de jogos eletrônicos está comprometida em ajudar crianças e adolescentes brasileiros a terem experiências online seguras e positivas e segue investindo no desenvolvimento de soluções que promovam a privacidade, a segurança e o envolvimento adequado dos pais.

A ESA agradece a oportunidade de participar desta consulta pública e poder esclarecer aspectos que o setor considera relevantes e até mesmo cruciais para a implementação do ECA Digital. Permanecemos à disposição da ANPD para responder a perguntas e consultas adicionais. Como comentário geral, a indústria de jogos eletrônicos entende que o processo de implementação do ECA Digital é importante demais para que seja feito de forma açodada.

A indústria de jogos eletrônicos insta o governo a conceder tempo adequado: (a) para que os órgãos estabeleçam canais apropriados de especialização e autoridade; (b) para que essas autoridades editem regulamentos bem fundamentados; e (c) para que as empresas desenvolvam e testem soluções tecnológicas que sejam adequadas para cumprir as novas obrigações legais. Consideramos que essas etapas devam ocorrer de forma sequencial, a fim de evitar ineficiências e conflitos regulatórios que possam gerar resultados não intencionais. Ademais, as empresas necessitarão de segurança regulatória para garantir que as novas soluções atendam aos níveis adequados de funcionalidade, precisão e minimização de dados antes do prazo de conformidade do ECA Digital. Cada uma dessas características é essencial para que as empresas atinjam os objetivos da nova lei. No entanto, ainda que se presuma que possa haver clareza regulatória antes do fim deste ano, tais características não poderão ser alcançadas nos quatro meses restantes até o prazo atualmente previsto para a entrada em vigor da lei.

A ESA solicita respeitosamente que o prazo para cumprimento das disposições do ECA Digital que exigirão mudanças nas práticas empresariais seja estendido para, no mínimo, 12 a 18 meses, com a previsão de períodos adicionais de transição. Isso permitiria uma conformidade tranquila e daria tempo para que os consumidores se adaptem às novas práticas. Os membros da ESA são incentivados a cumprir integral e adequadamente as obrigações, em conformidade com as orientações governamentais esperadas, após um período robusto de desenvolvimento e testes. Como referência, observa-se que o Online Safety Act do Reino Unido foi aprovado em 26 de outubro de 2023, e as medidas de garantia etária entraram em vigor apenas em 25 de julho de 2025. Isso significa que os requisitos de garantia etária foram implementados aproximadamente

1 ano e 9 meses após a promulgação. Mesmo após quase dois anos de preparação, ainda assim ocorreram perturbações significativas no mercado à medida que a indústria e os consumidores se adaptavam às novas exigências.

Implementação faseada

Para serviços legalmente obrigados, nos termos do ECA Digital, a prover soluções tecnológicas recém-desenvolvidas, como controles parentais, verificação de idade e supervisão parental de contas de crianças e adolescentes, a ESA apoia fortemente um processo de implementação faseado e pragmático, que minimize fricções para o usuário e maximize a adoção. Isso permitiria que os usuários compreendam o valor das novas ferramentas e se ajustem a como essas ferramentas podem impactar sua experiência em um serviço. No Reino Unido, a Ofcom reconheceu a necessidade de conceder aos provedores tempo suficiente para garantir que os deveres de segurança fossem implementados de forma eficaz. A Ofcom visa permitir até seis meses para conformidade antes de iniciar ações de fiscalização contra provedores, mesmo após a entrada em vigor das disposições relevantes, após longos períodos de implementação (conforme mencionado acima) - exceto nos casos de violações mais graves. Quando há complexidades técnicas, a Ofcom tem reconhecido que os provedores podem precisar de tempo adicional. *Ver Ofcom, Vol. 3: Transparency, trust and other guidance, [Protecting people from illegal harms online](#)*. Essa abordagem é característica de reguladores que buscam promover conformidade e resultados positivos para crianças e adolescentes. Em contraste, um sistema que expõe categoricamente as empresas a ações de fiscalização na data de vigência, após um período de implementação intencionalmente abreviado, tende a desestimular agentes bem-intencionados a participar do mercado ou a inovar em soluções coordenadas.

Acesso e uso inadequados

Recomendamos que a definição de “acesso inadequado” do Artigo 5º, § 1º, seja alinhada à definição de “acesso impróprio ou inadequado” prevista no Artigo 9º, § 2º, como aqueles explicitamente proibidos pela legislação vigente. É igualmente essencial que o ECA Digital respeite os critérios utilizados para informar cuidadores sobre conteúdos inadequados para menores, conforme o sistema de classificação indicativa de jogos eletrônicos regulado pela autoridade brasileira de classificação (ClassInd), preservando o caráter informativo, educativo e não compulsório das classificações etárias da ClassInd.

Padrões de design

O Artigo 8º, IV, do ECA Digital trata de escolhas de design que afetam o uso compulsivo.

A ESA recomenda que o governo estabeleça critérios objetivos para determinar o que constituiria “uso compulsivo” ou “configurações que evitem o uso compulsivo”. Sem parâmetros técnicos claros, há risco de interpretações divergentes, insegurança jurídica e dificuldade de aplicação uniforme pelo setor privado. Em particular, esses critérios devem ser respaldados por métricas claras, objetivas e baseadas em dados que demonstrem aumentos mensuráveis na duração ou frequência das sessões atribuíveis a uma funcionalidade específica, que não possam

ser mitigados por fatores atenuantes já oferecidos pelos provedores de serviços (controles parentais, configurações padrão, transparência sobre uso).

Verificação de idade

O governo irá esclarecer quais conteúdos, produtos e serviços estão abrangidos pelas obrigações do Artigo 9º, à luz das limitações previstas no § 2º do mesmo artigo? A redação da lei sugere que essa disposição se aplica apenas à pornografia e a produtos e serviços legalmente proibidos, como tabaco, drogas e serviços de apostas.

A ESA incorpora aqui, por referência, os comentários apresentados ao governo em 14 de novembro de 2025 na consulta “Aferição de Idade na Internet Brasileira”.

Mecanismos de aferição de idade

Os Artigos 10 e 11 tratam de mecanismos para oferecer experiências adequadas à idade. O governo deve reconhecer o papel relevante de sistemas voltados à tomada de decisão familiar, como classificações etárias e controles parentais voluntários — amplamente utilizados no contexto dos jogos eletrônicos — como mecanismos compatíveis para fornecer experiências apropriadas à idade, nos termos do Capítulo IV.

Verificação de idade no nível do dispositivo/aplicativo

Os Artigos 12 a 15 aplicam-se a lojas de aplicativos e sistemas operacionais. O governo promoverá flexibilidade tecnológica e segurança jurídica, de modo que uma variedade de ferramentas e sistemas, voltados tanto à segurança online quanto às preferências dos consumidores, possa cumprir as obrigações legais relativas a sinais etários e à prevenção do acesso a conteúdos inadequados?

No caso de um aplicativo disponibilizado no Brasil por meio de lojas de aplicativos e que tenha acesso a sinais etários provenientes de múltiplas fontes, solicita-se o esclarecimento de que o provedor do aplicativo poderá determinar de qual ou quais partes aceitará os sinais etários: do sistema operacional do dispositivo, da loja de aplicativos ou de suas próprias fontes ou contas.

Os provedores de aplicativos terão flexibilidade para determinar a melhor forma de resolver sinais etários conflitantes, ou o governo pretende emitir orientações adicionais sobre os critérios a serem utilizados nessa decisão?

Controles parentais

Os Artigos 16 a 18 tratam de mecanismos de supervisão parental.

Quando o governo pretende publicar minutas de regulamentos, diretrizes e padrões mínimos adicionais para os mecanismos de supervisão parental previstos no Artigo 17, inciso I (ou realizar consulta pública sobre o tema)? As empresas associadas à ESA possuem ampla

experiência e contribuições relevantes sobre ferramentas de controle parental e a ESA acolhe a oportunidade de responder a perguntas específicas sobre esse assunto.

As obrigações relativas a controles parentais devem manter flexibilidade para que os provedores desenvolvam ferramentas inovadoras apropriadas a diferentes faixas etárias, considerando a autonomia progressiva e as capacidades em evolução de crianças e adolescentes.

Como as empresas de jogos eletrônicos devem lidar com eventuais obrigações conflitantes relativas ao consentimento parental e aos controles parentais previstas no Artigo 21 do ECA Digital, em comparação com os Artigos 16 a 18 do ECA Digital e com as obrigações da Lei do Marco Legal para a Indústria dos Jogos Eletrônicos (Lei 14.852 de 3 de maio de 2024)?

O Artigo 17, § 4º, inciso III, exige que os provedores de serviços adotem configurações-padrão de ferramentas de supervisão parental com o mais alto nível de proteção disponível, incluindo ferramentas para restringir a comunicação de crianças e adolescentes por usuários não autorizados. A definição de “usuários não autorizados” deve ser feita com referência à capacidade dos usuários protegidos ou de seus responsáveis, conforme o caso, que tenham acesso às funcionalidades de bloqueio e restrição de comunicação, a fim de impedir comunicações por usuários “não autorizados”.

O Artigo 17, § 4º, inciso III, também exige a adoção de ferramentas para acompanhamento do uso adequado e saudável do produto ou serviço. A definição do que é “adequado e saudável” deve considerar a autonomia progressiva e as capacidades em evolução de crianças e adolescentes, pois o que é adequado para determinada faixa etária (adolescentes) pode não ser considerado adequado para usuários mais jovens.

Supervisão parental de contas de jovens

O Artigo 24 trata das contas de usuários menores de 16 anos, aparentemente apenas em relação a redes sociais, conforme indicado no título do Capítulo IX (“Das redes sociais”). Considerando que o Artigo 16 não se refere especificamente a “provedores de redes sociais”, solicita-se o esclarecimento de que as disposições do Artigo 24 são, de fato, limitadas em escopo aos provedores de redes sociais.

Loot boxes pagas

O Artigo 20 regula a disponibilidade de caixas de recompensa (*loot boxes*) pagas oferecidas em jogos eletrônicos direcionados a, ou de acesso provável por, crianças e adolescentes.

A ESA solicita confirmação de que as empresas podem cumprir a proibição de loot boxes pagas prevista no Artigo 20 por meio de qualquer uma das seguintes abordagens:

1. Restrição no nível do jogo, em que um jogo eletrônico que contenha loot boxes pagas exija verificação etária eficaz de que o jogador tem 18 anos ou mais antes de conceder acesso ao jogo, sendo classificado como 18+;
2. Restrição no nível da funcionalidade, em que o acesso ao jogo eletrônico seja permitido a todos os jogadores, mas menores de idade (ou qualquer pessoa que não tenha verificado

eficazmente ter 18 anos ou mais) sejam impedidos de comprar loot boxes pagas direta ou indiretamente; ou

3. Jogos com restrição geográfica, em que loot boxes pagas sejam totalmente desativadas em jogos destinados ao mercado brasileiro.

Solicita-se confirmação de que, especialmente nos casos em que as loot boxes pagas tenham sido efetivamente restringidas para crianças e adolescentes conforme descrito acima, as classificações etárias dos jogos que cumprirem as novas obrigações do Artigo 20 não precisarão ser alteradas.

A resposta a essa questão impacta a possibilidade de permanência no mercado de jogos afetados que já foram adquiridos por consumidores quando classificados como “Livre” no Brasil antes da promulgação do ECA Digital. Consumidores que legitimamente adquiriram um jogo existente com loot boxes pagas podem perder acesso à sua compra caso passem a ter que comprovar ter 18 anos ou mais por meio de verificação etária eficaz e a classificação etária desse mesmo jogo seja elevada para 18+.

Publicidade

O Artigo 22 trata de provedores que realizam publicidade direcionada (por meio de perfilamento, análise emocional, etc.) voltada ou suscetível de alcançar crianças e adolescentes.

Como a ANPD esclarecerá as obrigações relativas à publicidade previstas neste artigo, de modo a alinhá-las ao regime de consentimento da Lei Geral de Proteção de Dados (LGPD)?

Comunicação às autoridades

Os Artigos 27 a 30 tratam de denúncias, pedidos de remoção e recursos.

O governo fornecerá esclarecimentos adicionais sobre a conformidade adequada com as obrigações de comunicação às autoridades e de remoção de dados previstas no Artigo 27, bem como sobre os requisitos de denúncia, remoção, notificação e recurso previstos nos Artigos 28 a 30?

Em particular, no que se refere ao Artigo 27, o governo pode confirmar que a comunicação dos tipos de conteúdo mencionados (exploração, aliciamento, etc.) a autoridades internacionais reconhecidas (por exemplo, o *National Centre for Missing & Exploited Children*) satisfará as obrigações dos provedores previstas neste artigo, não sendo exigida a apresentação de relatório duplicado às autoridades nacionais brasileiras em relação ao mesmo conteúdo? Da mesma forma, o governo pode confirmar quais são as autoridades competentes às quais devem ser encaminhadas as comunicações previstas no Artigo 28?

Transparência

O Artigo 31, parágrafo único, exige que determinados provedores de aplicações de internet disponibilizem, gratuitamente, os dados necessários à realização de pesquisas sobre os impactos de seus produtos e serviços. A ESA recomenda que a regulamentação traga maior especificidade,

esclarecendo que a intenção dessa disposição é sua aplicação a redes sociais. Ademais, tanto as partes solicitantes dos dados quanto as pesquisas a serem realizadas devem atender a critérios prévios definidos em regulamento, com referência a padrões internacionalmente reconhecidos para pesquisas clínicas e acadêmicas, bem como a padrões globais relativos à segurança e integridade dos dados dos usuários.

Flexibilidade e responsabilidade dos provedores

O Artigo 39 trata das obrigações do ECA Digital e de sua aplicação proporcional, levando em conta o grau de interferência do fornecedor sobre o conteúdo, o número de usuários e o porte do fornecedor. O governo fornecerá orientações adicionais sobre como a aplicação das diversas disposições do ECA Digital mencionadas no Artigo 39 variará de acordo com as características e funcionalidades do serviço e sobre como o grau de interferência sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor contribuirão para essa avaliação?

Atenciosamente,



Amanda Denton
Conselheira Sênior, Política Global
Associação de Software de Entretenimento (ESA)



CONTRIBUIÇÃO DO INSTITUTO ALANA

**TOMADA DE SUBSÍDIOS SOBRE PRINCIPAIS CONCEITOS DO ECA
DIGITAL**

DEZEMBRO DE 2025



Participa + Brasil - Tomada de Subsídios: ECA digital - Principais conceitos

Prazo: 12/12/2025

O Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025) constitui um marco normativo robusto, cuidadosamente estruturado e dotado de definições precisas para orientar sua aplicação. A própria lei estabelece parâmetros interpretativos relevantes, como a noção de “melhor interesse”, definida como a proteção da privacidade, segurança, saúde física e mental, acesso à informação, liberdade de participação na sociedade, acesso significativo às tecnologias digitais e bem-estar (art.5ª,§ 2º).

Nesse contexto, a presente tomada de subsídios se insere no processo de aprimoramento interpretativo que acompanha a implementação de qualquer diploma legal recentemente em vigor, contribuindo para a coerência, efetividade e segurança jurídica na execução das disposições do Estatuto.

PERGUNTA: Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos? (*Parágrafo*)

SUMÁRIO

A. Clarificação sobre o caráter cumulativo ou não dos critérios de “acesso provável” (art. 1ª, § único).....	3
B. Parâmetros para a definição de “configurações que evitem o uso compulsivo de produtos”, (art. 8º, inciso IV) “recursos que possam resultar em uso excessivo do produto ou serviço por criança ou adolescente” (art. 17, §4º, inciso II) e sua relação com padrões manipulativos de design.....	4
C. Parâmetros para compreensão de “exploração comercial” de crianças e adolescentes e diretrizes para evitar práticas publicitárias predatórias e perfilamento com fins comerciais (art. 6ª, V, c/c arts. 22, 23 e 26).....	5
D. Parâmetros para a implementação do relatório de impacto (RIPD) previsto no art. 16 do ECA Digital.....	8
E. Grau de interferência do fornecedor, serviços com controle editorial e que veiculem conteúdos protegidos por direitos autorais.....	9
F. Revisão e harmonização dos regulamentos de fiscalização e sanção à luz do ECA Digital, incluindo coordenação obrigatória entre ANPD e Poder Judiciário.....	12

A. Clarificação sobre o caráter cumulativo ou não dos critérios de “acesso provável” (art. 1ª, § único)

A Lei nº 15.211/2025 (Doravante “ECA digital”) estabelece, no art. 1º, parágrafo único, três situações que caracterizam “acesso provável” por crianças e adolescentes. Embora o conteúdo dos incisos seja claro, a lei não explicita se tais critérios devem ser interpretados como cumulativos ou alternativos, o que pode gerar divergências relevantes em sua aplicação prática.

Para conferir maior previsibilidade, recomenda-se que a regulamentação da ANPD esclareça se:

- **Basta a presença de um único critério** (suficiente probabilidade e atratividade; ou considerável facilidade de acesso; ou significativo grau de risco), de modo que os incisos funcionem como critérios alternativos, capazes individualmente de caracterizar acesso provável; ou
- **Há necessidade de combinação de dois ou mais critérios**, adotando-se uma interpretação cumulativa, na qual, por exemplo, o risco ou a atratividade somente configuram acesso provável quando coexistentes.

Como parâmetro interpretativo, destaca-se que regimes internacionais de proteção infantil em ambientes digitais, como, por exemplo, o Age Appropriate Design Code (Reino Unido)¹ e a California Age-Appropriate Design Code Act², usualmente tratam critérios semelhantes como alternativos: basta que o serviço seja atraente, acessível ou apresente riscos significativos para que seja considerado “provável” à criança.

O *Online Safety Act* (2023)³ do Reino Unido segue racionalidade semelhante. O conceito de “provavelmente acessado por crianças” se estrutura de modo **alternativo** e baseado no risco, podendo ser configurado por três vias distintas (Seção 37): (i) **avaliação do próprio provedor**, que conclua ser possível o acesso infantil (s. 31(2)); (ii) **não realização** da avaliação obrigatória de acesso infantil (s. 31(4)–(5)); (iii) **determinação da OFCOM**, após investigação (s. 31(6)).

¹

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-of-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/>

² https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

³ <https://www.legislation.gov.uk/ukpga/2023/50>

Em nenhuma dessas hipóteses há exigência de que múltiplos fatores de atratividade, acessibilidade e risco coexistam. O critério central é a **possibilidade razoável de acesso de crianças e adolescentes**, diretamente associada ao risco a tais sujeitos.

B. Parâmetros para a definição de “configurações que evitem o uso compulsivo de produtos”, (art. 8º, inciso IV) “recursos que possam resultar em uso excessivo do produto ou serviço por criança ou adolescente” (art. 17, §4º, inciso II) e sua relação com padrões manipulativos de design

O art. 8º, IV, do ECA digital determina que fornecedores de produtos e serviços digitais adotem configurações que evitem o uso compulsivo por crianças e adolescentes. Embora o comando normativo seja claro em sua finalidade protetiva, as configurações a que se faz referência neste artigo demandam parâmetros interpretativos mais específicos para orientar práticas de conformidade, avaliação regulatória e desenho de produtos que atendam às particularidades do desenvolvimento de crianças e adolescentes. De igual modo, o que dispõe o art. 17, §4º, inciso II da Lei.

Nesse sentido, a regulamentação poderia explicitar as situações em que o design, a arquitetura de escolha ou o funcionamento da plataforma:

- Exploram vulnerabilidades de desenvolvimento, estruturando interações que se apoiam em limitações cognitivas e emocionais típicas da infância e adolescência.
- Induzem prolongamento artificial do uso, por meio de estímulos persuasivos contínuos, ausência de pontos de parada naturais, feeds de rolagem infinita, feedbacks intermitentes, sistemas de recompensas escalonadas, sistemas algorítmicos calibrados para esse fim ou conteúdo que se renova automaticamente (como feeds infinitos)⁴.
- Criam ciclos de retorno não totalmente voluntários, associados a ansiedade, medo de perda (FOMO), pressão social ou competição exacerbada, elementos frequentemente reforçados por notificações frequentes⁵, contadores regressivos, check-ins diários ou metas artificiais.

⁴ <https://link.springer.com/book/10.1007/978-3-032-05008-3>

⁵ <https://edition.cnn.com/2023/09/26/health/teen-hundreds-of-phone-notifications-report-wellness>

- Incorporam padrões manipulativos⁶ ou hostis, que dificultam a desconexão ou exigem esforço desproporcional para sair de uma atividade, cancelá-la, ajustar configurações ou exercer escolhas significativas.
- Geram riscos verificáveis ao bem-estar, como impactos negativos na autoestima, na saúde mental ou na percepção de competência, especialmente em ambientes gamificados que intensificam comparações sociais ou rankings.

Importante ressaltar que o problema reside na gamificação em si **no uso coercitivo ou manipulativo de mecanismos de engajamento**. Modelos éticos de gamificação, baseados em participação voluntária, desafios relevantes, autonomia do usuário e ausência de punições desmedidas podem fortalecer motivação intrínseca, autonomia e competências socioemocionais. Entretanto, quando esses elementos são empregados para maximizar engajamento a qualquer custo, inserem-se claramente na categoria de práticas que fomentam uso compulsivo, especialmente entre populações com menor capacidade de autorregulação.

Vale destacar que o **Guia sobre Uso de Dispositivos Digitais**, publicado pela SECOM-PR em 2025, já traz, em seu bojo, o reconhecimento de que diversos dos elementos típicos do *design* de produtos e serviços digitais têm o condão de induzir o uso excessivo e compulsivo de telas, como os *feeds* de rolagem infinita⁷, a reprodução automática de conteúdos audiovisuais, as notificações incessantes etc. É importante que o processo de regulamentação da lei garanta a sua coerência com outras políticas públicas, inclusive as derivadas do referido Guia, e proponha um olhar profundo sobre as técnicas de *design* adotadas por fornecedores de produtos e serviços digitais no contexto de explosão da chamada economia da atenção⁸.

Vale destacar, também, que o Instituto Alana está desenvolvendo o “**Guia de Práticas Éticas de Design em Plataformas Educacionais Usadas por Crianças e Adolescentes na Educação Básica**”, em parceria com o Grupo de Pesquisa “Aspas”, conduzido pelo professor George Valença (UFRPE). O material, que será publicado em breve, poderá contribuir para o aprofundamento deste debate. Entre seus insights centrais estão a identificação de elementos de design que promovem autonomia, clareza e segurança; a classificação de práticas manipulativas que geram coerção ou pressão indevida; e parâmetros técnicos para diferenciar engajamento saudável de uso compulsivo induzido.

⁶

<https://politics.org.br/pt-br/governanca-news/design-enganoso-e-manipulativo-em-plataformas-digitais-um-mapeamento-entre-estudos>

⁷ <https://www.deceptive.design/>

⁸



C. Parâmetros para compreensão de “exploração comercial” de crianças e adolescentes e diretrizes para evitar práticas publicitárias predatórias e perfilamento com fins comerciais (art. 6º, V, c/c arts. 22, 23 e 26)

O ECA digital estabelece um conjunto de salvaguardas voltadas a prevenir a **exploração comercial** de crianças e adolescentes em ambientes digitais. No art. 6º, V, a lei determina que fornecedores adotem medidas razoáveis desde a concepção e durante a operação de seus produtos e serviços para prevenir riscos relacionados a “práticas publicitárias predatórias, injustas ou enganosas, ou outras práticas conhecidas por acarretarem danos financeiros a crianças e adolescentes”.

Trata-se de um **comando central que se articula diretamente com as proibições previstas nos arts. 22, 23 e 26**, que vedam o direcionamento de publicidade comercial por perfilamento, o uso de tecnologias intrusivas para fins publicitários e a monetização de conteúdos que explorem a imagem sexualizada de crianças e adolescentes.

A compreensão do que constitui exploração comercial em ambientes digitais encontra importante base interpretativa na **Resolução nº 163/2014 do Conanda**, que consolidou diretrizes sobre publicidade dirigida a crianças. A resolução já define como abusivas e contrárias ao princípio da proteção integral práticas que: (i) se aproveitam da deficiência de julgamento e experiência da criança; (ii) empregam estratégias persuasivas que dificultam o reconhecimento do caráter comercial; (iii) utilizam personagens ou elementos de forte apelo infantil para incentivar consumo; ou (iv) buscam induzir comportamentos que comprometem o bem-estar físico, emocional ou financeiro do público infantojuvenil.

Além disso, a extensa atuação do **Programa Criança e Consumo**, do Instituto Alana, fornece um conjunto robusto de precedentes, análises técnicas e parâmetros aplicados a casos concretos envolvendo publicidade digital, *influencers*, plataformas de vídeo e aplicativos. Essas referências indicam que a exploração comercial não se limita à peça publicitária explícita, mas inclui um amplo espectro de dinâmicas digitais que visam maximizar conversões comerciais com base na vulnerabilidade infantil, especialmente quando sustentadas por técnicas de perfilamento e análise comportamental.

Nesse contexto, os arts. 22 e 26 do Estatuto digital representam importante avanço ao vedarem expressamente:



- **o uso de técnicas de perfilamento** para direcionamento de publicidade comercial a crianças e adolescentes;
- **a coleta de dados pessoais**, inclusive aqueles obtidos em processos de verificação de idade, para fins de criação de perfis comportamentais;
- **o uso de tecnologias imersivas** (realidade aumentada, estendida, virtual) e análise emocional para fins publicitários.

Essas proibições alinham o ordenamento brasileiro a padrões internacionais de proteção infantil em ambiente digital e refletem a compreensão de que o direcionamento de publicidade com base em perfis individuais ou emocionais constitui forma grave de exploração comercial.

Para orientar a implementação desses dispositivos, a ANPD pode considerar alguns parâmetros claros e tecnicamente viáveis:

- **Proibição de qualquer forma de coleta e tratamento de dados para publicidade personalizada**, incluindo inferências estatísticas, dados de navegação, análise emocional, dados sensíveis e dados gerados por processos de verificação de idade (nos termos do artigo 13 e do §3º, artigo 24 do ECA digital).
- **Estabelecimento de auditorias técnicas** para garantir que sistemas de recomendação e entrega de anúncios não utilizem dados ou padrões comportamentais de usuários identificados ou razoavelmente identificáveis como crianças ou adolescentes.
- **Obrigação de disponibilizar modos de operação sem publicidade comportamental**, com entregas não personalizadas, contextualizadas ou de interesse público.
- **Reforço de salvaguardas no design**, como vetar *deceptive patterns* que incentivem compras, assinaturas, microtransações, loot boxes (artigo 20 do ECA digital) ou outras dinâmicas que convertam vulnerabilidade em captura comercial.
- **Transparência ampliada**, com obrigações de documentação, logs e relatórios sobre ausência de perfilamento, podendo esse critério ser incorporado como um dos requisitos dos relatórios de transparência (artigo 31 do ECA digital)

É relevante observar que tais práticas já são **tecnicamente possíveis** e adotadas por diversas plataformas, que implementaram controles para impedir o perfilamento de contas classificadas como infantis ou de adolescentes. Isso demonstra que a



conformidade é plenamente realizável e depende sobretudo de diretrizes *enforcement* consistentes.

D. Parâmetros para a implementação do relatório de impacto (RIPD) previsto no art. 16 do ECA Digital

O artigo 16 do ECA Digital estabelece, de forma inovadora, a obrigatoriedade de instrumentos de avaliação, monitoramento e mitigação de impactos sempre que houver tratamento de dados pessoais de crianças e adolescentes, especialmente quando voltado a finalidades que não sejam estritamente necessárias à operação do produto ou serviço. O dispositivo estrutura-se a partir de **dois comandos distintos**, porém complementares: **(i)** a consideração prévia e sistemática dos impactos sobre os direitos de crianças e adolescentes; e **(ii)** a elaboração de relatório de impacto à proteção de dados pessoais (RIPD).

Embora relacionados, esses comandos não se confundem. O **RIPD, por si só, não esgota o conteúdo normativo do inciso I**, que exige uma avaliação mais ampla, orientada pela lógica da proteção integral e pelo melhor interesse da criança. Trata-se, portanto, de um novo patamar de diligência regulatória, que transcende a análise tradicional de riscos à privacidade e demanda uma abordagem centrada nos direitos da criança enquanto sujeito em peculiar condição de desenvolvimento.

Dada a atribuição conferida pela lei, compete à Autoridade Nacional de Proteção de Dados (ANPD) definir parâmetros que assegurem a efetividade prática do art. 16. Para tanto, recomenda-se que a implementação do relatório previsto no inciso II seja **informada por metodologias capazes de dar concretude ao inciso I**, em especial aquelas inspiradas no **Children's Rights Impact Assessment (CRIA)**, instrumento reconhecido por organismos internacionais como o UNICEF, o Comitê dos Direitos da Criança das Nações Unidas e o Conselho da Europa.

O modelo CRIA permite **uma avaliação integrada que contempla**: (i) riscos à privacidade e à segurança; (ii) impactos no desenvolvimento biopsicossocial; (iii) efeitos sobre autonomia, autodeterminação informacional e participação; (iv) potenciais desigualdades ou discriminações; (v) riscos decorrentes de design, arquitetura de informações e governança algorítmica.

A incorporação de metodologia inspirada no CRIA também responde à necessidade de superar limitações do atual regime regulatório. A **Resolução CD/ANPD nº 2/2022**, ao condicionar a obrigatoriedade de elaboração de RIPD à presença cumulativa de dois critérios de alto risco, trata o tratamento de dados de crianças e adolescentes como apenas um desses critérios. No contexto do ECA Digital, essa



lógica deve ser revista, uma vez que o legislador já determinou expressamente a obrigatoriedade do relatório como forma de tutela reforçada, independentemente da presença cumulativa de outros fatores.

Com base nisso, recomenda-se que a ANPD avalie:

- A definição de parâmetros específicos para o RIPD do ECA Digital, em articulação com o modelo previsto na LGPD, **explicitando que esse instrumento não esgota o cumprimento do inciso I do art. 16**, o qual demanda uma avaliação ampliada dos impactos sobre os direitos de crianças e adolescentes.
- A definição de **conteúdos mínimos** que incluam avaliação de design, análise de riscos, impactos decorrentes de perfilamento, engajamento compulsivo, publicidade e exploração comercial;
- A obrigatoriedade de **atualização contínua** do relatório, especialmente quando houver alterações substantivas no produto, no modelo de negócios ou nos fluxos de dados;
- A instituição de **parâmetros de participação e reconhecimento das vozes de crianças e adolescentes**, sempre que adequado, em harmonia com a autonomia progressiva e com diretrizes como a Resolução Conanda nº 245/2024;
- A utilização do relatório como instrumento de **prestação de contas** para demonstrar como o provedor implementa o melhor interesse da criança na concepção e operação do produto.

Ao reconhecer que o **RIPD não é suficiente, isoladamente, para cumprir o inciso I do art. 16**, e ao orientar sua implementação por metodologias inspiradas no CRIA, a ANPD fortalece a lógica da proteção integral, densifica o dever de prevenção e assegura que soluções tecnológicas voltadas ao público infantojuvenil sejam concebidas e operadas em conformidade com a prioridade absoluta assegurada pela Constituição Federal, pela LGPD e pelo próprio ECA Digital.

E. Grau de interferência do fornecedor, serviços com controle editorial e que veiculem conteúdos protegidos por direitos autorais

O art. 39 do ECA Digital estabelece que as obrigações previstas nos arts. 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 serão aplicadas conforme as características e funcionalidades do produto ou serviço, moduladas segundo o grau de interferência do fornecedor sobre os conteúdos disponíveis e de acordo com seu porte. O próprio dispositivo cria uma exceção relevante, no §1º, ao dispensar do cumprimento



dessas obrigações os serviços com controle editorial e os provedores de conteúdos previamente licenciados, desde que preencham requisitos estritos. A definição do art. 2º, IX complementa o cenário ao descrever serviço com controle editorial como aplicação de internet cuja finalidade principal é disponibilizar conteúdos previamente selecionados sem uso de meios automatizados de seleção, por responsável econômico que não se confunde com o usuário final.

O regulamento, portanto, precisa dar contornos mais claros ao alcance dessa exceção, evitando que ela se transforme, na prática, em uma porta aberta para fuga de responsabilidade, especialmente em ambientes que apresentam riscos típicos a crianças e adolescentes. Para isso, alguns critérios técnicos podem orientar a interpretação.

Primeiro, a lógica do controle editorial, segundo o art. 2º, IX, exige não apenas a ausência de seleção automatizada, mas uma supervisão humana robusta e fiel, capaz de exercer curadoria direta sobre o conjunto de conteúdos disponibilizados, em conformidade com a classificação indicativa, nos termos do art. 8º, I, II e III. Não basta que exista qualquer nível de moderação humana, é necessário que a disponibilização seja fruto de seleção prévia consciente, exercida por um agente econômico que define o catálogo e responde por ele. Essa interpretação decorre do próprio objetivo protetivo do capítulo e impede que plataformas que operam majoritariamente com fluxos de conteúdo dinâmico, distribuído automaticamente ou em escala industrial, se autodeclarem como editoriais quando, de fato, não o são.

Esse critério exclui, de forma clara, plataformas com conteúdos gerados por usuários (UGC), ainda que elas operem esquemas sofisticados de moderação humana ou comunitária. Fóruns abertos, plataformas de postagem pública, sistemas com feed, ranking, comentários, salas públicas ou recursos de descoberta de usuários não podem ser tratados como serviços com controle editorial, pois a lógica editorial pressupõe curadoria prévia e integral, e não revisão eventual ou moderação corretiva. A presença de moderação, mesmo a moderação humana tradicional, não descaracteriza a natureza participativa e dinâmica da plataforma, que se alinha ao regime de obrigações gerais do art. 39, e não ao regime de exceção do §1º.

Da mesma forma, a interpretação técnica demanda a exclusão dos sistemas que utilizam IA generativa e, de modo mais amplo, dos sistemas baseados em modelos de linguagem (LLMs) do escopo do controle editorial. Esses sistemas organizam, sintetizam e priorizam informações por meio de arranjos estatísticos e inferência probabilística que constituem, por definição, uma forma de mediação automatizada, justamente o que o art. 2º, IX proíbe. Além disso, a dinâmica de geração e apresentação de conteúdo nesses sistemas aciona diretamente os mecanismos de risco tratados no art. 6º, que trata dos deveres de segurança, mitigação, verificação



de idade e medidas proporcionais aos riscos vinculados à interferência da tecnologia na exposição de crianças e adolescentes. É tecnicamente impossível enquadrar uma curadoria algorítmica autônoma como “seleção humana prévia”; portanto, chatbots e serviços de IA generativa não devem ser incluídos na exceção editorial prevista no §1º.

Outro ponto importante diz respeito a plataformas de streaming. Embora o streaming tradicional, baseado em catálogo fixo e curadoria humana, possa se enquadrar no art. 2º, IX, muitos serviços modernos passaram a incorporar funcionalidades que os aproximam de redes sociais e jogos eletrônicos, como chats paralelos, comentários públicos, salas interativas, transmissões ao vivo com participação do público, rankings, perfis de usuários e mecanismos de conexão entre espectadores. Quando essas funcionalidades integram o serviço, sua natureza deixa de ser puramente editorial e passa a envolver riscos típicos do ambiente participativo, devendo, portanto, observar o escopo completo das obrigações dos arts. 6º, 17 a 20 e 27 a 33. A classificação deve seguir o risk-based approach previsto no art. 39 e evitar que a simples presença de um catálogo pré-selecionado seja usada para justificar a dispensa de obrigações protetivas, quando outras funcionalidades criam espaços de interação social não editorializados.

Importa destacar ainda que a mera existência de curadoria humana em canais individuais dentro de plataformas de compartilhamento de vídeos não autoriza a aplicação da exceção prevista no art. 39, §1º. Ainda que determinados canais em redes sociais exerçam seleção humana sobre seus próprios conteúdos (afinal, há um humano controlando e selecionando postagens), isso não altera a natureza geral da plataforma que os hospeda, a qual opera como uma rede social audiovisual, com mecanismos intrínsecos de interação entre usuários, comentários públicos, transmissões ao vivo, perfis abertos, algoritmos de recomendação, feeds personalizados e potenciais de conexão e descoberta entre pessoas desconhecidas. Além disso, o nível de controle da plataforma principal sobre o fluxo de informações, inclusive por meio de ferramentas de ranqueamento, amplificação, recomendação, moderação automatizada e políticas de governança, demonstra que ela mantém influência decisiva sobre a forma como conteúdos circulam e atingem usuários, especialmente crianças e adolescentes. Esse grau de interferência justifica que os deveres proativos de segurança, mitigação de riscos e transparência não possam ser excetuados, pois quem hospeda e estrutura o ambiente responde pelas dinâmicas de exposição e interação que ele possibilita, mesmo quando criadores individuais controlam seus próprios catálogos. Trata-se, portanto, de uma lógica de responsabilidade compartilhada, em que a curadoria humana do canal não substitui, nem diminui, a responsabilidade da plataforma pelas condições sistêmicas de circulação, descoberta e interação, nem deve ser reduzida a responsabilidade



individual dos fornecedores dos canais. Assim, canais hospedados em plataformas de natureza participativa não podem ser enquadrados como serviços com controle editorial, nem a própria plataforma, em razão do risco estrutural inerente à arquitetura social e algorítmica da plataforma.

Por fim, a interpretação sistemática do art. 39 exige que todo o regime de exceções seja lido conforme o princípio da proteção integral e da prioridade absoluta às crianças e aos adolescentes. Isso significa que dúvidas interpretativas devem ser resolvidas em favor da aplicação das obrigações de segurança, transparência, mitigação de riscos e supervisão parental. Para tanto, podem ser explicitados parâmetros adicionais, como: (i) a exceção editorial deve ser aplicada de forma restritiva; (ii) qualquer grau relevante de automatização na seleção, priorização ou distribuição de conteúdo deve afastar a exceção; (iii) funcionalidades de interação social ou conexão entre usuários são incompatíveis com o regime editorial; (iv) sempre que o serviço apresentar natureza híbrida, os dispositivos mais protetivos devem prevalecer.

F. Revisão e harmonização dos regulamentos de fiscalização e sanção à luz do ECA Digital, incluindo coordenação obrigatória entre ANPD e Poder Judiciário

A entrada em vigor do ECA digital traz novos desafios ao regime de fiscalização e sanções aplicáveis ao tratamento de dados de crianças e adolescentes, exigindo **revisão e reorganização antecipada** dos instrumentos normativos da ANPD.

Considerando a *vacatio legis* da Lei nº 15.211/2025, é essencial que a Autoridade disponha, já na data de início de vigência, de diretrizes claras, coerentes e plenamente alinhadas ao ECA Digital, evitando lacunas normativas que possam comprometer a efetividade da proteção integral.

A revisão das Resoluções CD/ANPD nº 1/2021 (fiscalização) e nº 4/2023 (dosimetria e sanções) torna-se necessária, especialmente porque o ECA digital introduz um regime sancionatório híbrido, distinto daquele previsto na LGPD. O seu artigo 35 estabelece penalidades administrativas que incluem advertência e multa (incisos I e II), de competência exclusiva da autoridade administrativa autônoma designada (ou seja, a ANPD), mas prevê que as sanções mais gravosas, como suspensão temporária e proibição de exercício de atividades (incisos III e IV), sejam aplicadas pelo Poder Judiciário.



Esse desenho institucional cria uma interdependência inédita entre ANPD e Judiciário, pois a **aplicação de parte das sanções depende de decisão judicial**, o que não ocorre na LGPD, em que todas as sanções administrativas são aplicadas diretamente pela ANPD.

Diante disso, a regulamentação da ANPD deverá:

- Harmonizar a **dosimetria** com as circunstâncias específicas previstas no art. 35, § 1º, incluindo o exame da extensão do dano em esferas individual e coletiva, a reincidência e o impacto social da atividade;
- Prever procedimento claro para **encaminhamento ao Judiciário** das hipóteses que extrapolam a competência sancionatória administrativa, garantindo fluxo seguro, tempestivo e padronizado de informações;
- Articular com o Conselho Nacional de Justiça (CNJ) e tribunais a criação de **protocolos de implementação das ordens de suspensão e bloqueio**, de modo equivalente ao que já existe para medidas de indisponibilidade de bens, ordens de remoção e ordens de interceptação em processos digitais;
- Estabelecer parâmetros sobre **cooperação interinstitucional** com Ministério Público, Conselhos Tutelares e varas da infância, assegurando que os instrumentos de fiscalização do ECA Digital sejam compatíveis com a rede já existente de proteção;



Ref.: Tomada de Subsídios da ANPD para esclarecer conceitos do ECA Digital

A Associação Brasileira de Medicina Diagnóstica – ABRAMED apresenta a seguir as suas propostas de contribuições à Tomada de Subsídios para esclarecer conceitos do ECA Digital, promovida pela Agência Nacional de Proteção de Dados (ANPD).

#	Conceitos selecionados	ECA Digital
1.	Fornecedores de produtos ou serviços de tecnologia da informação com “ <i>acesso provável</i> ”	Art. 1º, parágrafo único
2.	“ <i>Perfilamento</i> ” para publicidade comercial	Art. 2º, V c/c art. 22 e 26
3.	Tratamento dos dados pessoais de crianças e de adolescentes de forma que “ <i>cause, facilite ou contribua</i> ” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei	Arts. 2º, V, 22 e 26
4.	Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser “utilizados unicamente para essa finalidade”	Art. 13
5.	Mecanismos de Supervisão Parental	Arts. 2º, VIII, art. 12, III e art. 16 e ss
6.	Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais	Art. 16, parágrafo único, II
7.	Verificação de idade “ <i>a cada acesso</i> ” do usuário ao conteúdo, produto ou serviço	Art. 9, §1º

1. Fornecedores de produtos ou serviços de tecnologia da informação com “*acesso provável*”¹

a) Proposta: entendemos como necessária uma interpretação que requeira a cumulação de todos os requisitos previstos no parágrafo único do art. 1º, do ECA Digital. Além disso, é necessário definir com critérios objetivos o enquadramento nos incisos I e II.

b) Fundamento:

A conceituação de “*acesso provável*”, prevista no parágrafo único do art. 1º, do ECA Digital, é excessivamente abrangente. Caso seja interpretada de forma literal, tal definição tende a incluir, para todos os fins, praticamente toda e qualquer aplicação de internet, tornando ineficaz a própria criação da categoria (“**serviços de tecnologia da informação com *acesso provável*”**), o que não parece refletir a intenção do legislador.

O inciso I refere-se à “*suficiente probabilidade de uso e atratividade*”, mas utiliza terminologia genérica, desprovida de critérios objetivos capazes de orientar a interpretação do que efetivamente configuraria tal situação. Dessa forma, mostra-se necessária a previsão de parâmetros mensuráveis que permitam uma aplicação uniforme e verificável da norma, garantindo segurança jurídica.

Isso é especialmente relevante, considerando que interesses podem alterar-se significativamente entre as gerações. Por exemplo, a Geração Z possui interesse por questões religiosas superior ao da

¹ Art. 1º, parágrafo único, ECA Digital.



geração de seus pais², não existindo clareza no normativo se isso por si só tornaria páginas sobre essa temática de uso “suficientemente provável por crianças e adolescentes”.

Além disso, o conceito legal de “crianças e adolescentes” abrange uma faixa etária bastante ampla. Indivíduos situados no limite superior dessa faixa, por exemplo, entre 16 e 18 anos incompletos, possuem, em regra, interesses e comportamentos digitais muito próximos aos de adultos, especialmente jovens adultos. Aplicado isoladamente, o critério do inciso I tende, portanto, a abranger indiscriminadamente todo e qualquer produto ou serviço ofertado no ambiente virtual.

O inciso II estabelece como requisito a “considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes”. No entanto, considerando que vivemos em uma sociedade marcada por nativos digitais, muitas vezes mais aptos a utilizar tecnologias do que seus próprios responsáveis legais, a maior parte dos serviços digitais pode ser facilmente acessada e utilizada por menores.

Dessa forma, na falta de tal interpretação no sentido aqui proposto, existiria um enquadramento praticamente absoluto na categoria, excetuando-se apenas os casos em que existem barreiras artificiais robustas, sejam econômicas (ex.: cobrança de valores elevados para acesso) ou tecnológicas (ex.: processos rigorosos de verificação de idade), capazes de impedir ou dificultar significativamente o acesso de menores.

Tais barreiras, contudo, não estão presentes na ampla maioria das aplicações de internet. Demandá-las geraria entraves significativos para a economia de rede e para o próprio fluxo informacional, afetando, de modo desproporcional, especialmente os grupos mais vulneráveis, que já enfrentam dificuldades no acesso à internet, inclusive por falta de conhecimento. A título ilustrativo, segundo a Pesquisa Nacional por Amostra de Domicílios Contínua, 46% dos não usuários da internet no Brasil (equivalentes a 12% da população) deixam de utilizá-la justamente por não saberem como fazer isso³.

Diante do exposto, embora não se trate de uma leitura estritamente literal do dispositivo, entendemos que a interpretação teleológica da lei, que pressupõe uma distinção real entre serviços de tecnologia da informação de “acesso provável” e aqueles que não o são, exige que os critérios previstos no parágrafo único sejam satisfeitos de forma cumulativa. Caso contrário, a distinção será ineficaz, resultando, na prática, no enquadramento de todo e qualquer serviço da sociedade da informação.

2. “Perfilamento” para publicidade comercial⁴

a) Proposta: entendemos como necessária uma interpretação que limite o teor do escopo de perfilamento previsto no inciso V, do art. 2º, de modo que não abarque perfis não-intrusivos, como meros perfis demográficos, sobretudo para aplicação do art. 22.

b) Fundamento:

² Disponível em: <https://guiame.com.br/gospel/noticias/estudo-geracao-z-e-millennials-superam-geracoes-mais-velhas-na-frequencia-igreja.html>

³ Disponível em: <https://www.cnnbrasil.com.br/nacional/mais-de-10-milhoes-de-brasileiros-nao-acessam-internet-por-nao-saberem-usar-a-tecnologia-diz-ibge/>

⁴ art. 2º, V c/c art. 22 e 26, ECA Digital.



O art. 22 da Legislação estabelece uma proibição genérica à utilização de técnicas de perfilamento para práticas publicitárias comerciais envolvendo menores. No entanto, sua interpretação literal resultaria em uma restrição desproporcional, além de se mostrar em desacordo com a intenção aparente do legislador, que no art. 26 veda especificamente a criação de perfis comportamentais, e não a de quaisquer perfis.

A vedação absoluta ao perfilamento poderia, por consequência, impedir até mesmo direcionamentos publicitários baseados exclusivamente em perfis cadastrais, os quais são, por natureza, não intrusivos, vez que se baseiam em dados cadastrais básicos. No âmbito da saúde, por exemplo, informações cadastrais básicas podem possibilitar a divulgação de serviços voltados ao interesse do próprio menor, como campanhas de vacinação, orientações preventivas ou recomendações de exames pertinentes à região ou faixa etária.

Dessa forma, as restrições ao perfilamento de menores devem ter alcance razoável e proporcional, de modo a proteger o melhor interesse da criança e do adolescente sem inviabilizar desnecessariamente o desenvolvimento regular de atividades econômicas legítimas, sobretudo atividades que melhor resguardam o interesse do menor, como as do setor de saúde.

É, portanto, essencial que a interpretação da vedação ao perfilamento não seja operada de forma literal, isto é, como proibição de qualquer modalidade de perfilização. Pelo contrário, deve-se distinguir entre o perfilamento invasivo, efetivamente proibido, e o mero direcionamento cadastral de publicidade, que deve ser permitido.

O perfilamento invasivo caracteriza-se por práticas como análise emocional detalhada, criação de perfis comportamentais individualizados e rastreamento contínuo das atividades do menor, representando risco concreto à sua privacidade. Por outro lado, o direcionamento cadastral consiste apenas na segmentação básica de público com base em dados cadastrais elementares, como faixa etária, gênero ou localização geográfica, sem qualquer forma de monitoramento comportamental ou rastreamento individual da atividade online. Por sua natureza, esse tipo de segmentação não acarreta risco relevante ao menor.

A adoção de entendimento distinto poderia gerar prejuízos significativos tanto para entidades que oferecem serviços legítimos de interesse do menor, a exemplo do setor da saúde, quanto para o próprio menor, que deixa de receber informações de seu interesse, sem produzir qualquer benefício real à proteção dos menores. Na prática, crianças e adolescentes continuariam a receber publicidade, porém de produtos e serviços potencialmente irrelevantes ou incoerentes com seu interesse, o que contraria o próprio propósito da legislação.

3. Tratamento dos dados pessoais de crianças e de adolescentes de forma que “cause, facilite ou contribua” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei⁵

a) Proposta: entendemos como necessária uma interpretação clara do significado da expressão “cause, facilite ou contribua” para atividades de tratamento que gerem riscos desproporcionais aos direitos do menor ou sejam, em si mesmas, violadoras desses direitos.

⁵ Arts. 2º, V, 22 e 26, ECA Digital.



b) Fundamento:

A expressão “*cause, facilite ou contribua*” mostra-se excessivamente abrangente e, se interpretada literalmente, acaba por vedar, na prática, qualquer atividade de tratamento de dados envolvendo menores de idade.

Isso ocorre porque os verbos “*facilitar*” e “*contribuir*” sugerem que qualquer atividade capaz de gerar riscos aos direitos legais dos menores, inclusive direitos gerais, como o direito à privacidade, estaria proibida. Em tese, qualquer operação de tratamento poderia “*facilitar*” ou “*contribuir*” para um dano caso seus riscos, ainda que remotos, viessem a se materializar.

Como o dispositivo é silente quanto ao grau de risco, sua redação abarca indistintamente todos os tratamentos, já que toda atividade de tratamento envolve algum nível de risco aos titulares. É precisamente por essa razão que legislações modernas de proteção de dados, como a Lei Geral de Proteção de Dados, adotam abordagens baseadas em risco, abordagem esta que, em regra, os agentes de tratamento são recomendados a adotar em sua governança interna, como leciona a Autoridade de Dados da Irlanda⁶. Uma previsão genérica que veda tratamentos que apresentem riscos, sem qualquer qualificação, acaba, na prática, por proibir todas as atividades de tratamento.

Considerando que tal leitura não é razoável nem compatível com o sistema de proteção de dados vigente, recomenda-se que o dispositivo seja esclarecido para abranger apenas atividades de tratamento que: (i) gerem riscos desproporcionais aos direitos e liberdades do menor; ou (ii) sejam, em si mesmas, incompatíveis ou violadoras desses direitos. Essa interpretação assegura a proteção das crianças e adolescentes sem inviabilizar tratamentos legítimos e necessários.

4. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser “utilizados unicamente para essa finalidade”

a) Proposta: o conceito de “dados coletados para a verificação da idade”, para fins de aplicação do art. 13, não deve incluir o reaproveitamento de dados coletados em outros processos (ex. prevenção a fraudes) para fins de verificação de idade.

b) Fundamento:

No âmbito de seus processos ordinários, em especial aqueles voltados à prevenção de fraudes, grande parte das organizações já coleta dados que poderiam ser razoavelmente empregados em procedimentos de verificação de idade, tais como informações biométricas, documentos de identificação e demais dados correlatos.

Para evitar a coleta duplicada desses elementos, em afronta ao princípio da necessidade (art. 6º, III, da LGPD), é relevante que a interpretação do art. 13, do ECA Digital, não inviabilize o reaproveitamento de dados previamente tratados para outras finalidades legítimas, sobretudo a prevenção a fraudes, nos processos de verificação de idade.

⁶ Disponível em: <https://www.dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach>

⁷ Art. 13, ECA Digital.



Em outras palavras: o art. 13 deve ser objeto de interpretação restritiva, apenas proibindo-se a reutilização de dados pessoais quando coletados específica e exclusivamente para fins de verificação de idade.

Todavia, não entendemos suficiente que a ANPD apenas realize mera declaração quanto à possibilidade de reaproveitamento: considerando a insegurança jurídica decorrente da redação atual do dispositivo e o potencial de controvérsias acerca de eventual desvio de finalidade – isto é, se determinado dado foi reaproveitado para a verificação de idade ou se, ao contrário, foi coletado originalmente para esse fim e acabou empregado em outra finalidade legítima –, mostra-se essencial que a ANPD estabeleça orientações claras e operacionais que permitam a implementação dessa prática com segurança jurídica.

5. Mecanismos de Supervisão Parental ⁸

a) Proposta: entendemos como necessária a melhor delimitação dos limites aplicáveis a supervisão parental, sobretudo a adoção clara de limitações da interferência dos pais, considerado o direito à privacidade do menor.

b) Fundamento:

É importante que a definição de mecanismos de supervisão parental estabeleça limites claros quanto ao grau de interferência possível pelos responsáveis. Esses mecanismos devem, simultaneamente, resguardar a autoridade parental e proteger o direito à privacidade do menor, sobretudo em aplicações que envolvem aspectos sensíveis de sua intimidade ou em situações nas quais a independência do menor aumenta progressivamente em razão de sua maturidade e capacidade.

No setor da saúde isso é especialmente relevante, considerando que o art. 74, do Código de Ética Médica⁹ expressamente veda a divulgação de informações aos saúde dos menores, inclusive aos seus pais e representantes legais, desde que estes tenham razoável capacidade de discernimento.

Nesse sentido, o Serviço Nacional de Saúde da Inglaterra (*National Health Service*, “NHS”) orienta que os responsáveis legais apenas possam acessar livremente as informações de saúde de seus filhos até os 11 anos de idade, período após o qual o menor pode optar por permitir o acesso, negá-lo ou restringi-lo¹⁰.

Em outras palavras: inexistindo limites claros à capacidade de intervenção parental, de uso dos mecanismos de supervisão, subsiste elevada probabilidade que, a título de proteção das crianças e adolescentes, se tolha a sua privacidade em nível desarrazoado, efetivamente gerando óbice ao desenvolvimento de sua personalidade.

Assim, é necessário assegurar segurança jurídica no sentido de que os mecanismos de supervisão parental não resultem em intrusões indevidas na intimidade dos menores, devendo o nível de acesso e intromissão respeitar a razoável capacidade e maturidade do menor de idade e o grau de intimidade ao qual a informação se refere.

⁸ Arts. 2º, VIII, art. 12, III e art. 16 e ss., ECA Digital.

⁹ Disponível em: <https://portal.cfm.org.br/images/PDF/cem2019.pdf>

¹⁰ Disponível em: <https://www.england.nhs.uk/long-read/identity-verification/>



6. Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais¹¹

a) Proposta: o art. 16º, parágrafo único, II, estabelece a obrigação de as organizações elaborarem “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”. Entendemos necessário esclarecer que tal expressão deve ser interpretada como referência ao mesmo Relatório de Impacto à Proteção de Dados Pessoais (RIPD) previsto na LGPD, não se tratando, portanto, de documento distinto ou adicional.

b) Fundamento:

O legislador introduziu no ECA Digital a expressão “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”, sem, contudo, fornecer qualquer definição normativa para tal documento.

A Lei Geral de Proteção de Dados já incorporou ao ordenamento jurídico nacional o Relatório de Impacto à Proteção de Dados (“RIPD”), instrumento suficiente para a demonstração e gestão de riscos à privacidade nas atividades de tratamento que possam afetar direitos e liberdades fundamentais dos titulares – conceito que pode razoavelmente abranger as situações previstas no ECA Digital.

A adoção de entendimento contrário resultaria na alocação ineficiente de recursos pelos agentes de tratamento, tendo em vista a elevada complexidade técnica já inerente à elaboração de um RIPD, e, sobretudo, o consumo de recursos humanos demandado em sua elaboração – dado o tempo e esforço das áreas de negócio e das equipes técnicas envolvidas, além da participação de profissionais especializados em privacidade.

Deste modo, a criação de um segundo relatório implicaria um consumo duplicado desses recursos limitados, desviando-os de atividades mais relevantes para a própria defesa dos interesses das crianças e adolescentes. A saber: a correção de vulnerabilidades e a implementação dos controles identificados no próprio RIPD, para a elaboração de um documento adicional, de provável conteúdo substancialmente redundante.

Assim, entendemos recomendável que se esclareça que o “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais” se trata do mesmo “relatório de impacto à proteção de dados pessoais” previsto na LGPD.

7. Verificação de idade “a cada acesso” do usuário ao conteúdo, produto ou serviço¹²

a) Proposta: a interpretação literal da expressão “a cada acesso”, para a periodicidade da verificação de idade, conforme previsto no art. 9º, §1º, implicaria ônus desproporcionado e economicamente impraticável, sendo relevante que a ANPD apresente entendimento proporcional aos riscos concretos apresentados por cada serviço da sociedade da informação.

¹¹ Art. 16, parágrafo único, II, ECA Digital.

¹² Art. 9, §1º, ECA Digital.



b) Fundamento:

Embora o art. 9º, § 1º, do ECA Digital determine a adoção de mecanismos de verificação de idade “a cada acesso” do usuário a conteúdos, produtos ou serviços, a interpretação literal dessa exigência pode conduzir a distorções práticas, comprometer a própria experiência digital e se revelar economicamente impraticável para elevado número de organizações.

Conforme o estudo da *Family Online Safety Institute*, é fundamental considerar a experiência do usuário e a minimização de fricção. Isso porque existem preocupações sobre o potencial de que os processos de aferição de idade se tornem o próximo “*banner de cookies*”, obrigando os usuários a passarem por verificações de idade toda vez que visitam um novo site ou aplicativo. Soluções interoperáveis poderiam aliviar os problemas de frustração e fadiga dos usuários e facilitar para as empresas a otimização de seus esforços. Essa noção também apoiaria a ênfase em uma abordagem baseada em risco em que, uma vez que o usuário tenha verificado sua idade, ele só precisaria realizar nova verificação em sites considerados de maior risco, como aqueles com conteúdo adulto ou jogos de azar¹³.

Do ponto de vista corporativo, tecnologias de verificação de idade, não raramente, precisam ser contratadas de terceiros. Referidas soluções habitualmente envolvem um custo por consulta realizada. Ou seja: a cada atividade de verificação de idade, a companhia necessita pagar um determinado valor ao fornecedor.

Assim obrigar os entes privados a realizarem uma verificação de idade do usuário a cada acesso aos seus serviços, mesmo que estes já se encontrem previamente autenticados, implica impor-lhes um significativo aumento do custo operacional – que muitas vezes se revelará economicamente impraticável frente a natureza do negócio.

Por exemplo, em soluções de acesso recorrente, mas com assinatura mensal (com serviços de *streaming*) ou que inexistam custo no acesso em si mesmo (como aplicações para acesso a exames e outras informações médicas), realizar uma biometria ou documentoscopia a cada acesso implicaria provável inviabilidade no fornecimento desses serviços ou, minimamente, provável aumento substancial nos valores de sua assinatura, tornando-os inacessíveis a parte significativa da população.

Além disso, tal requerimento implicaria a necessidade da coleta repetitiva de dados pessoais, ampliando os riscos de segurança da informação e contrariando o princípio da minimização de dados, previsto no art. 6º, III, da Lei Geral de Proteção de Dados Pessoais (LGPD).

Assim, revela-se essencial que a ANPD adote entendimento regulatório que ajuste a periodicidade da verificação de idade aos riscos concretos apresentados por cada serviço da sociedade da informação, de modo a equilibrar a proteção do menor com a viabilidade técnica e econômica das medidas de conformidade.

¹³

Disponível

em:

[https://global-](https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf)

[uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf](https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf)

ANPD - ECA DIGITAL - Tomada de subsídios #1

Pergunta:

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Resposta:

O Kwai Brasil apresenta sua contribuição para esta consulta pública a partir de capítulos específicos da lei. Dentro dos capítulos escolhidos para contribuição, nossos apontamentos dividem-se em questionamentos e sugestões. Nos colocamos à disposição da autoridade para eventuais esclarecimentos acerca das informações compartilhadas nesta consulta.

Capítulo IV: Mecanismos de Aferição de Idade

Os termos sobre aferição de idade descritos nos arts. 10 a 12 (como “mecanismos para proporcionar experiências adequadas à idade”, “soluções técnicas de verificação de idade”, “sinal de idade aos provedores de aplicações de internet” e “mecanismos de aferição de idade”) carecem de clareza conceitual, visando à tradução dos textos legais em processos e interfaces de produto digital.

Considerando os itens mencionados nos arts. 12 a 15, fazem-se necessários esclarecimentos adicionais. Soma-se ainda o art. 24, inciso III, no qual, no caso das redes sociais, é mencionado o aprimoramento contínuo de mecanismos de verificação de idade.

Questionamentos:

- Qual será o mecanismo de aferição de idade a ser adotado pelas lojas de aplicativos? Esse acesso a APIs será de uso público ou haverá custos definidos unilateralmente pela loja?
- Quais serão os procedimentos de aferição de idade para aplicações de acesso provável por menores de idade, considerando as diferenças entre serviços e os diferentes riscos de cada um? Tratando-se de plataformas de compartilhamento de conteúdo gerado por terceiros, quais parâmetros serão adotados?
- Para além dos *age signals*, quais mecanismos complementares devem ser fornecidos pelas lojas de aplicativos?
- Considerando o custo provável para a aferição de idade de usuários, é preciso esclarecer se esses *age signals* serão disponibilizados às aplicações apenas para novos downloads ou se será possível a aplicação retroativa, considerando a base de usuários já existente em cada aplicação?
- O que se espera como padrões mínimos para o aprimoramento contínuo? (art. 24).

Sugestões:

- Sugere-se que, antes de estender a governança de verificação para a cadeia de aplicações, o processo tenha início com um período de integração com os *age signals* das lojas de aplicativos. Dessa forma, será possível:
 - Ter clareza do papel complementar dos sistemas de aferição de idade que serão adotados individualmente por cada serviço de provável acesso por menores, reduzindo os riscos de duplicidade e divergência entre os sinais das lojas de aplicativos e os sistemas individuais de cada plataforma.

Capítulo V: Controles Parentais

Questionamentos:

- Tratando-se do art. 17, faz-se necessária maior clareza, por parte do regulador, sobre quais mecanismos deverão ser adotados para a validação do controle parental. A vinculação a uma conta 18+ já seria suficiente? Haverá alguma base pública de dados disponível via API que permita a verificação das informações acerca do responsável legal do menor?
- Considera-se bem-vinda a orientação do regulador quanto aos padrões mínimos para a execução de relatórios de impacto, monitoramento e avaliação da proteção de dados pessoais, listados no art. 16, parágrafo único, inciso II.

Sugestões:

- Considerando a viabilidade de uma base de dados pública com informações sobre responsáveis, sugerimos a adoção de um período de testes para a validação dessa base e sua integração com os sistemas de controle parental de cada produto ou serviço.

Capítulo XI: Reportes de Violação aos Direitos de Crianças e Adolescentes

Questionamentos:

- "Tratando-se dos arts. 28 e 29, faz-se necessária uma melhor definição dos casos de "violações aos direitos de crianças e adolescentes", do formato de reporte (informações mínimas e padrões de privacidade) e dos canais de notificação para as autoridades competentes designadas. A redação do art. 28, parágrafo único, utiliza a expressão "quando for o caso" de forma ampla e genérica, portanto também merece melhor definição.
- Sugere-se a definição mínima e padronizada dos canais de comunicação para os atores legitimados à solicitação e retirada de conteúdo, a saber: Ministério Público, responsáveis legais e organizações de defesa de menores devidamente cadastradas.

- Tratando-se de vítimas e responsáveis, faz-se necessária uma definição mínima de critérios para validação da denúncia, visando à efetividade, à celeridade e à redução dos riscos de notificações que extrapolam o escopo do art. 29.

Capítulo XII: Relatórios de Transparência:

Questionamentos:

- Tratando-se do art. 31, visando à eficiência e ao alinhamento com o ordenamento jurídico, sugere-se que o regulador estabeleça classificações mínimas para a identificação de conteúdos e contas a serem objeto de reportes, nos termos do art. 31, inciso III. A publicização desse padrão mínimo é fundamental para subsidiar a estratégia de moderação dos serviços digitais e garantir que a elaboração dos relatórios de transparência esteja em consonância com as expectativas do regulador, além de adequada a cada tipo de serviço digital.

Sugestões:

- Sugere-se, seguindo a inteligência do Art. 19 do Marco Civil da Internet e do entendimento do STF, a determinação de necessidade de “identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material”, com a necessária indicação de URL.
- Sugere-se, por parte do regulador, a criação de diretrizes mínimas que orientem os atores regulados na construção de suas avaliações de impacto. As avaliações de impacto podem seguir diferentes métodos e níveis de abrangência, sendo bem-vinda uma padronização mínima que considere as características de cada tipo de serviço digital.

1. Conceito de design manipulativo exige precisão normativa no ECA Digital

O Estatuto Digital da Criança e do Adolescente introduz obrigações relevantes para evitar o uso compulsivo de serviços digitais e proíbe a manipulação de interfaces que comprometa a autonomia do usuário. Contudo, termos como “design manipulativo”, “configurações que evitem uso compulsivo”, “comprometer a autonomia” e “manipular interfaces” são expressões amplas, cuja interpretação pode variar substancialmente entre fornecedores, órgãos de fiscalização e responsáveis legais.

A ausência de parâmetros mais objetivos pode gerar assimetria regulatória, dificultar a responsabilização de práticas nocivas e, ao mesmo tempo, criar insegurança para fornecedores que desejam implementar padrões responsáveis. Por isso, tais conceitos demandam especificação para orientar de forma clara o que constitui uma prática aceitável, inadequada ou proibida, especialmente quando envolve crianças e adolescentes (um grupo com maior vulnerabilidade cognitiva, emocional e comportamental).

Do ponto de vista técnico, o design manipulativo opera por meio de mecanismos de interface, arquitetura de escolhas e estímulos comportamentais capazes de induzir ações não desejadas ou prolongar o uso para além da intenção original do usuário. Sem precisão normativa, práticas de alto risco (que vão da rolagem infinita às notificações insistentes e manipulativas, passando pela dificuldade de acesso a funcionalidades relevantes e anúncios disfarçados, além de métricas sociais de comparação) podem ser interpretadas como neutras, afetando o controle.

Crianças e adolescentes apresentam menor capacidade de reconhecer, resistir ou compreender estratégias persuasivas digitais, tornando-os desproporcionalmente suscetíveis a um design enganoso ou manipulativo, que explore padrões de dopamina, impulsividade ou pressão social, por exemplo. Uma definição vaga pode permitir que produtos destinados a ou acessados por este público adotem práticas de risco sob alegação de neutralidade tecnológica ou inovação.

Por outro lado, definições excessivamente amplas podem desencorajar soluções legítimas, como personalização responsável, recomendações educativas ou design ético / “iluminador”. Daí a importância de delimitar parâmetros técnicos, tais como: intensidade e frequência de estímulos, riscos decorrentes das escolhas de design, ativação padrão de recursos que prolongam o uso e transparência das alternativas. Assim, a especificação técnica dos conceitos relacionados a design manipulativo tem papel central para a efetiva implementação do ECA Digital, garantindo que a proteção das crianças e adolescentes se traduza em práticas concretas de design, supervisão e responsabilidade das empresas. Diante disso, sugere-se:

Acrescente-se o Art. 6-A (Design Manipulativo), com a seguinte redação:

“Art. 6-A – Os fornecedores de produtos e serviços de tecnologia, incluindo provedores de aplicações, sistemas operacionais, plataformas digitais e dispositivos conectados, deverão evitar a adoção de padrões de design enganosos ou manipulativos que possam comprometer a autonomia, a capacidade de escolha ou a formação crítica de crianças e adolescentes.

§1º Consideram-se padrões de design enganosos ou manipulativos aqueles que, por ação ou omissão, explorem vulnerabilidades cognitivas, emocionais, comportamentais ou de

desenvolvimento típico da infância e adolescência, gerando coerção, indução indevida, confusão, pressão social ou prolongamento compulsivo do uso.

§2º Para fins do disposto neste artigo, constituem práticas a serem evitadas, sem prejuízo de outras definidas em regulamento ou avaliadas caso a caso pela autoridade competente:

I – envio de notificações excessivas, persistentes, urgentes sem necessidade operacional, ou em horários inadequados para crianças e adolescentes;

II – implementação de mecanismos de rolagem infinita, linhas do tempo contínuas ou apresentações de conteúdo que impeçam ou dificultem pausas naturais no uso, sem oferecer alternativas adequadas de navegação com limites claros;

III – ativação padrão da reprodução automática de conteúdos audiovisuais, especialmente quando possa resultar em consumo prolongado não intencional;

IV – uso de métricas públicas de engajamento, curtidas, ranqueamentos, comparações de desempenho, indicadores de popularidade ou outros recursos que incentivem pressão social, comparação estética ou comportamental, sem disponibilizar alternativas adequadas ou versões adaptadas para crianças e adolescentes;

V – arquiteturas, fluxos de navegação ou opções de escolha que tornem difícil para crianças e adolescentes ou para seus responsáveis acessar, compreender ou configurar ferramentas de supervisão parental.

§3º O regulamento poderá estabelecer parâmetros objetivos para avaliação dessas práticas, considerando evidências científicas, diretrizes internacionais de segurança online e padrões de usabilidade ou design ético alinhados ao desenvolvimento de crianças e adolescentes”.

2. Conceitos ligados a funcionalidades de supervisão parental no ECA Digital

Sugere-se que, entre as funcionalidades de supervisão parental, esteja uma visão consolidada dos conteúdos publicados, mas com salvaguardas: apenas conteúdos publicados abertamente ou que a própria plataforma possa disponibilizar; com transparência para a criança/adolescente; com princípio da adequação etária (mais supervisão para crianças, mais privacidade para adolescentes). Diante disso, propõe-se a expansão do Art. 18, com o seguinte acréscimo:

“VII – acessar uma visão consolidada dos conteúdos publicados pela criança ou pelo adolescente no âmbito de aplicações e plataformas, de forma segura e proporcional à idade”.

3. Conceitos ligados a exposição vexatória, constrangedora e práticas que exploram humilhação, sofrimento emocional ou vulnerabilidades de crianças e adolescentes

Pontos críticos hoje em plataformas digitais envolvem conteúdos de desafio, “pegadinhas”, “humilhação pública” ou “conteúdos monetizados com sofrimento infantil”, por exemplo. Diante disso, deve-se evitar exploração não sexual, mas igualmente danosa, propondo-se a seguinte redação para o Art. 23:

“Art. 23. São vedados aos provedores de aplicações de internet a monetização, o impulsionamento, a recomendação ativa ou qualquer forma de amplificação algorítmica de conteúdos que:

I – retratam crianças ou adolescentes de forma erotizada, sexualmente sugestiva ou inseridos em contextos próprios do universo sexual adulto;

II – exponham crianças ou adolescentes a situações vexatórias, constrangedoras, humilhantes, degradantes, abusivas ou que explorem seu sofrimento físico ou emocional como forma de entretenimento, engajamento ou obtenção de vantagem econômica;

III – estimulem, promovam ou normalizem desafios, práticas, comportamentos ou encenações que coloquem em risco a saúde física ou mental de crianças e adolescentes, ainda que enquadrados como conteúdo humorístico, de competição ou recreação;

IV – utilizem imagens ou áudios de crianças ou adolescentes com finalidade de paródia, deepfake, remix, montagem ou recontextualização que possa resultar em exposição vexatória, discriminação, ridicularização ou violação de sua dignidade.

§1º O provedor deverá adotar mecanismos eficazes de detecção, moderação, resposta rápida e bloqueio de monetização para os conteúdos referidos neste artigo, inclusive quando gerados por inteligência artificial.

§2º A interpretação deste artigo observará os princípios da proteção integral, da prioridade absoluta, da dignidade da pessoa humana, da prevenção de danos digitais e da preservação do desenvolvimento saudável da criança e do adolescente.”.

Tomada de Subsídios da Agência Nacional de Proteção de Dados Conceitos do ECA Digital ([aqui](#))

A Samsung Eletrônica da Amazônia LTDA. ("**Samsung**"), respeitosamente, apresenta sua contribuição à tomada de subsídios de conceitos do ECA Digital.

Pergunta: Quais os principais conceitos, termos e expressões previstos no ECA Digital que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

- **Produto ou serviço de tecnologia da informação (art. 2º, I):** a definição legal é excessivamente ampla e heterogênea, podendo abarcar desde aplicações digitais destinadas ao usuário final até elementos de infraestrutura e funcionalidades técnicas essenciais ao funcionamento da internet, o que dificulta identificar com precisão quais atores e camadas tecnológicas estão sujeitos às obrigações da Lei. Há necessidade de esclarecer que o conceito deve recair prioritariamente sobre produtos e serviços cuja função principal envolva uma interface utilizada diretamente por crianças e adolescentes, sobre a qual o fornecedor tenha capacidade efetiva de influenciar funcionalidades, conteúdo ou tratamento de dados, distinguindo-se assim de componentes de *backend*, *firmware*, sistemas de conectividade, serviços de atualização, padrões técnicos e/ou funcionalidades digitais acessórias de bens físicos. A interpretação também deve se alinhar à lógica de proporcionalidade do art. 39, reconhecendo que obrigações diferentes decorrem do grau de intervenção e controle sobre a experiência digital e sobre a circulação de conteúdos acessíveis a menores, evitando que dispositivos multifuncionais, sistemas operacionais ou lojas de aplicativos sejam automaticamente responsabilizados por aplicações de terceiros instaladas nesses ambientes.
- **Acesso provável (art. 1º, parágrafo único):** mesmo com os critérios dos incisos I a III, o conceito permanece excessivamente vago e carece de critérios objetivos que permitam aos fornecedores avaliar, de forma previsível e proporcional, quando um produto ou serviço deve ser submetido ao regime da Lei. Sem esclarecimentos, os incisos I a III podem ser interpretados de maneira isolada e expansiva, bastando, por exemplo, a mera existência de algum risco residual para caracterizar acesso provável, o que geraria enquadramento excessivo de serviços que não são direcionados a menores e que adotam barreiras efetivas de acesso. Os termos usados pelo inciso I ("*suficiente probabilidade de uso e atratividade*") podem levar à conclusão equivocada quanto a dispositivos domésticos de uso compartilhado, como TVs, geladeiras e outros equipamentos conectados, que são usados por crianças não por apresentarem elementos de atratividade infantil, mas em virtude da presença no ambiente familiar. Já o inciso II ("*considerável facilidade de acesso e utilização*") também exige esclarecimentos, visto que a facilidade de uso é característica inerente à evolução tecnológica e atravessa todas as faixas etárias, especialmente diante do fato de que as crianças e adolescentes são nativos digitais; dessa forma, a avaliação de facilidade deve se concentrar no tipo de conteúdo acessível e, especialmente, no direcionamento do serviço, e não em características de usabilidade genéricas. Por fim, o inciso III ("*significativo grau de risco à privacidade, segurança ou desenvolvimento biopsicossocial*") demanda delimitação em relação ao que constitui esse risco, distinguindo riscos decorrentes de conteúdos potencialmente prejudiciais daqueles inerentes ao funcionamento de serviços legítimos. Para garantir segurança jurídica, a regulamentação deve explicitar que a análise deve ser integrada, considerando atratividade, facilidade de acesso e grau de risco à luz das salvaguardas existentes, de modo que apenas serviços nos quais haja, de forma combinada: (i) probabilidade relevante de uso por crianças e adolescentes ou facilidade material de acesso; e (ii) risco significativo não mitigado à privacidade, à segurança ou ao desenvolvimento biopsicossocial, sejam enquadrados. A regulamentação também deve permitir que fornecedores

demonstrem, com dados e controles técnicos (como classificação indicativa, verificação de idade, exigência de conta adulta, configuração padrão, barreiras de usabilidade, controles parentais), que o produto não apresenta acesso provável, garantindo segurança jurídica e evitando interpretações que ampliem indevidamente o escopo regulatório para aqueles sistemas, dispositivos ou serviços cuja experiência principal não é destinada a crianças ou adolescentes.

- **Conteúdo impróprio ou inadequado (art. 9º, *caput*):** a expressão é definida apenas pela referência genérica a material pornográfico e a outros conteúdos “vedados pela legislação vigente”, o que não fornece parâmetros suficientes para orientar fornecedores na identificação abrangente dos conteúdos que exigiriam mecanismos reforçados de verificação de idade. A ausência de critérios objetivos pode levar à interpretação inflacionada do conceito, especialmente em ecossistemas de dispositivos conectados e em plataformas que não exercem controle editorial sobre o conteúdo disponibilizado por terceiros. Embora o ECA Digital faça referência à adequação por faixa etária e classificação indicativa, não define **(i)** o que é considerado impróprio e/ou inadequado para cada faixa etária ou **(ii)** quais critérios ou categorias devem ser aplicados na avaliação. É necessário esclarecer que a caracterização de impropriedade ou inadequação deve estar vinculada às normas de classificação indicativa e a padrões já reconhecidos de risco ao desenvolvimento de crianças e adolescentes, evitando assim que conteúdos lícitos, educativos, jornalísticos ou contextuais sejam indevidamente enquadrados. Somado a isso, é importante diferenciar conteúdos cuja natureza é intrinsecamente proibida para menores (pornografia, violência extrema, jogos de azar) daqueles cujo impacto depende do contexto de uso, da idade e das configurações de supervisão parental, assegurando que obrigações reforçadas se concentrem em serviços que realmente disponibilizam ou recomendam conteúdos nocivos, e não em aplicativos ou lojas de aplicativos que atuam apenas como meios de acesso sem ingerência sobre o material veiculado. Assim, é necessário adotar como referência objetiva o novo sistema de classificação indicativa da Portaria MJSP nº 1.048/2025, que estabelece critérios específicos sobre inadequações por faixa etária, harmonizando o ECA Digital com a prática consolidada de classificação indicativa no Brasil.
- **Aferição de idade “a cada acesso” (art. 9º, §1º):** a exigência de verificação de idade a cada acesso gera insegurança técnica e operacional, sobretudo porque a Lei não esclarece se a verificação deve ocorrer a cada visita ao app, a cada sessão de uso, a cada tentativa de acesso a conteúdo sensível ou sempre que houver “suspeita” de uso por menores. É essencial esclarecer que a verificação a “cada acesso” não deve resultar em coleta reiterada ou excessiva de dados, nem procedimentos desproporcionais que comprometam a experiência do usuário ou a segurança da informação. A regulamentação deve permitir que fornecedores utilizem métodos alternativos e menos intrusivos (como sinal de idade do sistema operacional, controles parentais, perfis gerenciados, autenticação única ou verificações periódicas), evitando uma dupla verificação dentro do mesmo ecossistema. O próprio Ministério da Justiça e Segurança Pública, nos parágrafos 49 a 60 de sua Consulta Pública sobre Mecanismos de Aferição de Idade, destacou alguns desafios técnicos e econômicos relativos à verificação de idade, como o aumento de latência, fricção excessiva, riscos de evasão ou burla do mecanismo e prejuízo à usabilidade. Assim, é necessária interpretação mais precisa para evitar a criação de regime de verificação contínua, operacionalmente inviável, que poderia gerar riscos de privacidade e desincentivar o uso de soluções adequadas e proporcionais de proteção infantil. Além disso, deve-se especificar que a obrigação recai sobre o provedor que efetivamente disponibiliza o conteúdo, e não sobre fabricantes de dispositivos ou lojas de aplicativos, que não têm controle editorial sobre o conteúdo acessado.
- **Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais (art. 16, parágrafo único, II):** A Lei cria a obrigação de elaborar um relatório de impacto, de monitoramento

e de avaliação da proteção de dados pessoais, mas sem detalhar seu escopo, conteúdo mínimo, periodicidade e relação com outros instrumentos de governança de privacidade já exigidos para determinadas operações. Essa ausência de padronização poderá gerar duplicidade documental, insegurança jurídica e obrigações desproporcionais, especialmente para fornecedores que operam sistemas complexos com múltiplas camadas técnicas (como dispositivo, sistema operacional, lojas de aplicativos e aplicativos de terceiros). É necessário esclarecer: **(i)** se o relatório deve ser restrito aos tratamentos de dados que excedem o estritamente necessário à operação do produto ou do serviço; **(ii)** quais critérios de risco e quais parâmetros de “monitoramento” devem ser aplicados; **(iii)** qual a periodicidade da revisão; e **(iv)** como evitar conflitos ou sobreposições com o RIPD da LGPD, especialmente porque este já exige avaliação de riscos, salvaguardas e medidas mitigadoras. A interpretação sistemática e teleológica da legislação brasileira indica que o relatório mencionado no ECA Digital deve ser entendido como o próprio RIPD da LGPD, complementado pelas avaliações específicas exigidas para tratamentos que ultrapassem o estritamente necessário à operação do produto ou do serviço. Criar um novo relatório, sem integração com o RIPD já existente, implicaria alocação ineficiente de recursos e diminuiria a efetividade das salvaguardas, desviando esforços de mitigação de riscos reais para a produção de documentos substancialmente sobrepostos.

- **Rede social (art. 2º, III):** embora o conceito legal defina rede social como aplicação cuja “principal finalidade” é o compartilhamento e a disseminação de opiniões e informações entre usuários, não estão claros os critérios para distinguir serviços cujo propósito central é a interação social aberta daqueles que apenas contêm funcionalidades acessórias de comunicação. Dessa forma, para evitar interpretações expansivas que incluam plataformas voltadas primordialmente a suporte técnico, relacionamento com o cliente, assistência ao usuário e/ou serviços utilitários que não promovem interação social pública entre usuários, deve-se esclarecer que somente aplicações cuja essência seja a formação de redes sociais, o engajamento entre desconhecidos e a circulação orgânica ou algorítmica de conteúdo devem ser enquadradas nesse conceito. Serviços cuja finalidade principal é operacional, informativa ou de atendimento, ainda que permitam comentários, avaliações ou trocas limitadas, não atendem ao critério legal de finalidade social predominante e, portanto, não devem ser classificados como redes sociais.
- **Mecanismos de supervisão parental (art. 2º, inciso VIII):** o conceito abrange um conjunto amplo de configurações, ferramentas e salvaguardas tecnológicas, mas a Lei não define critérios mínimos, limites de responsabilidade ou grau de integração esperado entre diferentes níveis do ecossistema digital (dispositivo, sistema operacional, loja de aplicativos e serviços de terceiros). Esse cenário pode levar a obrigações desproporcionais a atores que não controlam o conteúdo, a experiência ou o tratamento de dados no serviço efetivamente utilizado pela criança. A regulamentação deve esclarecer que tais mecanismos devem recair prioritariamente sobre o fornecedor da aplicação ou serviço que interage diretamente com a criança ou adolescente, e não sobre camadas técnicas ou sobre plataformas cujo papel é meramente habilitador. Além disso, os requisitos detalhados nos arts. 17 e 18 precisam ser modulados conforme a efetiva capacidade técnica de cada ator e a natureza do produto ou serviço, evitando expectativas de supervisão universalizada ou integração completa entre serviços independentes.
- **Medidas proporcionais, auditáveis e tecnicamente seguras (art. 12, I):** a expressão não é definida pela Lei e pode gerar expectativa de implementação de mecanismos de verificação de idade e/ou salvaguardas técnicas com grau de robustez, interoperabilidade e/ou detalhamento incompatíveis com a realidade tecnológica de certos produtos e com o papel efetivamente desempenhado por cada ator do ecossistema digital. A ausência de critérios objetivos pode levar à interpretação de

que qualquer fornecedor, inclusive fabricantes de dispositivos e lojas de aplicativos, deverá adotar soluções igualmente sofisticadas ou integradas, independentemente de seu nível de ingerência sobre conteúdo, funcionalidades ou tratamento de dados. A fim de assegurar proporcionalidade e evitar a imposição de requisitos inviáveis ou que criem barreiras técnicas desnecessárias, deve-se definir parâmetros mínimos claros, diferenciando expectativas para serviços que controlam a experiência do usuário daqueles que apenas fornecem infraestrutura ou habilitam o acesso. Essas medidas devem considerar limitações técnicas reais, custos de implementação, riscos de perda de usabilidade, cumprimento de princípios da LGPD (como minimização de dados e transparência) e o potencial impacto de exigências de auditoria contínua, que podem ser viáveis tão somente para fornecedores que efetivamente determinam as finalidades e meios do tratamento.

- **Serviço com controle editorial (art. 2º, IX):** a definição não explicita os critérios operacionais que permitam distinguir uma curadoria ativa de conteúdo, baseada em seleção prévia e intervenção humana significativa, de modelos em que o provedor apenas disponibiliza, organiza ou transmite conteúdos previamente licenciados de agentes econômicos responsáveis. Essa lacuna é relevante porque o art. 39, § 1º prevê regime diferenciado não apenas para serviços com controle editorial, mas também para provedores de conteúdo protegido por direitos autorais licenciados, categoria que abrange serviços cuja função é disponibilizar ao público conteúdos selecionados e autorizados por titulares de direitos autorais, ainda que não realizem curadoria editorial própria. Para garantir segurança jurídica e coerência regulatória, é necessário esclarecer que os serviços estruturados a partir de catálogos licenciados, cuja oferta não depende de produção ou de moderação direta de conteúdo pelo provedor, mas de acordos contratuais com detentores de direitos, também podem ser enquadrados na hipótese do § 1º, desde que cumpram os requisitos de classificação indicativa, transparência e disponibilização de mecanismos técnicos de mediação parental. Tal interpretação está alinhada ao § 2º do art. 39, segundo o qual as obrigações devem ser moduladas pelo grau real de intervenção do fornecedor sobre a disponibilização, a circulação ou o alcance dos conteúdos, evitando impor obrigações desproporcionais aos serviços que atuam predominantemente como canais de distribuição de conteúdo licenciado.
- **Adesivo (art. 38):** a obrigação de inserir adesivo nas embalagens de equipamentos eletrônicos de uso pessoal informando a necessidade de proteger crianças e adolescentes do acesso a conteúdo impróprio ou inadequado carece de esclarecimentos quanto ao seu conteúdo mínimo, alcance e forma de implementação. A redação ampla pode levar a interpretações divergentes sobre: (i) quais dispositivos são considerados “de uso pessoal” – especialmente em contextos em que produtos multifuncionais, como smart TVs, tablets e dispositivos IoT, são utilizados por múltiplos membros da família; (ii) se o aviso deverá contemplar orientações genéricas e/ou referências a mecanismos específicos de supervisão parental; e (iii) como harmonizar a obrigação com a rotulagem existente, normas de segurança do consumidor e limitações de espaço físico. A ausência de definições claras, somada ao curto prazo para adaptação, impacta diretamente a cadeia produtiva e a logística de fabricantes de eletrônicos, gerando riscos de aumento de custo, redução de disponibilidade e até mesmo prejuízos ao consumidor final. Além disso, é importante que a regulamentação esclareça se o aviso deve necessariamente constar na embalagem física ou se pode ser cumprido por meios equivalentes, como manuais do usuário ou pop-ups acessíveis no momento da configuração inicial do dispositivo. Essa interpretação preserva a função informativa da norma, mas reduz os impactos logísticos e evita todo retrabalho na produção de embalagens, sem comprometer a efetividade da comunicação aos pais e responsáveis. Finalmente, é igualmente importante que a regulamentação esclareça que dispositivos de “uso coletivo” ou “acesso compartilhado” instalados em ambientes domésticos, como *smart TVs*, não se enquadram como “equipamentos eletrônicos de uso pessoal” para fins do art. 38. Por não serem atribuídos a um único usuário e por constituírem produtos de

acesso compartilhado por natureza, tais dispositivos não deveriam ser submetidos à obrigação de adesivagem, destinada a equipamentos capazes de proporcionar experiências individualizadas.

- **Produto de acesso compartilhado:** O ECA Digital não define esse conceito, embora seja essencial para delimitar obrigações relacionadas ao acesso provável por crianças e adolescentes. A ausência de definição é especialmente relevante para os dispositivos multifuncionais amplamente utilizados em ambientes familiares, como TVs, tablets, geladeiras conectadas, alto-falantes inteligentes e demais dispositivos IoT, que, por sua natureza, são instalados em espaços comuns e utilizados por múltiplos membros da família, inclusive crianças, de forma não individualizada. É fundamental, por esse motivo, que a regulamentação esclareça que tais dispositivos não constituem “equipamentos eletrônicos de uso pessoal”, uma vez que não são atribuídos a um único usuário e não viabilizam experiências digitais personalizadas que pressupõem titularidade individual. Sem essa delimitação, há risco de que TVs e os outros dispositivos domésticos venham a ser erroneamente classificados como produtos pessoais e sujeitos a obrigações desproporcionais, apesar de não haver controle sobre o conteúdo, interação social ou tratamento de dados realizados por serviços terceiros. O conceito de “produto de acesso compartilhado” deve, portanto, abranger dispositivos cujo uso coletivo decorre da própria finalidade do produto, garantindo segurança jurídica e modulando as responsabilidades conforme o nível real de controle exercido pelo fornecedor.

Atenciosamente,

Samsung e VLK Advogados

**MANIFESTAÇÃO TÉCNICA DA FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO
(FIESP) SOBRE A LEI Nº 15.211/2025 (ESTATUTO DIGITAL DA CRIANÇA E DO ADOLESCENTE)**

À Agência Nacional de Proteção de Dados (ANPD)

A Federação das Indústrias do Estado de São Paulo (FIESP) reconhece a importância de um marco legal para a proteção de crianças e adolescentes no ambiente digital e vem, portanto, por meio de seu Departamento de Defesa e Segurança (DESEG), respeitosamente, apresentar sua contribuição técnica à Tomada de Subsídios sobre a Lei nº 15.211/2025 (ECA Digital).

Considerando sua relevância, compreende-se que para que a lei seja eficaz, exequível e promova um ambiente de inovação responsável, é imperativo que seus termos e obrigações sejam claros e objetivos.

Assim, essa manifestação concentra-se na análise de 11 conceitos a fim de garantir a indispensável segurança jurídica, além da aplicação proporcional e razoável da norma, sobretudo em se considerando a abrangência de sua aplicabilidade e as particularidades individuais de cada setor pela nova lei alcançado.

1. Acesso provável (Art. 1º, Parágrafo único)

A lei condiciona sua aplicação ao "acesso provável" por crianças e adolescentes, definindo-o a partir de três situações de elevada subjetividade: (I) "suficiente probabilidade de uso e atratividade"; (II) "considerável facilidade ao acesso e utilização"; e (III) "significativo grau de risco". Os qualificadores "suficiente", "considerável" e "significativo" são vagos, não oferecem um critério objetivo e transferem um ônus interpretativo desproporcional às empresas, que não têm como aferir com segurança se seus serviços se enquadram na norma.

Proposta de parâmetro:

- ✓ Probabilidade de uso: aferida com base em dados empíricos comprováveis, tais como perfil etário majoritário de usuários, conteúdo explícito direcionado a crianças, campanhas publicitárias orientadas ao público infantojuvenil, e não estimativas genéricas.
- ✓ Facilidade de acesso: sugere-se que o critério não seja vinculado à mera possibilidade de acesso por ausência de barreiras tecnológicas.
- ✓ Grau de risco: aferido de forma objetiva e mensurável, com base no tipo de dado tratado, natureza do serviço e modelo de interação entre usuários.

2. Acesso possível

O termo "acesso possível", embora não definido explicitamente em contraste com "acesso provável", permeia a interpretação da lei e gera incerteza, posto que se tem observado uma confusão recorrente, inclusive em veículos de imprensa, consultorias e pareceres técnicos entre **o que é "acesso possível"** (qualquer serviço pode, em tese, ser acessado por uma criança) e **o que é "acesso provável"** (quando o acesso se mostra previsível, **frequente** ou atraído por elementos do serviço).

Essa confusão conceitual tem levado à interpretação equivocada de que qualquer serviço acessível via internet estaria automaticamente sujeito ao regime mais rígido da lei, o que **desvirtua o critério de proporcionalidade** previsto no próprio texto legal.

Proposta de parâmetro:

A regulamentação deve esclarecer que:

- ✓ “Acesso possível” é um conceito amplo e irrestrito e que qualquer serviço conectado está potencialmente ao alcance de uma criança.
- ✓ “Acesso provável” demanda previsibilidade, indícios concretos e evidências objetivas de que crianças e adolescentes, na prática:
 - (a) acessam com frequência;
 - (b) procuram aquele tipo de serviço;
 - (c) são atraídos por elementos temáticos, estéticos ou funcionais;
 - (d) formam uma parte relevante da audiência;
 - (e) são alvo direto ou indireto de estratégias de comunicação.

3. Atratividade (Art. 1º, Parágrafo único, I)

Sendo um dos componentes do "acesso provável", a "atratividade" é um conceito particularmente subjetivo. A mera utilização de cores vibrantes, design lúdico ou elementos de gamificação em um serviço destinado ao público adulto poderia, por si só, ser interpretada como "atratividade" para crianças?

Proposta de parâmetro:

- ✓ A análise de atratividade deve se basear em um conjunto de fatores concretos e intencionais, e não em elementos estéticos isolados. Sugerimos que a ANPD considere como critérios: (a) o tema e o conteúdo principal do serviço serem manifestamente infantis; (b) o uso de linguagem, personagens, celebridades ou trilhas sonoras licenciadas do universo infantil; e (c) evidências de marketing e publicidade direcionados a esse público. A intenção do fornecedor deve ser um fator preponderante.

4. Medidas razoáveis (Art. 6º)

O Art. 6º exige que fornecedores adotem "medidas razoáveis" para prevenir e mitigar uma lista de riscos. "Razoável" é um padrão jurídico clássico, mas sem critérios mínimos tende a gerar incerteza e subjetividade de interpretação, sobretudo por que o que é razoável para uma startup de 10 pessoas é drasticamente diferente do que é razoável para uma plataforma global com milhares de moderadores.

Proposta de parâmetro:

- ✓ É preciso definir um padrão de diligência esperado, escalonado pelo porte da empresa e pelo nível de risco do serviço, estabelecendo um parâmetro para que comprovem a adesão a um framework de gerenciamento de riscos, que poderia incluir a realização e a apresentação de relatórios de avaliações de impacto, a implementação de medidas de mitigação proporcionais, além da manutenção de canais de denúncia eficazes. O foco deve ser na comprovação de processos, não na garantia de resultados infalíveis, o que nunca haverá.

5. Medidas adequadas (Art. 3º)

De forma similar, o Art. 3º exige "medidas adequadas e proporcionais" para assegurar um nível elevado de privacidade e segurança. O termo "adequadas" é tão subjetivo quanto "razoáveis" e carece de um padrão técnico mínimo que sirva de referência para as empresas.

Proposta de parâmetro:

- ✓ É preciso traduzir "medidas adequadas" em um catálogo de controles técnicos e organizacionais mínimos, também de forma escalonada por risco e porte. Por exemplo: para serviços de baixo risco, "medidas adequadas" poderiam significar a implementação de uma política de privacidade clara e configurações padrão protetivas. Para serviços de alto risco, poderiam incluir criptografia de ponta-a-ponta, autenticação multifator e auditorias de segurança periódicas.

6. Exploração comercial (Art. 4º, VI)

A lei estabelece como fundamento a "proteção contra a exploração comercial", mas não define o que constitui o termo "exploração", o que pode levar a dúvida: Será que toda e qualquer forma de monetização ou publicidade digital que envolva crianças e adolescentes poderia ser questionada ou interpretada como "exploração"? Surge, por exemplo, a necessidade de esclarecer se práticas amplamente utilizadas e juridicamente permitidas, como publicidade contextual, venda de produtos licenciados ou a atuação profissional legítima de adolescentes como influenciadores, estariam ou não compreendidas nesse conceito.

Proposta de parâmetro:

- ✓ Importante delimitar o conceito de "exploração comercial", vinculando-o a práticas abusivas e predatórias, e não a modelos de negócio legítimos. A regulamentação poderia focar em proibir práticas que: (a) se aproveitem da hiper vulnerabilidade e da deficiência de julgamento da criança para induzir compras; (b) criem pressão psicológica para o consumo; (c) utilizem mecânicas enganosas para promover produtos ou serviços; ou (d) exponham crianças a publicidade de produtos inadequados (álcool, tabaco, etc.).

7. Uso compulsivo (Art. 8º, IV)

A exigência de desenvolver configurações que "evitem o uso compulsivo" pode estar entre as mais problemáticas da lei, uma vez tratar-se de um diagnóstico clínico/psicológico, cuja aferição e prevenção extrapolam a capacidade e a responsabilidade de um fornecedor de tecnologia, o que torna impossível para uma empresa determinar o que constitui uso "compulsivo" para cada indivíduo, pois isso depende de fatores pessoais, sociais e de saúde mental.

Proposta de parâmetro:

- ✓ A obrigação precisa ser reformulada do dever de "evitar" para o dever de "disponibilizar ferramentas que promovam o bem-estar digital e o uso consciente", substituindo uma meta inatingível por outra que ofereça recursos como: (a) painéis de controle de tempo de uso; (b) alertas e lembretes configuráveis para pausas; (c) opções para limitar notificações; e (d) modos de "não perturbe". O foco deve ser em empoderar o usuário e seus responsáveis, e não em atribuir uma responsabilidade de diagnóstico ao provedor.

8. Desenvolvimento progressivo (Art. 7º)

A lei determina que as configurações de privacidade devem considerar o "desenvolvimento progressivo do indivíduo", um princípio fundamental do Estatuto da Criança e do Adolescente, mas que cuja aplicação prática no ambiente digital carece de parâmetros. A partir de que idade um adolescente pode ter mais autonomia para configurar sua privacidade? Como uma plataforma pode aferir o nível de maturidade de cada usuário para conceder-lhe mais ou menos controle?

Proposta de parâmetro:

- ✓ A ANPD deve estabelecer faixas etárias como referência para a aplicação do princípio. Por exemplo, poderia ser criada uma “presunção relativa” de que: (a) crianças (até 12 anos) devem estar sob um regime de proteção máxima, com controles parentais mandatórios; (b) adolescentes mais jovens (13-15 anos) teriam um regime intermediário, com maior autonomia, mas ainda com forte supervisão parental e configurações padrão protetivas; e (c) adolescentes mais velhos (16-17 anos) teriam autonomia para configurar sua experiência, mantendo-se a possibilidade de supervisão e o acesso a ferramentas de segurança, criando assim um padrão mais previsível para as empresas.

9. Mecanismos confiáveis (Art. 9º)

A exigência de "mecanismos confiáveis de verificação de idade", vedando a autodeclaração, é sem dúvida, um dos maiores desafios da lei, mas é preciso começar esclarecendo o que pode ser considerado um mecanismo "confiável". A falta de definição deixa as empresas entre o risco de adotar uma solução considerada insuficiente pela fiscalização e o risco de violar a privacidade dos usuários com métodos excessivamente invasivos.

Proposta de parâmetro:

- ✓ É preciso adotar um enfoque baseado em risco, ou seja, a robustez do mecanismo de verificação deve ser proporcional ao risco do conteúdo ou serviço. Além disso, a ANPD poderia fomentar e certificar soluções que garantam a privacidade desde a concepção (privacy by design), como sistemas de atribuição de idade (que apenas confirmam se o usuário é maior ou menor de idade, sem revelar a data de nascimento) e o uso de sinais de idade via API de terceiros confiáveis (setor financeiro, governo), minimizando a coleta de dados pelas plataformas.

10. A cada acesso (Art. 9º, §1º)

O art. 9º, §1º da Lei determina que sejam adotados mecanismos confiáveis de verificação de idade “a cada acesso” do usuário ao conteúdo, produto ou serviço, vedada a autodeclaração. A redação do dispositivo, tal como está, suscita dúvidas relevantes quanto ao tipo de “acesso” que exige verificação e à frequência com que esses mecanismos devem ser acionados ao longo da jornada do usuário.

Proposta de parâmetro:

- ✓ Diante disso, propõe-se que a ANPD esclareça que a expressão “a cada acesso” deve ser interpretada de forma material e não meramente técnica, no seguinte sentido: “Acesso” não deve abarcar indiscriminadamente todos os eventos técnicos (como simples

abertura do aplicativo ou carregamento de tela), mas sim momentos relevantes da jornada, de forma alternativa. Por exemplo, no cadastro ou criação de conta; no acesso a categorias de produtos sujeitas a restrição etária; OU no momento de checkout ou conclusão da transação relativa a tais produtos, no caso de comércio eletrônico. A exigência de verificação plena de idade em absolutamente todos os acessos técnicos implicaria em custos operacionais e tecnológicos elevados, sobretudo quando envolvem integrações com terceiros; aumento substancial de fricção na experiência do usuário; e um volume de tratamento de dados pessoais desproporcional aos objetivos perseguidos.

11. Vedada a autodeclaração (Art. 9º, §1º)

O ECA Digital não define “autodeclaração” em seu art. 2º, nem em qualquer outro dispositivo, o que gera incerteza quanto ao alcance da proibição. A finalidade da vedação é impedir mecanismos manifestamente ineficazes. A proibição deve ser entendida como vedação ao ato unilateral e não validado pelo qual o usuário declara sua idade, sem elemento externo de confiabilidade.

Considerações finais:

A segurança jurídica é condição indispensável para a efetividade da Lei nº 15.211/2025 e acreditamos que a regulamentação dos onze conceitos aqui analisados representa um passo importante para transformar um texto de intenções legítimas em um marco regulatório claro, previsível e exequível, capaz de promover um ambiente digital mais seguro sem comprometer a inovação, a competitividade e o desenvolvimento da indústria brasileira.

Esperamos que os parâmetros sugeridos contribuam de forma objetiva para o trabalho da ANPD, oferecendo esclarecimentos que permitam às empresas de todos os portes e setores compreenderem com precisão suas obrigações legais e investirem em conformidade de maneira proporcional, eficaz e tecnicamente fundamentada.

A FIESP reafirma seu compromisso institucional com a proteção integral de crianças e adolescentes no ambiente digital e permanece à disposição para colaborar na construção de um ecossistema regulatório sólido, equilibrado e tecnicamente consistente.

Respeitosamente,

Federação das Indústrias do Estado de São Paulo (FIESP)



SUBMISSÃO DA FUNDAÇÃO WIKIMEDIA À TOMADA DE SUBSÍDIOS DA ANPD PARA ESCLARECER CONCEITOS DO ECA DIGITAL

Introdução

A Fundação Wikimedia (WMF) agradece a oportunidade de participar da Tomada de Subsídios para esclarecer conceitos do ECA Digital, como desdobramento da aprovação da Lei 15.211. Embora os esforços do Brasil para criar uma internet mais segura para crianças e adolescentes sejam louváveis, as disposições da lei devem ser aplicadas de maneira proporcional, de modo a não afetar excessivamente os pequenos e médios provedores de forma negativa. Continuamos preocupados com o fato de que algumas exigências afetam desproporcionalmente projetos sem fins lucrativos e comunitários, bem como plataformas de bens públicos digitais, impondo obrigações de compliance incompatíveis com suas funcionalidades e que podem ter profundas implicações em termos de segurança de dados e privacidade.

A Fundação Wikimedia é uma organização sem fins lucrativos que hospeda a Wikipédia e outros projetos de conhecimento livre.¹ Nossa visão é um mundo onde todos os seres humanos possam compartilhar livremente a soma de todo o conhecimento. Para isso, apoiamos uma comunidade vibrante de mais de 260.000 voluntários em todo o mundo, que contribuem para os projetos da Wikimedia adicionando, editando e verificando conteúdo em mais de 63 milhões de artigos em mais de 300 idiomas.

Projetos como a Wikipédia têm uma comunidade ativa e significativa presença e popularidade no Brasil. Eles atraem entre 250 milhões e 500 milhões de visitas por mês no país, com um total de 394 milhões de acessos somente no mês passado. A Wikipédia em português tem aproximadamente 8.000 a 9.000 editores ativos por mês, cada um contribuindo com uma média de 150 edições.

A questão apresentada para esta tomada de subsídios foi: “*Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de*

¹ É importante ressaltar que a WMF tentou, mas não conseguiu, submeter essa resposta à Tomada de Subsídios da ANPD na aba dedicada a “estrangeiros”. Para garantir que os argumentos da WMF fossem apreciados pelo órgão regulador, essa submissão foi realizada por um de seus prestadores de serviços que atualmente reside no Brasil.

setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?” Em relação à resposta, os principais conceitos da lei que requerem esclarecimentos adicionais podem ser encontrados em seu artigo 39, caput, e seus parágrafos 2 e 3, que afirmam:

Art. 39. As obrigações previstas nos arts. 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 desta Lei aplicar-se-ão conforme as características e as funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o **grau de interferência** do fornecedor do produto ou serviço sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor. (...)

§2 As obrigações referidas no caput deste artigo serão **aplicadas de forma proporcional** à capacidade do fornecedor de influenciar, de moderar ou de intervir na disponibilização, na circulação ou no alcance dos conteúdos acessíveis por crianças e adolescentes.

§3 A regulamentação definirá critérios objetivos para a aferição do **grau de intervenção** e para a aplicação proporcional das obrigações previstas neste artigo. **(Destacado)**

A chave para a aplicação adequada da lei é compreender qual é o “grau de interferência” e o “grau de intervenção” que o regulador irá considerar ao aplicar as suas disposições e o que entende por “aplicadas de forma proporcional”. O ECA Digital está correto ao afirmar que nem todos os produtos ou serviços de tecnologia da informação devem ter o mesmo grau de interferência sobre o conteúdo hospedado nas suas plataformas, nem que seja necessário o mesmo grau de intervenção por parte do regulador. Portanto, o que é necessário esclarecer melhor é como o regulador irá classificar os diferentes tipos de provedores, os critérios que utilizará para fazê-lo e como a lei será aplicada a cada categoria de provedor.

O ECA Digital não deve tratar todas as plataformas online como idênticas. Em vez disso, deve reconhecer que as plataformas diferem entre si em termos de finalidade, governança e perfil de risco. A totalidade dos requisitos impostos pela lei não deve ser aplicada sem alguma mitigação a sites de baixo risco, educacionais e de interesse público que beneficiem menores, um argumento que a WMF levantou em sua contribuição à recente consulta pública do Ministério da Justiça sobre verificação de idade. A aplicação do princípio da proporcionalidade aos requisitos impostos pela lei estaria alinhada com os princípios mais amplos já reconhecidos pelo ECA Digital e pelos votos dos ministros do STF na recente ação que questionou a constitucionalidade

do artigo 19 do Marco Civil da Internet. Isso garantiria que as obrigações variassem de acordo com a finalidade, o interesse público, o público-alvo e as práticas de governança de dados de cada plataforma.

1. Evitar impor um modelo de compliance homogêneo

Diferentes plataformas online têm arquiteturas e sistemas de governança distintos para moderar o conteúdo e o comportamento de seus usuários, bem como riscos únicos associados a elas. Ainda que não seja aplicável às obrigações de verificação de idade, o ECA Digital alude, no artigo 39, § 2, ao reconhecimento das diferenças na funcionalidade de cada plataforma em relação à maioria de suas obrigações.

O artigo 1º do ECA Digital² estabelece que a lei se aplica a todos os produtos ou serviços de tecnologia da informação que sejam (1) atraentes para menores, (2) facilmente acessíveis por menores ou (3) representem riscos à privacidade, segurança ou ao seu desenvolvimento psicossocial, especialmente quando permitem interação e compartilhamento em grande escala. Interpretada literalmente, essa definição é ampla o suficiente para abranger sites de interesse público como a Wikipédia, mesmo que seus objetivos e modelos operacionais sejam fundamentalmente diferentes de sites voltados especificamente para usuários menores de idade. O contexto mais amplo em que essa lei se insere também não deve ser esquecido. O ECA Digital coexistirá com outras leis que pretendem regulamentar a internet de alguma forma: desde o próprio Estatuto da Criança e do Adolescente até o Código de Defesa do Consumidor, e especialmente o Marco Civil da Internet.

O Ministro André Mendonça, em seu voto divergente na recente decisão do STF sobre a constitucionalidade do artigo 19 do Marco Civil, destacou sobre a Wikipédia que “o sítio eletrônico se organiza em torno da moderação realizada pelos próprios usuários, os quais, inquestionavelmente, possuem maior condição de atestar a higidez da informação inserida, dada a natureza enciclopédica da plataforma”. Isso significa que “ponderam os responsáveis pela plataforma sua peculiar dificuldade em moderar o conteúdo nela veiculado de modo direto, ou seja, sem o envolvimento e atuação da comunidade de autores coletivamente organizada”.³

² Artigo 1º da Lei 15.211 “ECA Digital”.

³ RE 1037396 / SP - par 161-163, p. 544.

No entanto, há espaço para interpretar o ECA Digital de forma mais proporcional e considerar modelos comunitários, como o da Wikipédia. Conforme mencionado acima, isso significa que todo o conteúdo (imagens, resumos de filmes, datas, biografias, etc.) nos projetos da Wikimedia é totalmente adicionado, modificado e revisado em primeiro lugar pelos usuários da plataforma. A própria Fundação Wikimedia não adiciona nem faz a curadoria de nenhum conteúdo visto pelos usuários nos sites, intervindo apenas quando algo é manifestamente ilegal. A ANPD deve levar em consideração estruturas como a da Wikipédia ao estabelecer suas categorias de provedores, pois esses são modelos que interferem menos no conteúdo de seus sites e que merecem um grau de intervenção substancialmente reduzido.

A ANPD deve aplicar os princípios de proporcionalidade existentes à interpretação do ECA Digital. Essa lei já reconhece que há situações em que o interesse público e a proporcionalidade devem ser ponderados em sua aplicação. O artigo 35, por exemplo, estabelece critérios para determinar sanções de acordo com os princípios de proporcionalidade e razoabilidade, e caso a caso.⁴ Uma interpretação razoável deste artigo é que ele reconhece que medidas desproporcionais podem prejudicar projetos de interesse público e suas comunidades. Como visto acima, o mesmo princípio de proporcionalidade na compreensão da funcionalidade de cada plataforma é mencionado no artigo 39. Uma interpretação holística e contextual que considere tanto a intenção da lei quanto a jurisprudência recente evitaria excessos e alinharia a aplicação da lei com o objetivo declarado do ECA Digital de proteger menores, em vez de sobrecarregar projetos educacionais ou comunitários de baixo risco.

O Ministro Barroso, em seu voto no recente caso relacionado ao Marco Civil, enfatizou a importância de evitar a censura indevida e a necessidade de proteger a liberdade de expressão ao defender a continuação da aplicação do artigo 19 a provedores “neutros ou com baixa interferência sobre a circulação de conteúdos de terceiros, que não são abrangidos pela decisão, como provedores de e-mail, reuniões fechadas e enciclopédias colaborativas.”⁵ Esses provedores “neutros” devem estar sujeitos a um regime mais brando, pois “não interferem substancialmente na circulação de conteúdo”, uma vez que as premissas que fundamentam tanto o caso do STF

⁴ Artigo 35, §1º, da Lei 15.211 “ECA Digital”. “Para fixação e gradação da sanção, deverão ser observadas, além da proporcionalidade e da razoabilidade, as seguintes circunstâncias (...)”.

⁵ RE 1037396 / SP - par 99, p. 415.

quanto o ECA Digital “não se aplicam a eles”.⁶

É evidente que tanto a decisão judicial quanto a lei não tinham como alvo plataformas de interesse público, como a Wikipédia. Leis e regulamentações promulgadas com as melhores das intenções podem, às vezes, levar a consequências prejudiciais, incluindo a restrição da liberdade de expressão e da participação em espaços online. A Fundação Wikimedia até mesmo desenvolveu o [Teste da Wikipédia](#) como uma ferramenta para ajudar os legisladores a identificar se uma proposta ou projeto de lei “facilitaria ou dificultaria a leitura, a contribuição e/ou a confiança em um projeto como a Wikipédia”.

A aplicação homogênea do ECA Digital a todos os tipos de provedores de aplicativos da internet seria prejudicial para o ecossistema online em geral. É fundamental, portanto, que a ANPD identifique e distinga quais tipos de serviços representam um risco para seus usuários e aqueles que contribuem para o seu desenvolvimento e para a sociedade em geral.

2. Distinguir entre perfis de risco e criar uma exceção para plataformas educacionais e de interesse público.

Os riscos associados às redes sociais com fins lucrativos diferem significativamente daqueles apresentados por plataformas educacionais e sem fins lucrativos em sua natureza, magnitude, probabilidade e impacto potencial. A quantidade de interferência desses tipos de plataformas no conteúdo hospedado nelas tende a ser mínima, justificando uma menor necessidade de intervenção por parte da agência reguladora.

Em 2024, a Fundação publicou um relatório independente de Avaliação de Impacto sobre os Direitos da Criança ([Child Rights Impact Assessment Report](#)) para cumprir nosso compromisso de proteger os direitos humanos de todos os indivíduos que interagem com os projetos da WMF. O relatório destaca que o modelo organizacional da Wikimedia não apresenta os mesmos riscos que uma plataforma com fins lucrativos. Por exemplo, ela não se envolve em publicidade direcionada nem coleta ou monetiza dados de crianças. Este relatório também confirma que os processos existentes liderados pela comunidade para identificar e remover a rara ocorrência de material de abuso sexual infantil (child sexual abuse material - CSAM) são altamente eficazes.

⁶ RE 1037396 / SP - par 127, p. 424.

Como a plataforma não possui mensagens privadas, todas as conversas se concentram na construção da enciclopédia e seu conteúdo existente. Qualquer comunicação entre usuários, seja em tópicos ou de outra forma, é publicada e visível publicamente, de modo que comportamentos predatórios privados não podem ocorrer na plataforma Wikimedia. Reconhecer esses perfis de risco distintos é essencial para elaborar uma regulamentação proporcional e eficaz. Aplicar os requisitos gerais do ECA Digital em todas as plataformas, independentemente de sua natureza ou finalidade, poderia restringir acidentalmente o acesso a recursos educacionais e cívicos valiosos.

A ANPD poderia desenvolver seu próprio sistema de categorização para interpretar e aplicar essa lei, o que proporcionaria clareza sobre como ela poderia ser interpretada para diferentes tipos de plataformas. O Comitê Gestor da Internet no Brasil (CGI.br) preparou uma [proposta preliminar](#) para a tipologia dos provedores de aplicativos da internet, utilizando como critério para distinguir cada um deles o nível de interferência/neutralidade do provedor em relação à circulação do conteúdo hospedado, o que poderia ser um ponto de partida útil para a ANPD considerar.

Isso é particularmente importante para iniciativas abertas e sem fins lucrativos que atendem ao interesse público e são reconhecidas como Bens Públicos Digitais. As Nações Unidas definiram os [Bens Públicos Digitais \(DPGs\)](#) como “software de código aberto, dados abertos, modelos de IA abertos, padrões abertos e conteúdo aberto que cumprem as leis de privacidade e outras leis aplicáveis e as melhores práticas, não causam danos e promovem os Objetivos de Desenvolvimento Sustentável”. Esses recursos desempenham um papel crucial na expansão do acesso à educação, na promoção do compartilhamento de conhecimento e na viabilização da inovação.

Dada a sua missão de interesse público e natureza não comercial, os DPGs deveriam ou ser isentos da lei ou colocados no “nível” mais baixo possível no que diz respeito ao “grau de interferência” no conteúdo dos projetos e ao “grau de intervenção” que o regulador exerceria. Tais isenções são consistentes com o princípio da proporcionalidade e essenciais para salvaguardar o direito fundamental à liberdade de expressão e ao acesso à informação sem barreiras desnecessárias. Essas isenções poderiam ser formuladas para:

- I. Serviços de enciclopédia
- II. Serviços educacionais
- III. Plataformas de interesse público
- IV. Plataformas que não se envolvem em práticas especificamente prejudiciais ao consumidor (ou seja: publicidade direcionada, coleta de dados em grande escala ou venda)

Para DPGs como os projetos da Wikimedia, devido à sua própria natureza, um nível de “menor interferência” seria o mais adequado. Conforme mencionado acima, o conteúdo é adicionado à plataforma diretamente por seus usuários. A Fundação interfere muito pouco no que é exibido e não faz uso de curadoria algorítmica, sem padrões obscuros e sem editorialização. Assim, a capacidade da Fundação de “influenciar, de moderar ou de intervir na disponibilização, na circulação ou no alcance dos conteúdos”⁷ é incrivelmente baixa em comparação com outras plataformas. Como o conteúdo dos projetos da Wikimedia é de natureza educacional e enciclopédica, há poucas chances de que sejam adicionados materiais inadequados para crianças e adolescentes. Nas raras ocasiões em que esse tipo de conteúdo é encontrado, [medidas são tomadas rapidamente](#), o conteúdo é removido e as contas infratoras são bloqueadas e denunciadas.

Conclusão

A missão da Fundação Wikimedia está profundamente enraizada no direito à participação no conhecimento e na cultura livres, e elogiamos os esforços do Brasil para garantir uma experiência segura na internet para todos. A WMF insta a ANPD a levar em consideração os diferentes “graus de interferência” que cada tipo de provedor exerce sobre o conteúdo em suas plataformas para determinar o “grau de intervenção” apropriado para cada um. Essa é a única maneira de garantir que a lei seja “aplicada de forma proporcional” às suas respectivas capacidades. O ECA Digital pode ser uma oportunidade para o governo proteger e promover um ecossistema de informação diversificado que apoie projetos sem fins lucrativos de interesse público e a tomada de decisões com base na comunidade, ao mesmo tempo em que protege a privacidade e os direitos de crianças e adolescentes.

⁷ Artigo 39, §2º, da Lei 15.211 “ECA Digital”.



Ref.: Tomada de Subsídios da ANPD para esclarecer conceitos do ECA Digital

A **Associação Brasileira de Medicina Diagnóstica – ABRAMED** apresenta a seguir as suas propostas de contribuições à Tomada de Subsídios para esclarecer conceitos do ECA Digital, promovida pela Agência Nacional de Proteção de Dados (ANPD).

#	Conceitos selecionados	ECA Digital
1.	Fornecedores de produtos ou serviços de tecnologia da informação com “ <i>acesso provável</i> ”	Art. 1º, parágrafo único
2.	“ <i>Perfilamento</i> ” para publicidade comercial	Art. 2º, V c/c art. 22 e 26
3.	Tratamento dos dados pessoais de crianças e de adolescentes de forma que “ <i>cause, facilite ou contribua</i> ” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei	Arts. 2º, V, 22 e 26
4.	Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser “ <i>utilizados unicamente para essa finalidade</i> ”	Art. 13
5.	Mecanismos de Supervisão Parental	Arts. 2º, VIII, art. 12, III e art. 16 e ss
6.	Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais	Art. 16, parágrafo único, II
7.	Verificação de idade “ <i>a cada acesso</i> ” do usuário ao conteúdo, produto ou serviço	Art. 9º, §1º
8.	Autonomia progressiva	Art. 10
9.	Mecanismos de notificações acerca de violações aos direitos de crianças e adolescentes	Art. 28, caput e art. 29, §3º
10.	Ofício às autoridades competentes	Art. 28, parágrafo único e 29, §2º

1. Fornecedores de produtos ou serviços de tecnologia da informação com “*acesso provável*”¹

a) Proposta: entendemos como necessária uma interpretação que requeira a cumulação de todos os requisitos previstos no parágrafo único do art. 1º, do ECA Digital, ou seja, é importante delimitar a abrangência da expressão “acesso provável por crianças e adolescentes” para que ela seja definida pelos critérios elencados no artigo e que devem ser considerados cumulativos. Assim seja, a “suficiente probabilidade de uso e atratividade”, a “considerável facilidade ao acesso e utilização” e o “significativo grau de risco”, como expressa a literalidade do texto, devem ser lidos cumulativamente para que o “acesso provável” esteja caracterizado. Além disso, é necessário definir com critérios objetivos o enquadramento nos incisos I e II.

b) Fundamento:

¹ Art. 1º, parágrafo único, ECA Digital.



A conceituação de “*acesso provável*”, prevista no parágrafo único do art. 1º, do ECA Digital, é excessivamente abrangente. Caso seja interpretada de forma literal, tal definição tende a incluir, para todos os fins, praticamente toda e qualquer aplicação de internet, tornando ineficaz a própria criação da categoria (“**serviços de tecnologia da informação com *acesso provável***”), o que não parece refletir a intenção do legislador.

O inciso I refere-se à “*suficiente probabilidade de uso e atratividade*”, mas utiliza terminologia genérica, desprovida de critérios objetivos capazes de orientar a interpretação do que efetivamente configuraria tal situação. Dessa forma, mostra-se necessária a previsão de parâmetros mensuráveis que permitam uma aplicação uniforme e verificável da norma, garantindo segurança jurídica.

Isso é especialmente relevante, considerando que interesses podem alterar-se significativamente entre as gerações. Por exemplo, a Geração Z possui interesse por questões religiosas superior ao da geração de seus pais², não existindo clareza no normativo se isso por si só tornaria páginas sobre essa temática de uso “*suficientemente provável por crianças e adolescentes*”.

Além disso, o conceito legal de “*crianças e adolescentes*” abrange uma faixa etária bastante ampla. Indivíduos situados no limite superior dessa faixa, por exemplo, entre 16 e 18 anos incompletos, possuem, em regra, interesses e comportamentos digitais muito próximos aos de adultos, especialmente jovens adultos. Aplicado isoladamente, o critério do inciso I tende, portanto, a abranger indiscriminadamente todo e qualquer produto ou serviço ofertado no ambiente virtual.

O inciso II estabelece como requisito a “*considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes*”. No entanto, considerando que vivemos em uma sociedade marcada por nativos digitais, muitas vezes mais aptos a utilizar tecnologias do que seus próprios responsáveis legais, a maior parte dos serviços digitais pode ser facilmente acessada e utilizada por menores.

Dessa forma, na falta de tal interpretação no sentido aqui proposto, existiria um enquadramento praticamente absoluto na categoria, excetuando-se apenas os casos em que existem barreiras artificiais robustas, sejam econômicas (ex.: cobrança de valores elevados para acesso) ou tecnológicas (ex.: processos rigorosos de verificação de idade), capazes de impedir ou dificultar significativamente o acesso de menores.

Tais barreiras, contudo, não estão presentes na ampla maioria das aplicações de internet. Demandá-las geraria entraves significativos para a economia de rede e para o próprio fluxo informacional, afetando, de modo desproporcional, especialmente os grupos mais vulneráveis, que já enfrentam dificuldades no acesso à internet, inclusive por falta de conhecimento. A título ilustrativo, segundo a Pesquisa Nacional por Amostra de Domicílios Contínua, 46% dos não

² Disponível em: <https://guiame.com.br/gospel/noticias/estudo-geracao-z-e-millennials-superam-geracoes-mais-velhas-na-frequencia-igreja.html>



usuários da internet no Brasil (equivalentes a 12% da população) deixam de utilizá-la justamente por não saberem como fazer isso³.

Diante do exposto, embora não se trate de uma leitura estritamente literal do dispositivo, entendemos que a interpretação teleológica da lei, que pressupõe uma distinção real entre serviços de tecnologia da informação de “*acesso provável*” e aqueles que não o são, exige que os critérios previstos no parágrafo único sejam satisfeitos de forma cumulativa. Caso contrário, a distinção será ineficaz, resultando, na prática, no enquadramento de todo e qualquer serviço da sociedade da informação.

2. “*Perfilamento*” para publicidade comercial⁴

a) **Proposta:** entendemos como necessária uma interpretação que limite o teor do escopo de perfilamento previsto no inciso V, do art. 2º, de modo que não abarque perfis não-intrusivos, como meros perfis demográficos, sobretudo para aplicação do art. 22.

b) **Fundamento:**

O art. 22 da Legislação estabelece uma proibição genérica à utilização de técnicas de perfilamento para práticas publicitárias comerciais envolvendo menores. No entanto, sua interpretação literal resultaria em uma restrição desproporcional, além de se mostrar em desacordo com a intenção aparente do legislador, que no art. 26 veda especificamente a criação de perfis comportamentais, e não a de quaisquer perfis.

A vedação absoluta ao perfilamento poderia, por consequência, impedir até mesmo direcionamentos publicitários baseados exclusivamente em perfis cadastrais, os quais são, por natureza, não intrusivos, vez que se baseiam em dados cadastrais básicos. No âmbito da saúde, por exemplo, informações cadastrais básicas podem possibilitar a divulgação de serviços voltados ao interesse do próprio menor, como campanhas de vacinação, orientações preventivas ou recomendações de exames pertinentes à região ou faixa etária.

Dessa forma, as restrições ao perfilamento de menores devem ter alcance razoável e proporcional, de modo a proteger o melhor interesse da criança e do adolescente sem inviabilizar desnecessariamente o desenvolvimento regular de atividades econômicas legítimas, sobretudo atividades que melhor resguardam o interesse do menor, como as do setor de saúde.

É, portanto, essencial que a interpretação da vedação ao perfilamento não seja operada de forma literal, isto é, como proibição de qualquer modalidade de perfilização. Pelo contrário, deve-se distinguir entre o perfilamento invasivo, efetivamente proibido, e o mero direcionamento cadastral de publicidade, que deve ser permitido.

O perfilamento invasivo caracteriza-se por práticas como análise emocional detalhada, criação de perfis comportamentais individualizados e rastreamento contínuo das atividades do menor, representando risco concreto à sua privacidade. Por outro lado, o direcionamento cadastral consiste apenas na segmentação básica de público com base em dados cadastrais elementares,

³ Disponível em: <https://www.cnnbrasil.com.br/nacional/mais-de-10-milhoes-de-brasileiros-nao-acessam-internet-por-nao-saberem-usar-a-tecnologia-diz-ibge/>

⁴ Art. 2º, V c/c art. 22 e 26, ECA Digital.



como faixa etária, gênero ou localização geográfica, sem qualquer forma de monitoramento comportamental ou rastreamento individual da atividade online. Por sua natureza, esse tipo de segmentação não acarreta risco relevante ao menor.

A adoção de entendimento distinto poderia gerar prejuízos significativos tanto para entidades que oferecem serviços legítimos de interesse do menor, a exemplo do setor da saúde, quanto para o próprio menor, que deixa de receber informações de seu interesse, sem produzir qualquer benefício real à proteção dos menores. Na prática, crianças e adolescentes continuariam a receber publicidade, porém de produtos e serviços potencialmente irrelevantes ou incoerentes com seu interesse, o que contraria o próprio propósito da legislação.

3. Tratamento dos dados pessoais de crianças e de adolescentes de forma que “cause, facilite ou contribua” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei⁵

a) **Proposta:** entendemos como necessária uma interpretação clara do significado da expressão “cause, facilite ou contribua” para atividades de tratamento que gerem riscos desproporcionais aos direitos do menor ou sejam, em si mesmas, violadoras desses direitos.

b) Fundamento:

A expressão “cause, facilite ou contribua” mostra-se excessivamente abrangente e, se interpretada literalmente, acaba por vedar, na prática, qualquer atividade de tratamento de dados envolvendo menores de idade.

Isso ocorre porque os verbos “facilitar” e “contribuir” sugerem que qualquer atividade capaz de gerar riscos aos direitos legais dos menores, inclusive direitos gerais, como o direito à privacidade, estaria proibida. Em tese, qualquer operação de tratamento poderia “facilitar” ou “contribuir” para um dano caso seus riscos, ainda que remotos, viessem a se materializar.

Como o dispositivo é silente quanto ao grau de risco, sua redação abarca indistintamente todos os tratamentos, já que toda atividade de tratamento envolve algum nível de risco aos titulares. É precisamente por essa razão que legislações modernas de proteção de dados, como a Lei Geral de Proteção de Dados, adotam abordagens baseadas em risco, abordagem esta que, em regra, os agentes de tratamento são recomendados a adotar em sua governança interna, como leciona a Autoridade de Dados da Irlanda⁶. Uma previsão genérica que veda tratamentos que apresentem riscos, sem qualquer qualificação, acaba, na prática, por proibir todas as atividades de tratamento.

Considerando que tal leitura não é razoável nem compatível com o sistema de proteção de dados vigente, recomenda-se que o dispositivo seja esclarecido para abranger apenas atividades de tratamento que: (i) gerem riscos desproporcionais aos direitos e liberdades do menor; ou (ii) sejam, em si mesmas, incompatíveis ou violadoras desses direitos. Essa interpretação assegura a proteção das crianças e adolescentes sem inviabilizar tratamentos legítimos e necessários.

⁵ Arts. 2º, V, 22 e 26, ECA Digital.

⁶ Disponível em: <https://www.dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach>



4. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser “utilizados unicamente para essa finalidade”⁷

a) Proposta: o conceito de “dados coletados para a verificação da idade”, para fins de aplicação do art. 13, não deve incluir o reaproveitamento de dados coletados em outros processos (ex. prevenção a fraudes) para fins de verificação de idade.

b) Fundamento:

No âmbito de seus processos ordinários, em especial aqueles voltados à prevenção de fraudes, grande parte das organizações já coleta dados que poderiam ser razoavelmente empregados em procedimentos de verificação de idade, tais como informações biométricas, documentos de identificação e demais dados correlatos.

Para evitar a coleta duplicada desses elementos, em afronta ao princípio da necessidade (art. 6º, III, da LGPD), é relevante que a interpretação do art. 13, do ECA Digital, não inviabilize o reaproveitamento de dados previamente tratados para outras finalidades legítimas, sobretudo a prevenção a fraudes, nos processos de verificação de idade.

Em outras palavras: o art. 13 deve ser objeto de interpretação restritiva, apenas proibindo-se a reutilização de dados pessoais quando coletados específica e exclusivamente para fins de verificação de idade.

Todavia, não entendemos suficiente que a ANPD apenas realize mera declaração quanto à possibilidade de reaproveitamento: considerando a insegurança jurídica decorrente da redação atual do dispositivo e o potencial de controvérsias acerca de eventual desvio de finalidade – isto é, se determinado dado foi reaproveitado para a verificação de idade ou se, ao contrário, foi coletado originalmente para esse fim e acabou empregado em outra finalidade legítima –, mostra-se essencial que a ANPD estabeleça orientações claras e operacionais que permitam a implementação dessa prática com segurança jurídica.

5. Mecanismos de Supervisão Parental⁸

a) Proposta: entendemos como necessária a melhor delimitação dos limites aplicáveis a supervisão parental, sobretudo a adoção clara de limitações da interferência dos pais, considerado o direito à privacidade do menor.

b) Fundamento:

É importante que a definição de mecanismos de supervisão parental estabeleça limites claros quanto ao grau de interferência possível pelos responsáveis. Esses mecanismos devem, simultaneamente, resguardar a autoridade parental e proteger o direito à privacidade do menor, sobretudo em aplicações que envolvem aspectos sensíveis de sua intimidade ou em situações nas quais a independência do menor aumenta progressivamente em razão de sua maturidade e capacidade.

⁷ Art. 13, ECA Digital.

⁸ Arts. 2º, VIII, art. 12, III e art. 16 e ss., ECA Digital.



No setor da saúde isso é especialmente relevante, considerando que o art. 74, do Código de Ética Médica⁹ expressamente veda a divulgação de informações aos saúde dos menores, inclusive aos seus pais e representantes legais, desde que estes tenham razoável capacidade de discernimento.

Nesse sentido, o Serviço Nacional de Saúde da Inglaterra (*National Health Service*, “NHS”) orienta que os responsáveis legais apenas possam acessar livremente as informações de saúde de seus filhos até os 11 anos de idade, período após o qual o menor pode optar por permitir o acesso, negá-lo ou restringi-lo¹⁰.

Em outras palavras: inexistindo limites claros à capacidade de intervenção parental, de uso dos mecanismos de supervisão, subsiste elevada probabilidade que, a título de proteção das crianças e adolescentes, se tolha a sua privacidade em nível desarrazoado, efetivamente gerando óbice ao desenvolvimento de sua personalidade.

Assim, é necessário assegurar segurança jurídica no sentido de que os mecanismos de supervisão parental não resultem em intrusões indevidas na intimidade dos menores, devendo o nível de acesso e intromissão respeitar a razoável capacidade e maturidade do menor de idade e o grau de intimidade ao qual a informação se refere.

6. Relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais¹¹

a) Proposta: o art. 16º, parágrafo único, II, estabelece a obrigação de as organizações elaborarem “*relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais*”. Entendemos necessário esclarecer que tal expressão deve ser interpretada como referência ao mesmo Relatório de Impacto à Proteção de Dados Pessoais (RIPD) previsto na LGPD, não se tratando, portanto, de documento distinto ou adicional.

Além disso, importante ressaltar que a lei estabelece a obrigação de RIPD para utilização de dados de crianças e adolescentes para fins que não os estritamente necessários para a operação do produto ou serviço. É importante esclarecer que essa obrigação se delimita a casos em que o tratamento dos dados de crianças e adolescentes considerem o titular dentro desse contexto e o difiram como tal. Em muitos casos na área de saúde, existirão dados sobre a idade do titular, mas não haverá distinção entre titulares (pacientes) adultos ou crianças e adolescentes. É dizer, o tratamento de dados não será direcionado para finalidades secundárias voltadas à infância e juventude e sim para outras atividades relevantes para a área da saúde.

b) Fundamento:

O legislador introduziu no ECA Digital a expressão “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”, sem, contudo, fornecer qualquer definição normativa para tal documento.

A Lei Geral de Proteção de Dados Pessoais já incorporou ao ordenamento jurídico nacional o Relatório de Impacto à Proteção de Dados (“RIPD”), instrumento suficiente para a demonstração

⁹ Disponível em: <https://portal.cfm.org.br/images/PDF/cem2019.pdf>

¹⁰ Disponível em: <https://www.england.nhs.uk/long-read/identity-verification/>

¹¹ Art. 16, parágrafo único, II, ECA Digital.



e gestão de riscos à privacidade nas atividades de tratamento que possam afetar direitos e liberdades fundamentais dos titulares – conceito que pode razoavelmente abranger as situações previstas no ECA Digital.

A adoção de entendimento contrário resultaria na alocação ineficiente de recursos pelos agentes de tratamento, tendo em vista a elevada complexidade técnica já inerente à elaboração de um RIPD, e, sobretudo, o consumo de recursos humanos demandado em sua elaboração – dado o tempo e esforço das áreas de negócio e das equipes técnicas envolvidas, além da participação de profissionais especializados em privacidade.

Deste modo, a criação de um segundo relatório implicaria um consumo duplicado desses recursos limitados, desviando-os de atividades mais relevantes para a própria defesa dos interesses das crianças e adolescentes. A saber: a correção de vulnerabilidades e a implementação dos controles identificados no próprio RIPD, para a elaboração de um documento adicional, de provável conteúdo substancialmente redundante.

Assim, entendemos recomendável que se esclareça que o “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais” se trata do mesmo “relatório de impacto à proteção de dados pessoais” previsto na LGPD.

7. Verificação de idade “a cada acesso” do usuário ao conteúdo, produto ou serviço¹²

a) Proposta: a interpretação literal da expressão “a cada acesso”, para a periodicidade da verificação de idade, conforme previsto no art. 9º, §1º, implicaria ônus desproporcionado e economicamente impraticável, sendo relevante que a ANPD apresente entendimento proporcional aos riscos concretos apresentados por cada serviço da sociedade da informação.

b) Fundamento:

Embora o art. 9º, § 1º, do ECA Digital determine a adoção de mecanismos de verificação de idade “a cada acesso” do usuário a conteúdos, produtos ou serviços, a interpretação literal dessa exigência pode conduzir a distorções práticas, comprometer a própria experiência digital e se revelar economicamente impraticável para elevado número de organizações.

Conforme o estudo da *Family Online Safety Institute*, é fundamental considerar a experiência do usuário e a minimização de fricção. Isso porque existem preocupações sobre o potencial de que os processos de aferição de idade se tornem o próximo “*banner de cookies*”, obrigando os usuários a passarem por verificações de idade toda vez que visitam um novo site ou aplicativo. Soluções interoperáveis poderiam aliviar os problemas de frustração e fadiga dos usuários e facilitar para as empresas a otimização de seus esforços. Essa noção também apoiaria a ênfase em uma abordagem baseada em risco em que, uma vez que o usuário tenha verificado sua idade, ele só precisaria realizar nova verificação em sites considerados de maior risco, como aqueles com conteúdo adulto ou jogos de azar¹³.

¹² Art. 9º, §1º, ECA Digital.

¹³ Disponível em: https://global-uploads.webflow.com/5f4dd3623430990e705ccbba/64b0011a158eea37fb7796c4_FOSI%20White%20Paper%20Coming%20to%20Terms%20with%20Age%20Assurance%20FOR%20WEBSITE.pdf



Do ponto de vista corporativo, tecnologias de verificação de idade, não raramente, precisam ser contratadas de terceiros. Referidas soluções habitualmente envolvem um custo por consulta realizada. Ou seja: a cada atividade de verificação de idade, a companhia necessita pagar um determinado valor ao fornecedor.

Assim obrigar os entes privados a realizarem uma verificação de idade do usuário a cada acesso aos seus serviços, mesmo que estes já se encontrem previamente autenticados, implica impor-lhes um significativo aumento do custo operacional – que muitas vezes se revelará economicamente impraticável frente a natureza do negócio.

Por exemplo, em soluções de acesso recorrente, mas com assinatura mensal (com serviços de *streaming*) ou que inexistam custos no acesso em si mesmo (como aplicações para acesso a exames e outras informações médicas), realizar uma biometria ou documentoscopia a cada acesso implicaria provável inviabilidade no fornecimento desses serviços ou, minimamente, provável aumento substancial nos valores de sua assinatura, tornando-os inacessíveis a parte significativa da população.

Além disso, tal requerimento implicaria a necessidade da coleta repetitiva de dados pessoais, ampliando os riscos de segurança da informação e contrariando o princípio da minimização de dados, previsto no art. 6º, III, da Lei Geral de Proteção de Dados Pessoais (LGPD).

Assim, revela-se essencial que a ANPD adote entendimento regulatório que ajuste a periodicidade da verificação de idade aos riscos concretos apresentados por cada serviço da sociedade da informação, de modo a equilibrar a proteção do menor com a viabilidade técnica e econômica das medidas de conformidade.

8. Autonomia progressiva¹⁴

- a) **Proposta:** A lei impõe a obrigação da adoção de mecanismos para proporcionar experiências adequadas à idade, respeitada a “autonomia progressiva”. O conceito de “autonomia progressiva” em ambiente digital tem sido explorado pela academia, mas é importante que a ANPD estabeleça critérios de avaliação para essa análise, de forma a torná-la menos subjetiva e casuística.

9. Mecanismos de notificações acerca de violações aos direitos de crianças e adolescentes¹⁵

- a) **Proposta:** A lei impõe a obrigatoriedade da criação e da publicização de mecanismo para notificações acerca de violações aos direitos de crianças e de adolescentes. É importante delimitar que essa obrigação se refere a violações que possam eventualmente ocorrer dentro do ambiente digital do serviço/produto em questão.

10. Ofício às autoridades competentes¹⁶

- a) **Proposta:** A lei também estabelece a obrigatoriedade de oficiar às autoridades competentes sobre as violações de direitos de crianças e adolescentes *quando for o caso*. É importante

¹⁴ Art. 10, ECA Digital.

¹⁵ Art. 28, caput e art. 29, §3º, ECA Digital.

¹⁶ Art. 28, parágrafo único e 29, §2º, ECA Digital.



esclarecer qual é o papel esperado da empresa nessa análise, o que é importante documentar em termos de eventual prestação de contas às Autoridades e quais são os “elementos de identificação técnica” das violações que deverão ser notificados para que a notificação não seja considerada nula.

ANPD TS conceitos previstos no ECA Digital

Contribuição do Idec - Instituto de Defesa de Consumidores

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Contribuição do Idec - Instituto de Defesa de Consumidores

Os principais conceitos, termos e expressões que demandam esclarecimentos são:

I. “De acesso provável” (art. 1º e ss.)

É necessário aprofundar os parâmetros estabelecidos nos incisos do art. 1º para não restarem dúvidas sobre a inaplicabilidade da autodeclaração das plataformas por meio dos Termos de Uso. A definição de “acesso provável” não deve basear-se na intenção formal da empresa, mas sim em evidências fáticas de uso por crianças e adolescentes. Para isso, devem ser considerados elementos como o design e apelo visual da interface (presença de personagens, gamificação), a existência de uma base de usuários menores de idade e a presença de conteúdos da cultura infanto-juvenil.

Embora a lei estabeleça critérios como probabilidade de uso, facilidade de acesso e grau de risco, é preciso esclarecer objetivamente quais indicadores poderão ser utilizados para caracterizar plataformas sujeitas ao regime protetivo. Estudos como o TIC Kids Online 2024 [1], que apontam que 82% das crianças de 11 e 12 anos possuem redes sociais mesmo quando a idade mínima declarada é 13 anos, reforçam que a regulamentação deve considerar o uso real e não apenas a destinação formal do serviço. O parâmetro impede brechas frequentemente exploradas por plataformas que alegam não serem destinadas a crianças, apesar de ampla evidência de presença infantil, como já discutido em procedimentos perante a ANPD - como nos casos TikTok (Processo nº 00261.004725/2024-81 e WhatsApp (Processo nº 00261.001296/2022-29). Logo, entendemos que para a definição de “acesso provável”, deve-se considerar a presença de elementos infantis ou de apelo juvenil na arquitetura da plataforma, como personagens, cores vibrantes, músicas virais, desafios (trends) e mecânicas de gamificação. Se a plataforma, por seu design e conteúdo, atrai o público infantil, ela deve ser considerada como de “acesso provável”, independentemente dos seus termos de serviço.

II. “Medidas razoáveis” (art. 6, caput e § 2º):

A expressão “razoáveis” não pode ser utilizada para justificar inação ou medidas paliativas baseadas apenas no esforço mínimo das empresas tendo em vista seus interesses comerciais. A norma deve ser interpretada segundo a lógica do dever de prevenção, de forma que os fornecedores de serviços e produtos digitais utilizem toda tecnologia disponível para diminuir riscos de violações dos direitos das crianças, como ferramentas de moderação sobre conteúdos proibidos ou ilícitos.

III. “Experiências adequadas à idade” (art. 10):

É preciso identificar se essa obrigação será vinculada aos critérios relacionados ao desenvolvimento biopsicossocial e/ou a classificação indicativa, considerando que, diferente

do audiovisual tradicional, o ambiente digital exige que a adequação a idade também esteja relacionada a parâmetros de interatividade e riscos de contato com terceiros. Nesse sentido, a Portaria nº 1.048/2025 [2], que atualizou as regras da Classificação Indicativa no Brasil para ambientes digitais, reconheceu que o risco e a adequação não estão apenas no conteúdo visual, mas também funcionalidades (compras no app, chats com IA e interação com desconhecidos). Ao mesmo tempo, essa classificação é meramente indicativa, não vinculando obrigatoriamente a prestação de serviços digitais.

IV. “Funcionamento básico” (art. 17, VIII):

É fundamental distinguir o funcionamento básico da aplicação de suas ferramentas voltadas à exploração comercial, como a perfilização e a maximização do engajamento. A legislação prevê a desabilitação de ferramentas de IA não essenciais, e isso não deve ser confundido com a inviabilização do serviço. O funcionamento básico refere-se, por exemplo, a utilidade central do serviço ou produto digital (enviar mensagens, postar fotos, fazer pesquisas). Enquanto isso, recursos como reprodução automática, rolagem infinita e recomendações algorítmicas agressivas são estratégias de modelo de negócio, não requisitos funcionais.

V. “Publicidade comercial” (art. 22):

O conceito deve ser aprofundado para que não fique restrito ao imperativo de consumo em sentido estrito, ignorando as complexidades do marketing digital atual. Diante da dificuldade da criança em identificar conteúdo patrocinado, defendemos uma interpretação ampla que abranja qualquer impulsionamento de conteúdo, publicidade patrocinada e estratégias de formação de opinião ou marca. Há de se considerar a hipervulnerabilidade do público infantil, tratando como publicidade comercial qualquer comunicação mercadológica impulsionada, independentemente de haver uma oferta direta de produto.

VI. “Fundados indícios de operação por crianças e adolescentes” (art. 24, §3º e §4º):

O termo está relacionado a possível suspensão da conta de um usuário. Em que pese a seriedade dessa situação, não existem elementos ou padrões pré-definidos para a determinação dos indícios de uso, levando a uma situação de insegurança jurídica tanto aos provedores como para os usuários e responsáveis legais. É necessária uma maior fundamentação para definir as evidências que indicam que a conta está sendo usada por uma criança ou adolescente.

Para além das questões mencionadas, entendemos que os parâmetros de interpretação devem ser considerados da absoluta prioridade (art. 227, CRFB) e do melhor interesse de crianças e adolescentes (art. 14, LGPD e art. 5º, ECA Digital).

Referências

[1] CETIC.br. TIC Kids Online Brasil 2024: Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Núcleo de Informação e Coordenação do Ponto BR (NIC.br), 2024. Disponível em:

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2024/>. Acesso em: 3 dez. 2025

[2] BRASIL. Ministério da Justiça e Segurança Pública. MJSP lança nova faixa etária e amplia regras da Classificação Indicativa para o ambiente digital. Brasília: Ministério da Justiça e Segurança Pública, 15 out. 2025. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-lanca-nova-faixa-etaria-e-amplia-regras-da-classificacao-indicativa-para-o-ambiente-digital>. Acesso em: 3 dez. 2025.

CONTRIBUIÇÃO À TOMADA DE SUBSÍDIOS: CONCEITOS DO ECA DIGITAL

Elora Fernandes

Pesquisadora de Pós-Doutorado no KUL Centre for IT & IP Law

1) PRODUTO OU SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

DISPOSITIVOS RELEVANTES

Art, 2º, I – produto ou serviço de tecnologia da informação: produto ou serviço fornecido **a distância, por meio eletrônico e provido em virtude de requisição individual**, tais como aplicações de internet, programas de computador, softwares, sistemas operacionais de terminais, lojas de aplicações de internet e jogos eletrônicos ou similares conectados à internet ou a outra rede de comunicações;

A noção de produto ou serviço de tecnologia da informação, no ECA Digital, parece ter sido diretamente inspirada no conceito de “serviço da sociedade da informação”, presente na Diretiva Europeia 2015/1535. Na diretiva, estes serviços são entendidos como “qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrônica e mediante pedido individual de um destinatário de serviços” (Artigo 1.º (1)(b)). Essa definição, porém, apresenta algumas limitações importantes, especialmente por depender dos conceitos de fornecimento “à distância” e “requisição individual”.

De acordo com o mesmo dispositivo da diretiva, um serviço prestado “à distância” é aquele prestado sem que as partes estejam simultaneamente presentes. Isso poderia gerar dúvidas sobre a aplicação do ECA Digital a produtos físicos conectados (como brinquedos inteligentes), experiências digitais acessadas presencialmente (como totens, máquinas de jogos ou quiosques interativos) e outros serviços híbridos.

Da mesma forma, um serviço provido em virtude de requisição individual é entendido pela diretiva como aquele fornecido por transmissão de dados mediante pedido individual. A expressão sugere que apenas serviços acionados diretamente pelo usuário estariam incluídos, o que poderia deixar de fora, por exemplo, serviços que são utilizados por crianças e adolescentes, mas que não são de sua solicitação individual, como tecnologias educacionais que são adotadas pelas escolas.

Por fim, percebe-se que a definição europeia é centrada na ideia de “serviço”, o que pode dificultar sua adaptação a “produtos” digitais. Assim, **recomenda-se:**

R1) Que a ANPD esclareça se adota o mesmo entendimento da diretiva europeia ou se interpreta de forma mais ampla os conceitos de “fornecimento à distância” e “requisição individual”;

R2) Que a ANPD esclareça se as noções de produto ou serviço são as mesmas adotadas no Código de Defesa do Consumidor (CDC).

2) EXPRESSÃO DO MELHOR INTERESSE DA CRIANÇA E DO ADOLESCENTE

DISPOSITIVOS RELEVANTES

Art, 5º, § 2º Para os fins desta Lei, considera-se como expressão do melhor interesse da criança e do adolescente a proteção de sua privacidade, segurança, saúde mental e física, acesso à informação, liberdade de participação na sociedade, acesso significativo às tecnologias digitais e bem-estar.

O princípio do melhor interesse da criança (como estabelecido na Convenção sobre os Direitos da Criança – pessoa de 0 a 18 anos) é necessariamente um conceito **aberto e dinâmico**. O conteúdo do melhor interesse (ou seja, aquilo que de fato é de melhor interesse de uma criança ou grupo de crianças em uma determinada situação) não é possível de se estabelecer em abstrato, mas é o resultado de um **exercício de ponderação no caso concreto**. Este exercício deve considerar a indivisibilidade, interdependência e universalidade de todos os direitos previstos na Convenção (como alguns dos mencionados no rol, como o direito à privacidade, o acesso à informação ou ao desenvolvimento - incluindo a saúde física e mental), bem como interesses mais amplos (como a liberdade de participação na sociedade, o acesso significativo às tecnologias digitais e bem-estar).

Ao selecionar apenas determinados direitos e interesses, o rol sugerido pelo ECA Digital produz um enquadramento restritivo injustificado, o que é incompatível com a exigência de que a análise envolva o conjunto total de direitos de proteção, provisão e participação presentes na Convenção. Direitos importantíssimos como à educação ou à participação não são incluídos no rol.

Além disso, a definição fixa pode gerar **conflitos internos de interpretação**, na medida em que alguns elementos da lista podem entrar em tensão entre si. Assim, a partir da abordagem de risco, provedores de produtos ou serviços de tecnologia da informação deveriam considerar os impactos positivos e negativos daquele produto ou serviço (incluindo possíveis medidas de mitigação) em todos os direitos e interesses de crianças a partir das Análises de Impacto a Direitos de Crianças (as chamadas metodologias CRIA). Essa metodologia inclui, necessariamente, impactos presentes e futuros (a partir de uma abordagem de prevenção), bem como considera o desenvolvimento progressivo das capacidades da criança.

A partir do balanceamento de direitos e interesses da criança, é possível determinar, portanto, aquilo que é de melhor interesse dela (ou de um grupo) naquele caso concreto (por exemplo, disponibilizar ou não uma funcionalidade em um aplicativo). É apenas neste estágio que esse resultado pode ser balanceado com direitos de terceiros, considerando que o melhor interesse deve ser uma **consideração primordial**, isto é, ganha precedência sempre, a não ser que haja

um interesse público ou um direito de igual ou maior peso que, no caso concreto, justifique de forma fundamentada sua prevalência.

Assim, **recomenda-se:**

R3) Que a definição de “expressão do melhor interesse” seja entendida como um **rol aberto**, que lista apenas alguns direitos que devem ser considerados pelos provedores de produtos ou serviços de tecnologia da informação;

R4) Que a ANPD elabore diretrizes e metodologias a partir dos CRIA para guiar provedores de produtos ou serviços de tecnologia da informação na implementação do melhor interesse da criança na prática.

2) GARANTIA/AFERIÇÃO DE IDADE

DISPOSITIVOS RELEVANTES

Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos.

§ 1º Para dar efetividade ao disposto no *caput*, deverão ser adotados **mecanismos confiáveis de verificação de idade** a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o *caput* deste artigo, vedada a autodeclaração.

[...]

CAPÍTULO IV

DOS MECANISMOS DE AFERIÇÃO DE IDADE

Art. 12. Os provedores de lojas de aplicações de internet e de sistemas operacionais de terminais deverão:

I – tomar medidas proporcionais, auditáveis e tecnicamente seguras para **afерir a idade ou a faixa etária dos usuários**, observados os princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

[...]

§ 3º Ato do Poder Executivo regulamentará os requisitos mínimos de transparência, de segurança e de interoperabilidade para os **mecanismos de aferição de idade** e de supervisão parental adotados pelos sistemas operacionais e pelas lojas de aplicativos.

Art. 13. Os dados coletados para a **verificação de idade** de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito.

CAPÍTULO IX

DAS REDES SOCIAIS

Art. 24, §1º, III – aprimorar, de maneira contínua, seus mecanismos de **verificação de idade** para identificar contas operadas por crianças e adolescentes.

[...]

§ 4º Diante de fundados indícios de que a conta é operada por criança ou adolescente em desconformidade com os requisitos de idade mínima previstos na legislação, os provedores de redes sociais deverão suspender o acesso do usuário e assegurar a instauração de procedimento célere e acessível no qual o responsável legal possa apresentar apelação e **comprovar a idade** por meio adequado, nos termos de regulamento.

Mecanismos de garantia ou aferição de idade são extremamente importantes em legislações protetivas a crianças e adolescentes e pode-se dizer que possuem uma dupla função:

Primeiramente, podem ser utilizados para separar audiências e, eventualmente, restringir o acesso a determinados produtos, serviços ou conteúdos. Isso pode ter origem na proibição por lei desse acesso (produtos como tabaco, álcool, facas e pornografia, bem como serviços como jogos de azar), mas também inclui situações em que o mecanismo é implementado como dever de diligência, isto é, como um requisito implícito para cumprir adequadamente as obrigações legais. Isso se verifica, por exemplo, na necessidade de implementar mecanismos de garantia de idade para implementar princípios da LGPD como minimização ou proteção de direitos dos titulares (a partir de uma abordagem de risco e proteção por desenho). Assim, por exemplo, se um aplicativo não permite que crianças e adolescentes o acessem, não pode então tratar os dados deste público sem que uma violação da lei seja identificada. Assim, o mecanismo de garantia de idade é um requisito implícito para o cumprimento de outros dispositivos da LGPD.

Em segundo lugar, esses mecanismos podem ser utilizados para garantir a licitude e validade de determinados atos jurídicos. Em muitas situações, é essencial confirmar se o indivíduo possui capacidade jurídica para realizar determinados atos, tornando a garantia de idade uma ferramenta crucial para assegurar que a pessoa cumpre os requisitos mínimos estabelecidos por lei para agir sem assistência ou representação dos responsáveis legais. Isso é essencial, por exemplo, para garantir a validade de contratos assinados online ou do consentimento para tratamento de dados pessoais.

No caso do ECA Digital, esses mecanismos são importantes de maneira geral, considerando que a lei, como um todo, estabelece obrigações para produtos e serviços direcionados a crianças e adolescentes e aqueles de acesso provável por esse público. Dessa forma, a aplicação prática da lei depende diretamente da existência de mecanismos capazes de identificar a idade dos usuários. Contudo, percebe-se que a linguagem utilizada pelo texto legal é imprecisa, pouco sistemática e não alinhada com a literatura especializada e com *standards* internacionais. A lei utiliza de forma fluida conceitos variados como “verificação de idade”, “aferição de idade”, “comprovação de idade” etc. Isso pode gerar insegurança jurídica e interpretações excessivamente rígidas. Por exemplo, quando se utiliza um termo mais como “verificação de idade”, seria correto inferir que apenas mecanismos de comprovação documental – como identidade, passaporte ou outros atributos verificáveis – podem ser empregados? Ou o legislador pretendia abarcar um espectro mais amplo de técnicas?

Em seu Radar Tecnológico sobre Mecanismos de Aferição de Idade a ANPD reconhece essas nuances terminológicas e faz a diferenciação entre três grandes categorias, isto é, autodeclaração, verificação de idade e estimação de idade. Assim, recomenda-se:

R5) Que a ANPD esclareça o sentido técnico preciso dos diferentes termos utilizados pela lei;

R6) Que a ANPD desenvolva diretrizes sobre as situações nas quais cada uma das técnicas pode/deve ser utilizada ou parâmetros que devem ser levados em consideração para a escolha do mecanismo apropriado.

Tomada de Subsídios conceitos previstos no ECA Digital

“Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?”

1. O artigo 1º do Estatuto estabelece um critério de aplicabilidade amplo, baseado na "suficiente probabilidade de uso", "facilidade de acesso" e "significativo grau de risco". O problema reside na falta de uma régua objetiva para medir esses fatores.

Como uma empresa pode, em sua fase de concepção de produto (privacy by design), avaliar com segurança se sua solução possui "atratividade" suficiente para ser considerada de "acesso provável" por menores? A interpretação pode variar drasticamente entre a visão da empresa e a de um órgão fiscalizador.

É importante que a ANPD estabeleça um modelo de avaliação, como acontece no RIPD, com critérios e métricas concretas. A regulamentação poderia, por exemplo, definir parâmetros baseados em objetivo do negócio e do produto de tecnologia que está sendo desenvolvido, se há coleta de dados, entre outros critérios.

2. O art. 2º não traz a definição de acesso provável e demais termos acima mencionados. Consideramos relevante a inclusão destes;
3. Art. 2º - Produto ou Serviço de TI

A definição de "produto ou serviço de TI" é muito ampla e abre uma brecha perigosa. O texto tenta incluir tudo (apps, jogos, sistemas operacionais), mas ao mesmo tempo poderia englobar "funcionalidades essenciais da internet". A linha entre o que é um serviço e o que é só um protocolo básico da web é muito tênue.

O exemplo clássico é o navegador de internet. O Chrome é o quê? Ele é um programa que lê protocolos abertos (a exceção da lei), mas também é um produto do Google que coleta dados e está ligado a um modelo de negócio gigantesco. O mesmo vale para serviços de DNS, como o da Cloudflare.

Entendemos que a ANPD precisaria regulamentar isso focando no modelo de negócio e no serviço final entregue ao usuário, e não na tecnologia que roda por baixo. Se a empresa empacota um protocolo, adiciona funcionalidades, coleta dados e oferece isso como um serviço comercial, ela tem que estar sob

o guarda-chuva da lei. Precisamos de regras claras para definição, pois como está fica objetivo os momentos de aplicação da lei.

4. O art. 6º ao mencionar “medidas razoáveis” sem apresentar critérios mínimos sobre o que seria razoável, dificulta a compreensão pelos agentes quanto ao que exatamente devem considerar para fins de implementação. Importante que a ANPD estabeleça critérios mínimos sobre o que seriam medidas razoáveis para atendimento a cada um dos incisos deste artigo 6º.
5. O Art 8º, IV faz referência ao “uso compulsivo de produtos ou serviços por crianças e adolescentes”, mas não há indicação sobre o que deve ser considerado este uso compulsivo. Dessa forma, importante que sejam estabelecidos critérios quanto a tempo e quantidade de acessos mínimos para a melhor compreensão do termo indicado.
6. "Conteúdo Impróprio" - Art. 9º - A regulamentação deve especificar o escopo dessa remissão. O ideal seria que a ANPD, em colaboração com outros órgãos, criasse e mantivesse uma taxonomia ou uma lista de referência de categorias de conteúdo consideradas de alto risco, como apologias à automutilação, transtornos alimentares, discursos de ódio e desafios perigosos, conferindo previsibilidade às obrigações de moderação. Há alguma métrica que poderia ser aplicada como referência, como a de produções audiovisuais?
7. Art. 9º, §1º - “mecanismos confiáveis de verificação de idade” – Entendemos que a ANPD deverá regulamentar sobre os mecanismos confiáveis de verificação de idade, tal como disposto no art 11º, p.u. da Lei, trazendo definições e critérios para sua aplicabilidade de acordo com o contexto setorial dos agentes.

São Paulo, 12 de dezembro de 2025.

À Coordenação-Geral de Normatização da Agência Nacional de Proteção de Dados (ANPD)

Assunto: Tomada de Subsídios referente a conceitos previstos na Lei nº 15.211/2025 (“ECA Digital”).

Prezados(as),

Em atenção à Consulta Pública aberta em 28 de novembro de 2025, o escritório de advocacia **Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados (SBSA Advogados)**¹ vem apresentar recomendações e sugestões para esclarecimento de conceitos da Lei nº 15.211/2025 (“ECA Digital”).

Fundado em 2002, SBSA Advogados é escritório pioneiro e especializado em Direito do Terceiro Setor, com mais de duas décadas de atuação dedicada a organizações da sociedade civil que promovem direitos fundamentais, incluindo direitos de crianças e adolescentes. Ao longo de sua trajetória, o escritório desenvolveu expertise específica em Proteção de Dados Pessoais e Direito Digital aplicados às particularidades das organizações sem fins lucrativos que atuam em áreas como assistência social, educação, saúde, cultura, defesa de direitos e pesquisa científica.

Essas organizações, entretanto, enfrentam desafios particulares quando normas regulatórias não consideram suas especificidades operacionais, limitações de recursos e natureza não lucrativa de suas atividades. A ausência de clareza conceitual em legislações como o ECA Digital pode criar barreiras desproporcionais ao trabalho dessas entidades, prejudicando justamente o interesse público que buscam promover: a proteção integral de crianças e adolescentes.

Nesta contribuição, buscaremos responder à pergunta formulada pela ANPD: *“Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?”*

Nossa análise priorizará conceitos que impactam diretamente organizações da sociedade civil que atuam na proteção de crianças e adolescentes, bem como aqueles cuja interpretação demanda harmonização com a Lei Geral de Proteção de Dados Pessoais (LGPD), buscando inspiração em padrões internacionais consolidados.

1. “Acesso provável por crianças e adolescentes” (art. 1º, parágrafo único, ECA Digital)

¹ Sociedade de advogados inscrita no CNPJ/MF sob o n. 05.276.071/0001-35, com sede em Curitiba/PR, na Rua Marechal Deodoro, nº 869, 2º andar, e sua filial inscrita no CNPJ/MF sob o n. 05.276.071/0002-16, localizada na Capital do Estado de São Paulo, na Av. Nove de Julho, nº 4865 – 8º andar, conj. 81.

De acordo com seu art. 1º, a Lei nº 15.211/2025 “aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles”.

O parágrafo único deste artigo busca definir o conceito de “acesso provável”:

“Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações:

I – suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes;

II – considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes; e

III – significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital.”

Um primeiro ponto que demanda esclarecimento é a cumulatividade ou alternatividade dessas três situações. A conjunção "e" ao final do inciso II sugere cumulatividade entre os três requisitos, interpretação que encontra respaldo doutrinário, como exposto no artigo "O 'E' que define o futuro do ECA Digital", publicado no Jota: "A estrutura gramatical é a viga mestra da interpretação. A conjunção aditiva 'e' conecta os incisos II e III. O legislador não escreveu 'ou'; ele escreveu 'e'. A escolha vocabular não é um acaso nem um preciosismo. Em bom português, a partícula 'e' soma, adiciona, exige a presença de todos os elementos que conecta."²

“A estrutura gramatical é a viga mestra da interpretação. A conjunção aditiva "e" conecta os incisos II e III. O legislador não escreveu "ou"; ele escreveu "e". A escolha vocabular não é um acaso nem um preciosismo. Em bom português, a partícula "e" soma, adiciona, exige a presença de todos os elementos que conecta. Ignorar isso não é interpretar, é reescrever a lei.”³

Recomendamos que a ANPD esclareça expressamente que as três situações são cumulativas, sendo necessária a presença conjunta de todos os elementos para caracterização do "acesso provável".

Superada essa questão, os conceitos indeterminados presentes nos três incisos também demandam maior precisão: "suficiente probabilidade", "atratividade", "considerável facilidade", "significativo grau de risco".

² VIDIGAL, Paulo. O 'E' que define o futuro do ECA Digital. JOTA, 9 out. 2025. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-e-que-define-o-futuro-do-eca-digital-09102025>. Acesso em: 4 dez. 2025.

³ VIDIGAL, Paulo. O 'E' que define o futuro do ECA Digital. JOTA, 9 out. 2025. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-e-que-define-o-futuro-do-eca-digital-09102025>. Acesso em: 4 dez. 2025.

2. “Suficiente probabilidade de uso e atratividade”: parâmetros sugeridos com base em padrões internacionais

Um dos conceitos mais abertos do ECA Digital é a “suficiente probabilidade de uso e atratividade” por crianças e adolescentes. Para subsidiar a compreensão e a aplicação desse conceito na prática, consideramos interessante o exemplo da legislação do estado da Califórnia (EUA), denominada *California Age-Appropriate Design Code Act*⁴.

A referida legislação do estado da Califórnia (EUA) oferece parâmetros concretos para definir quando um serviço online é “de provável acesso por crianças” (*likely to be accessed by children*). Segundo o item 1798.99.30, (b), (4) dessa legislação, é razoável esperar que um serviço seja acessado por crianças com base nos seguintes indicadores⁵:

- (a) O serviço online é direcionado a crianças, conforme definido pela Lei Federal de Proteção à Privacidade Online das Crianças dos EUA (*Children's Online Privacy Protection Act - COPPA*, 15 U.S.C. § 6501 et seq.)⁶;
- (b) O serviço online é determinado, com base em evidências competentes e confiáveis sobre a composição do público, como sendo acessado rotineiramente por um número significativo de crianças;
- (c) O serviço possui anúncios direcionados a crianças;
- (d) O serviço é substancialmente semelhante ou idêntico a outro serviço que atenda ao critério (b);
- (e) O serviço possui elementos de design conhecidos por serem do interesse de crianças, incluindo, mas não se limitando a jogos, desenhos animados, música e celebridades que atraem crianças;
- (f) Uma parte significativa do público do serviço é determinada, com base em pesquisas internas da empresa, como sendo composta por crianças.

⁴ **California Age-Appropriate Design Code Act**. Bill Text: CA AB2273 | 2021-2022 | Regular Session | Chaptered. Sacramento, CA: LegiScan, 2022. Disponível em: <https://legiscan.com/CA/text/AB2273/id/2606836>. Acesso em: 4 dez. 2025.

⁵ “(4) “Likely to be accessed by children” means it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children:

(A) The online service, product, or feature is directed to children as defined by the Children’s Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.).

(B) The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

(C) An online service, product, or feature with advertisements marketed to children.

(D) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B).

(E) An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children.

(F) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.”

⁶ FEDERAL TRADE COMMISSION (FTC). Children's Online Privacy Protection Rule (“COPPA”). 16 CFR Part 312. Disponível em: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>. Acesso em: 12 dez. 2025

Esses critérios podem subsidiar a regulamentação brasileira, especialmente os itens (b), (e) e (f), que trazem parâmetros objetivos baseados em:

- Evidências sobre composição do público (dados demográficos, pesquisas de mercado);
- Elementos de design (presença de gamificação, personagens infantis, interfaces coloridas e lúdicas);
- Pesquisas internas das próprias empresas sobre perfil etário dos usuários.

O COPPA, mencionado no item (a), define como "direcionado a crianças" serviços que:

- Sejam destinados a crianças menores de 13 anos;
- Possuam conteúdo, linguagem visual ou áudio claramente dirigido a esse público;
- Utilizem personagens, celebridades ou linguagem que apele a crianças;
- Sejam anunciados ou promovidos em canais frequentados por crianças.⁷

A Agência Nacional de Proteção de Dados pode utilizar como inspiração a legislação mencionada no subparágrafo (A) ("*Children's Online Privacy Protection Act*" (COPPA), legislação federal dos Estados Unidos da América) para aprofundar o conceito de "suficiente probabilidade de uso e atratividade" do ECA Digital – especialmente considerando que muitos produtos e serviços digitais utilizados nos EUA também são acessados por público brasileiro.

Já o subparágrafo (e) pode subsidiar a conclusão de que o conceito é abrangente, sendo aplicável a qualquer plataforma que permita a inserção livre de conteúdos por seus usuários (como é o caso da maioria das redes sociais). Essa abordagem nos parece suficientemente cautelosa, priorizando o melhor interesse da criança.

Recomendamos que a ANPD considere a elaboração de Guia Orientativo ou Regulamento que estabeleça critérios objetivos inspirados nesses padrões internacionais, adaptados à realidade brasileira e em consonância com a LGPD.

Especificamente quanto ao inciso III (significativo grau de risco), sugerimos que a ANPD esclareça que plataformas de interação social com capacidade de compartilhamento em larga escala e sem controle editorial prévio são presumidamente de "acesso provável", considerando o alto grau de risco inerente a esses ambientes. Isso harmoniza com o princípio da proteção integral e da prioridade absoluta das crianças e adolescentes (art. 227 da Constituição Federal).

3. "Instituições de pesquisa" (Art. 31, parágrafo único)

O art. 31, parágrafo único, do ECA Digital estabelece que fornecedores devem disponibilizar gratuitamente dados agregados e não identificáveis sobre o acesso de crianças e adolescentes a seus produtos ou serviços a "instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas, para pesquisa, produção de estatísticas e estudos".

Esse dispositivo possui interface direta com o conceito de "órgão de pesquisa" definido pela LGPD, porém não há menção expressa a essa definição no ECA Digital. Essa lacuna gera insegurança jurídica sobre quais entidades se qualificam para acesso aos dados.

A LGPD define "órgão de pesquisa" no art. 5º, XVIII, como: "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico".

Essa definição foi cuidadosamente elaborada e já consolidada na jurisprudência e prática regulatória da ANPD. Além disso, a LGPD prevê bases legais específicas que autorizam o tratamento de dados pessoais, inclusive sensíveis, para fins de pesquisas científicas, históricas, estatísticas ou de interesse público (arts. 7º, IV e § 4º; 11, II, "d" e § 4º).

Tais bases legais exigem: (i) anonimização dos dados sempre que possível; (ii) ausência de finalidade comercial; (iii) adoção de salvaguardas de segurança e confidencialidade; (iv) vinculação estrita à finalidade de pesquisa. Esses elementos se alinham integralmente às exigências do próprio art. 31 do ECA Digital, que condiciona o acesso gratuito aos dados à observância dos princípios da finalidade, necessidade, segurança e confidencialidade, além da proibição expressa de uso para fins comerciais.

Há, portanto, plena convergência normativa entre os objetivos da LGPD e do ECA Digital: ambos reconhecem o papel essencial desempenhado por instituições de pesquisa na produção de conhecimento relevante para a formulação de políticas públicas e para a proteção integral de grupos vulneráveis como crianças e adolescentes.

A inclusão expressa do conceito de "órgão de pesquisa" da LGPD no ECA Digital garante que todas as organizações que possuam em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada sejam contempladas. Isso inclui:

- Universidades públicas e privadas;
- Centros de pesquisa vinculados a órgãos públicos;
- Institutos independentes de pesquisa;
- Organizações da sociedade civil sem fins lucrativos cuja missão inclua pesquisa científica (como institutos, fundações privadas e associações);

- Entidades de produção de estatísticas oficiais.

Essa harmonização é particularmente importante para organizações da sociedade civil que atuam na defesa de direitos de crianças e adolescentes e que dependem de dados para monitorar a efetividade de políticas públicas, produzir evidências científicas e realizar advocacy baseado em dados.

Recomendamos, portanto, que a ANPD esclareça em Guia Orientativo ou Regulamento que o termo "instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas" do art. 31 do ECA Digital abrange expressamente os "órgãos de pesquisa" definidos no art. 5º, XVIII, da LGPD, garantindo segurança jurídica e preservando a coerência interpretativa entre as legislações.

Adicionalmente, sugerimos que a ANPD esclareça os requisitos procedimentais para que essas instituições possam requerer os dados agregados mencionados no art. 31, estabelecendo: modelo de requerimento padronizado; prazo razoável para fornecimento pelos fornecedores (ex: 30 dias); formato e granularidade mínima dos dados agregados a serem fornecidos; mecanismo de resolução de conflitos quando houver recusa de fornecimento.

4. Bases legais para tratamento de dados de crianças e adolescentes - Harmonização entre ECA Digital, LGPD e Enunciado CD/ANPD nº 1/2023

O art. 9º do ECA Digital estabelece que "o tratamento de dados pessoais de crianças e adolescentes deverá observar o seu melhor interesse e será realizado exclusivamente para a proteção e garantia dos seus direitos". Adicionalmente, diversos dispositivos do ECA Digital fazem referência ao "consentimento" (arts. 13, § 2º; 14; 15, entre outros).

Essa redação pode gerar dúvidas sobre quais bases legais da LGPD são aplicáveis ao tratamento de dados de crianças e adolescentes no contexto do ECA Digital, especialmente considerando que a LGPD prevê dez bases legais para dados pessoais comuns (art. 7º) e dez para dados sensíveis (art. 11º), além do consentimento.

Organizações da sociedade civil que atuam na proteção de direitos de crianças e adolescentes frequentemente tratam dados desse público para finalidades como: prestação de serviços de assistência social, educação ou saúde; execução de políticas públicas em parceria com o Estado; realização de pesquisas científicas sobre direitos da infância; defesa de direitos e advocacy baseado em evidências; cumprimento de obrigação legal ou regulatória (ex: Cadastro Único, SUAS, registros exigidos por conselhos tutelares).

Em muitos desses casos, o consentimento não é a base legal mais adequada ou mesmo viável, sendo necessário recorrer a outras hipóteses como execução de políticas públicas (art. 7º, VIII), exercício regular de direitos (art. 7º, VI), proteção da vida (art. 7º, VII), tutela da saúde (art. 11, II, "f"), ou cumprimento de obrigação legal (art. 7º, II), para citar alguns exemplos.

O Enunciado CD/ANPD nº 1, de 22 de maio de 2023, já estabeleceu interpretação oficial sobre esta questão:

"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 prevalente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

Este Enunciado esclarece, de forma definitiva, que:

- Todas as bases legais da LGPD são aplicáveis ao tratamento de dados de crianças e adolescentes;
- O diferencial reside na necessidade de que o melhor interesse seja observado e prevalente;
- O melhor interesse deve ser avaliado no caso concreto, conforme art. 14 da LGPD.

Esta interpretação é essencial para viabilizar a atuação de organizações da sociedade civil na proteção de direitos de crianças e adolescentes, pois muitas dessas organizações não conseguiriam operar adequadamente se limitadas exclusivamente ao consentimento como base legal.

Recomendamos que a ANPD, ao elaborar Guias Orientativos ou Regulamentação sobre o ECA Digital, esclareça expressamente:

- (a) Reafirmação da aplicabilidade do Enunciado nº 1/2023 ao contexto do ECA Digital: o Enunciado nº 1/2023 permanece plenamente aplicável mesmo após a entrada em vigor do ECA Digital, devendo ser lido em conjunto com as disposições da nova lei. O requisito do "melhor interesse" previsto no art. 9º do ECA Digital harmoniza-se com o Enunciado, não o substitui ou restringe.
- (b) Esclarecimento sobre organizações da sociedade civil sem fins lucrativos: organizações da sociedade civil que prestam serviços de assistência social, educação, saúde ou proteção de direitos de crianças e adolescentes podem basear o tratamento de dados em hipóteses legais como:
 - Execução de políticas públicas (art. 7º, VIII e art. 11, II, "b" da LGPD), quando em parceria com o Poder Público mediante instrumentos previstos na Lei nº 13.019/2014 (MROSC);
 - Tutela da saúde (art. 11, II, "f" da LGPD), quando a organização presta serviços de saúde;
 - Exercício regular de direitos (art. 7º, VI e art. 11, II, "d" da LGPD), quando o tratamento é necessário para defesa de direitos em processos administrativos ou judiciais;

- Proteção da vida (art. 7º, VII e art. 11, II, "e" da LGPD), em situações de vulnerabilidade ou risco;
 - Cumprimento de obrigação legal (art. 7º, II e art. 11, II, "a" da LGPD), quando exigido por legislação específica.
- (c) Requisitos para avaliação do "melhor interesse" por organizações da sociedade civil: entendemos que a avaliação do melhor interesse deve considerar:
- A finalidade institucional da organização e seu histórico de atuação na proteção de direitos;
 - A adequação entre o tratamento de dados e a proteção ou promoção de direitos fundamentais da criança ou adolescente;
 - A proporcionalidade entre os dados tratados e a finalidade perseguida (princípio da necessidade);
 - A existência de salvaguardas de segurança e confidencialidade adequadas;
 - A impossibilidade ou inadequação de alcançar a mesma finalidade sem o tratamento de dados.
- (d) Interação entre consentimento parental e outras bases legais: quando o ECA Digital exige "consentimento" em dispositivos específicos (ex: art. 14 - sistemas de recomendação; art. 15 - geolocalização), este se soma à necessidade de base legal da LGPD, não a substitui. Assim:
- Para tratamentos previstos no ECA Digital que exigem consentimento, este deve ser obtido dos pais/responsáveis (consentimento parental do ECA Digital);
 - Adicionalmente, deve haver base legal adequada da LGPD para o tratamento;
 - Na maioria dos casos, a base legal adequada da LGPD será o próprio consentimento (art. 7º, I ou art. 11, I), mas harmonizado com o consentimento parental do ECA Digital.
- (e) Situações em que o consentimento é dispensável: mesmo no contexto do ECA Digital, há situações em que o consentimento parental é dispensável, em consonância com o Enunciado nº 1/2023 e com o próprio Estatuto da Criança e do Adolescente (Lei nº 8.069/90), tais como:
- Cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II da LGPD) - ex: envio de dados ao Cadastro Único, SUAS, Censo Escolar;
 - Execução de políticas públicas previstas em lei (art. 7º, VIII da LGPD) - quando a organização atua em parceria formal com o Poder Público;
 - Proteção da vida ou incolumidade física da criança/adolescente (art. 7º, VII e art. 11, II, "e" da LGPD) - em situações de emergência ou risco;

- Exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI e art. 11, II, "d" da LGPD) - quando o tratamento é necessário para defesa de direitos.

Nestas hipóteses, o "melhor interesse" continua sendo requisito obrigatório de avaliação, mas o consentimento não é necessário.

Ressaltamos que esta harmonização é crucial para que organizações da sociedade civil possam continuar desempenhando seu papel essencial na proteção de direitos de crianças e adolescentes. Sem clareza sobre a aplicabilidade de bases legais além do consentimento, muitas organizações poderiam:

- Interromper programas de assistência social por impossibilidade de obter consentimento de todos os responsáveis;
- Deixar de realizar pesquisas científicas essenciais para formulação de políticas públicas;
- Comprometer a defesa de direitos em processos judiciais e administrativos por receio de violar a proteção de dados;
- Descontinuar parcerias com o Poder Público na execução de políticas públicas.

Recomendamos, portanto, que a ANPD priorize a elaboração de Guia Orientativo específico sobre a aplicação do Enunciado nº 1/2023 no contexto do ECA Digital, com exemplos práticos voltados às situações enfrentadas por organizações da sociedade civil.

5. Outros conceitos que demandam esclarecimento:

Considerando a limitação de tempo para esta contribuição (prazo até 12/12/2025), destacamos brevemente outros conceitos do ECA Digital que merecem atenção regulatória futura:

- (a) "Produto ou serviço de tecnologia da informação" (art. 2º, I c/c § 2º): embora o ECA Digital defina esse conceito, a exclusão das "funcionalidades essenciais para o funcionamento da internet" (§ 2º) demanda maior precisão. Sugerimos que a ANPD elabore lista exemplificativa do que são "protocolos e padrões técnicos abertos e comuns", evitando interpretações que restrinjam indevidamente o âmbito de aplicação da lei.
- (b) "Mecanismo de supervisão parental" (art. 2º, VIII): O conceito é definido de forma ampla como "conjunto de configurações, ferramentas e salvaguardas tecnológicas". Recomendamos que a ANPD estabeleça requisitos mínimos de funcionalidade desses mecanismos, considerando diferentes faixas etárias (crianças vs. adolescentes) e os princípios da progressiva autonomia e participação de crianças e adolescentes previstos no ECA.
- (c) "Serviço com controle editorial" (art. 2º, IX) e "Provedores de conteúdos protegidos por direitos autorais" (art. 39, § 1º): Esses conceitos são centrais para definir exceções à aplicação

de determinadas obrigações do ECA Digital. Sugerimos que a ANPD esclareça que "controle editorial" implica curadoria humana significativa sobre o conteúdo disponibilizado, não bastando moderação automatizada ou remoção reativa de conteúdo. Quanto aos "conteúdos protegidos por direitos autorais", sugerimos esclarecimento sobre se a exceção se aplica apenas a plataformas de streaming tradicionais (ex: Netflix, Spotify) ou também a plataformas híbridas com conteúdo editorial e *user-generated content*.

- (d) "Expressão do melhor interesse da criança e do adolescente" (art. 5º, § 2º): O ECA Digital lista elementos que constituem expressão desse princípio constitucional. Recomendamos que a ANPD esclareça como fornecedores devem documentar e demonstrar que suas práticas de tratamento de dados efetivamente promovem esses elementos, considerando a necessidade de avaliações de impacto específicas sobre direitos de crianças e adolescentes (*Children's Rights Impact Assessment*).

CONSIDERAÇÕES FINAIS

A regulamentação dos conceitos do ECA Digital pela ANPD é oportunidade essencial para garantir que a lei alcance sua finalidade de proteção integral de crianças e adolescentes no ambiente digital, sem impor ônus desproporcionais a organizações que atuam justamente na promoção desses direitos.

Legislações internacionais consolidadas, como o *California Age-Appropriate Design Code Act* dos EUA, as *Guidelines 2/2024* do *European Data Protection Board* sobre processamento de dados de crianças⁸ e o *Age Appropriate Design Code* do Reino Unido (*Children's Code* da ICO)⁹, oferecem parâmetros concretos que podem inspirar a regulamentação brasileira, sempre com as adaptações necessárias ao nosso contexto legal e cultural.

A harmonização com a LGPD é igualmente fundamental, especialmente no que diz respeito aos conceitos de "órgão de pesquisa", bases legais para tratamento de dados de crianças e adolescentes, e requisitos de segurança da informação. Essa harmonização previne conflitos normativos e garante aos agentes econômicos e às organizações da sociedade civil um ambiente regulatório coerente e previsível.

A harmonização entre o ECA Digital, a LGPD e o Enunciado CD/ANPD nº 1/2023 é elemento central para garantir que a nova legislação alcance seus objetivos de proteção integral sem inviabilizar

⁸ EUROPEAN DATA PROTECTION BOARD (EDPB). Guidelines 2/2024 on processing of personal data of children. Version 1.0, adotada em 26 de outubro de 2024. Disponível em: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf. Acesso em: 12 dez. 2025

⁹ INFORMATION COMMISSIONER'S OFFICE (ICO). Age-appropriate design: a code of practice for online services. Version 1.1, atualizada em outubro de 2021. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/?search=consent>. Acesso em: 12 dez. 2025.

o trabalho de organizações que atuam justamente na promoção desses direitos. O Enunciado nº 1/2023 representa avanço significativo ao esclarecer que todas as bases legais da LGPD são aplicáveis, desde que observado o melhor interesse da criança e do adolescente. Esta interpretação deve ser reafirmada e detalhada no contexto do ECA Digital.

Por fim, reiteramos que organizações da sociedade civil que atuam na proteção de crianças e adolescentes – como institutos de pesquisa, fundações de defesa de direitos, associações de educação e entidades de assistência social – devem ser consideradas nas regulamentações da ANPD como agentes essenciais ao ecossistema de proteção integral, merecendo tratamento que facilite, e não obstrua, seu acesso a dados necessários para suas missões institucionais.

Sendo assim, prestada nossa contribuição à Tomada de Subsídios, permanecemos à disposição para quaisquer esclarecimentos adicionais e para participação em eventuais audiências públicas sobre o tema.

Aproveitamos a oportunidade para renovar nossos agradecimentos pela abertura deste processo participativo e reafirmar nosso compromisso com a proteção de dados pessoais de crianças e adolescentes e com o fortalecimento do marco regulatório brasileiro.

Atenciosamente,

p. Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados (SBSA Advogados)

Laís de Figueirêdo Lopes
OAB/SP nº 182.480

Pedro Henrique Monteiro de Barros da Silva Néto
OAB/SP nº 488.756

Beatriz da Fonseca Massa
OAB/SP nº 510.162

Maíra Vasconcelos Silva
OAB/SP nº 499.713

Brasscom
Considerações à Tomada de Subsídios para esclarecer
conceitos do ECA Digital

Dezembro, 2025

A **Brasscom – Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais** – é uma entidade sem fins lucrativos de representatividade nacional que congrega algumas das mais dinâmicas e inovadoras empresas de TIC alinhadas com a Era Digital. Por meio deste documento, a Associação compartilha considerações sobre o Regulamento sobre o Uso Compartilhado de Dados Pessoais pelo Poder Público.

Introdução

A Brasscom gostaria de parabenizar a abertura da tomada de subsídios pela ANPD para discutir os principais conceitos, termos e expressões do Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025), no entendimento de que representa um passo fundamental para assegurar a correta compreensão e aplicação do novo marco legal. Trata-se de um diploma que inaugura direitos, deveres e salvaguardas específicos para a proteção de crianças e adolescentes no ambiente digital, mas que, ao fazê-lo, introduz também no ordenamento um conjunto de termos que ainda carecem de maior precisão técnica e conceitual. Diante disso, a iniciativa da Agência é especialmente relevante para identificar eventuais ambiguidades, mapear lacunas interpretativas e colher insumos da

sociedade para calibrar o alcance de dispositivos centrais da lei. Ao se discutir quais conceitos demandam esclarecimentos adicionais — e quais parâmetros devem orientar sua precisão — cria-se uma base regulatória mais clara, aplicável e proporcional, evitando distorções na implementação do ECA Digital e garantindo que seus objetivos de proteção sejam plenamente alcançados.

1) Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Dispositivo	Conceito Impreciso	Parâmetro Interpretativo Sugerido
Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.	“De acesso provável”	A lei adota uma aplicação excessivamente ampla ao abranger qualquer serviço “de acesso provável por crianças e adolescentes”, sem diferenciar os diversos níveis de risco entre eles, o que leva a tratar, de forma igual, serviços com perfis de risco radicalmente distintos. Uma alternativa mais adequada seria adotar uma abordagem verdadeiramente baseada em risco, como no Artigo 28 do DSA europeu, considerando fatores como finalidade do serviço, natureza do conteúdo, funcionalidades, público-alvo, presença significativa de menores, estratégias de mitigação e características de acesso. Assim, recomenda-

		se que orientações regulamentares delimitem o alcance apenas a serviços que representem risco significativo e garantam flexibilidade proporcional ao perfil de risco, além de deixar claro que obrigações devem recair somente sobre serviços destinados a menores ou sobre as partes voltadas a esse público.
Art. 1º, Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações: I – suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes;	“Suficiente probabilidade de uso e atratividade”	Esclarecer os critérios que configurariam a “suficiente probabilidade de uso e atratividade” mencionada no art. 1º, I. Como parâmetros, poderiam ser adotados, por exemplo: - o critério da popularidade entre menores (quantidade de acessos, downloads, engajamento);

II – considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes;	"Considerável facilidade ao acesso"	A expressão é subjetiva e pode gerar dúvidas sobre quando um serviço deve ser enquadrado nesse conceito. O que é "considerável"? Como parâmetro, poderia ser adotado, por exemplo: - a quantidade de etapas para acessar (ex.: login simples vs. aferição robusta); e - a disponibilidade em lojas de aplicativos (gratuito vs. pago);
III – significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital.	"Significativo grau de risco" "Larga escala"	A expressão é subjetiva e pode gerar dúvidas sobre quando um serviço deve ser enquadrado nesse conceito. Não está claro o que tornaria o risco "significativo", nem o conceito de "larga escala" neste contexto. Por exemplo, seria um critério quantitativo (probabilidade estatística de dano)? Ou qualitativo (gravidade do dano, mesmo que raro)? Como parâmetro, poderia ser adotado, por exemplo: - avaliar tipo de interação (chat, compartilhamento); - coleta de dados sensíveis; - histórico de incidentes, dentre outros;

Art. 7º [...] § 1º O produto ou serviço referido no caput deste artigo deverá, por padrão, operar com o grau mais elevado de proteção da privacidade e dos dados pessoais, observado que será obrigatória a disponibilização de informações claras, acessíveis e adequadas para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à eventual adoção de configurações menos protetivas.	"O grau mais elevado de proteção da privacidade e dos dados pessoais" e "Disponibilização de informações claras, acessíveis e adequadas"	O Artigo 7º e dispositivos correlatos impõem às empresas a obrigação de operar com "o grau mais elevado de proteção da privacidade e dos dados pessoais", mas o termo não é definido, gerando incerteza sobre quais práticas devem ser adotadas na configuração padrão de serviços destinados a menores — especialmente no que diz respeito à publicidade, marketing e compartilhamento de dados com terceiros. Nesse sentido, importante que a ANPD construa parâmetros orientativos sobre o que deverá ser considerado no contexto do privacy by design para crianças e adolescentes. Também não há clareza sobre o que caracteriza informações "claras, acessíveis e adequadas" para permitir escolhas informadas por menores e seus responsáveis. Por isso, recomenda-se que as orientações regulatórias esclareçam tanto quais controles compõem esse "grau mais elevado de proteção" quanto que a inclusão de uma seção específica sobre menores na política de privacidade seja considerada suficiente para atender ao requisito de informação clara, acessível e adequada.

Art. 8º [...] V – informar extensivamente a todos os usuários sobre a faixa etária indicada para o produto ou serviço no momento do acesso, conforme estabelecido pela política de classificação indicativa. Art. 9º [...] § 1º Para dar efetividade ao disposto no caput, deverão ser adotados mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração.	"No momento/ a cada acesso do usuário"	Necessário esclarecer, de forma objetiva, o que se entende como "no momento/ a cada acesso do usuário", pois a interpretação é subjetiva dependendo da atividade realizada por cada agente.
Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o	"Conteúdo impróprio ou inadequado para menores"	O artigo 9º inclui referência a conteúdo que seja "impróprio, inadequado ou proibido para menores de 18 anos". Essa abordagem é ambígua e pode criar desafios significativos para serviços de conteúdo literário. Sem limites de definição claros, esses descritores subjetivos poderiam abranger praticamente qualquer tema adulto na literatura, incluindo obras com significado educacional, histórico ou cultural significativo. A orientação deve

seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos. § 2º Para os fins desta Lei, consideram-se impróprios ou inadequados para crianças e adolescentes os produtos, serviços ou conteúdos de tecnologia da informação que contenham material pornográfico, ou quaisquer outros vedados pela legislação vigente.		ênfatizar que o escopo do conteúdo “impróprio, inadequado ou proibido” se aplica apenas ao conteúdo de natureza pornográfica ou <u>explicitamente proibido</u> pela legislação brasileira vigente para menores de idade. Também recomendamos que a ANPD reconheça a natureza sugestiva da classificação indicativa do Ministério da Justiça atualmente existente, que não possui natureza obrigatória nem caráter de vedação, servindo apenas como um instrumento orientador destinado a informar pais, responsáveis e o próprio público sobre a adequação etária dos conteúdos. Trata-se de uma referência para apoiar escolhas mais conscientes, sem impor censura, restrições compulsórias ou proibições absolutas de acesso. Além disso, no que diz respeito ao Artigo 9º, §2º, a orientação deve ser precisa na definição de conteúdo “pornográfico” para distinguir entre material explícito destinado principalmente à excitação sexual e obras literárias que incluem temas sexuais adultos como parte de contextos narrativos, educacionais, históricos ou culturais mais amplos. Sem esse esclarecimento, existe o risco de que obras literárias legítimas e valiosas possam ser indevidamente classificadas como materiais pornográficos.

Art. 12. Os provedores de lojas de aplicações de internet e de sistemas operacionais de terminais deverão: [...] III – possibilitar, por meio de Interface de Programação de Aplicações (Application Programming Interface – API) segura e pautada pela proteção da privacidade desde o padrão, o fornecimento de sinal de idade aos provedores de aplicações de internet, exclusivamente para o cumprimento das finalidades desta Lei e com salvaguardas técnicas adequadas.	“Fornecimento de sinal de idade”	A lei impõe requisitos uniformes a todos os sistemas operacionais e lojas de aplicativos, desconsiderando que diferentes dispositivos apresentam níveis muito distintos de risco para menores. Enquanto celulares e tablets pessoais oferecem ampla navegação e exposição a conteúdo variado, muitos sistemas operacionais operam em dispositivos compartilhados ou de uso restrito — como TVs conectadas, assistentes inteligentes ou eReaders — cujo desenho e uso cotidiano reduzem significativamente o risco de acesso indevido. Além disso, não há hoje infraestrutura técnica capaz de transmitir sinais de idade entre sistemas e serviços, e o prazo previsto torna inviável desenvolver soluções confiáveis. Por isso, recomenda-se que as orientações regulamentares adotem uma abordagem baseada em risco, diferenciando dispositivos de alto risco (pessoais, com telas e navegação ampla) daqueles de risco reduzido (domésticos compartilhados ou com navegação limitada), permitindo exigências proporcionais e isenções quando apropriado. As orientações também devem reconhecer que medidas adequadas para um celular não se aplicam a TVs conectadas ou eReaders, esclarecer o escopo das lojas de aplicativos e estender os prazos de implementação para viabilizar o desenvolvimento de padrões e infraestrutura técnica.

Art. 13. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito.	"Vedado seu tratamento para qualquer outro propósito"	A ANPD deverá esclarecer que a vedação prevista aplica-se exclusivamente ao contexto específico da coleta de dados pessoais de crianças e adolescentes para fins de verificação de idade. Trata-se de uma limitação circunscrita a essa finalidade determinada, não alcançando outras operações de tratamento legítimas e previstas na legislação. Esse esclarecimento é essencial para evitar interpretações ampliadas ou equivocadas que possam restringir indevidamente atividades regulares de tratamento de dados, assegurando segurança jurídica aos agentes e coerência com os princípios da necessidade, finalidade e proporcionalidade.
Art. 15. O cumprimento das obrigações previstas neste Capítulo não exime os demais agentes da cadeia digital das suas responsabilidades legais, cabendo a todos os envolvidos garantir de forma solidária a proteção integral de crianças e de adolescentes.	"Esclarecer que a responsabilidade solidária se refere exclusivamente a mecanismos de aferição de idade"	É importante esclarecer que a responsabilidade solidária prevista na lei deve ser interpretada exclusivamente no contexto dos mecanismos de aferição de idade, pois os sistemas operacionais e as lojas de aplicações atuam apenas como infraestrutura técnica e não têm visibilidade, controle ou capacidade de moderação sobre o conteúdo acessado por meio de seus dispositivos. As obrigações dirigidas a provedores de conteúdo — que hospedam, selecionam ou disponibilizam conteúdo diretamente aos usuários — não são tecnicamente viáveis nem proporcionais quando aplicadas a intermediários de infraestrutura. Recomenda-se, portanto, a inclusão de orientações

		adicionais assegurando que a solidariedade prevista no art. 15 se restrinja às obrigações do Capítulo IV, relativas aos mecanismos de aferição de idade, evitando interpretações que ampliem indevidamente o escopo de deveres para atores que não controlam conteúdo.
Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão: § 4º As configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo V – controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação	"Mais alto nível de proteção disponível" "Sistemas de recomendação personalizados"	Necessidade de esclarecer o que seria "o mais alto nível de proteção disponível" de modo que se tenha critérios orientativos a serem considerados sem que, contudo, a ANPD estabeleça critérios prescritivos e que sejam "one size fits all". Além disso, a lei presume que todos os sistemas de recomendação personalizados representam risco para menores, mas esses sistemas têm finalidades muito distintas e não devem ser tratados de forma uniforme. Em muitos serviços, a personalização simplesmente ajuda o usuário a navegar por grandes catálogos e encontrar conteúdo adequado à idade, cumprindo uma função essencial e não voltada a aumentar engajamento. Já sistemas projetados para ampliar tempo de uso ou promover conteúdo viral apresentam riscos maiores. Por isso, recomenda-se que as orientações regulatórias diferenciem sistemas segundo sua finalidade e seu potencial de dano, impondo controles mais rígidos apenas àqueles voltados a maximizar engajamento ou expor

		menores a conteúdo prejudicial. A regulação deve focar práticas de design nocivas — e não a personalização em si — preservando sistemas que melhoram a experiência ao facilitar o acesso a conteúdo apropriado.
Art. 17. [...] § 4º [...] VIII – revisão regular das ferramentas de inteligência artificial, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas;	“Inteligência Artificial”	A ANPD deve esclarecer que, no âmbito do ECA Digital, sua obrigação regulatória não consiste em avaliar o funcionamento específico ou os resultados concretos das ferramentas de IA utilizadas pelos fornecedores. A obrigação dos agentes, e, portanto, o foco da atividade regulatória e fiscalizatória da agência, limita-se a assegurar que esses fornecedores adotem mecanismos de revisão regular das tecnologias empregadas, de forma a verificar continuamente sua adequação, segurança e conformidade com a legislação. Assim, o foco regulatório está no processo de governança e monitoramento das ferramentas de IA — e não em uma validação de mérito sobre o que cada sistema faz ou como opera em detalhe.

Art. 22. Para além das demais disposições desta Lei, é vedada a utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e a adolescentes, bem como o emprego de análise emocional, de realidade aumentada, de realidade estendida e de realidade virtual para esse fim.	“Técnicas de perfilamento para direcionamento de publicidade comercial”	A ANPD deve esclarecer que a vedação ao uso de técnicas de perfilamento no ECA Digital é restrita à finalidade específica de veiculação de publicidade comercial direcionada a crianças e adolescentes. O perfilamento permanece permitido para outras finalidades legítimas e necessárias, como segurança, prevenção à fraude, detecção de riscos, integridade de serviços e demais operações compatíveis com a proteção do interesse do usuário. É igualmente importante definir com precisão o que se entende por publicidade comercial, distinguindo-a de outros tipos de comunicação digital — como mensagens institucionais, informativas ou de utilidade pública — e separar claramente as práticas de curadoria ou recomendação de conteúdo. Recomendações personalizadas que têm como objetivo melhorar a experiência do usuário e organizar o conteúdo disponível não devem ser confundidas com publicidade, desde que não envolvam promoções ou estímulos comerciais direcionados. Além disso, a ANPD deve esclarecer que a publicidade contextual — aquela baseada exclusivamente no conteúdo da página ou do vídeo que está sendo visualizado, sem uso de perfil comportamental do usuário — é permitida, pois

		não envolve monitoramento prévio nem construção de perfis individuais.



CONTRIBUIÇÕES A TOMADA DE SUBSÍDIOS DA ANPD DESTINADA A ESCLARECER CONCEITOS DO ECA DIGITAL

SUMÁRIO

I. INTRODUÇÃO.....	1
II. ACESSO PROVÁVEL POR CRIANÇAS E ADOLESCENTES.....	2
III. PERFILAMENTO.....	4
IV. LOJA DE APLICAÇÕES DE INTERNET.....	6
V. MECANISMO DE SUPERVISÃO PARENTAL.....	8
VI. MELHOR INTERESSE DA CRIANÇA E DO ADOLESCENTE.....	10
VII. CONTEÚDO PORNOGRÁFICO E MATERIAL PORNOGRÁFICO.....	11
VIII. CONTEÚDO IMPRÓPRIOS OU INADEQUADOS PARA CRIANÇAS E ADOLESCENTES.....	13
IX. PUBLICIDADE COMERCIAL.....	17
X. CONTEÚDOS VIOLADORES DE DIREITOS DE CRIANÇAS E ADOLESCENTES.....	19
XI. CONDIÇÃO PECULIAR DE PESSOA EM DESENVOLVIMENTO.....	20
XII. VERIFICAÇÃO DE IDADE VS. AFERIÇÃO DE IDADE.....	22

I. INTRODUÇÃO

Esta contribuição é apresentada à Agência Nacional de Proteção de Dados (ANPD) no âmbito da Tomada de Subsídios destinada a esclarecer conceitos do ECA Digital (Lei nº 15.211/2025). Alinhado ao escopo definido pela Agência, o objetivo central deste documento é apontar e discutir eventuais dúvidas, ambiguidades e dubiedades de terminologia presentes na lei, que possam dificultar seu pleno entendimento e aplicação em ambientes digitais.

Para tanto, foram selecionados termos e conceitos que, pela sua centralidade no sistema normativo do ECA Digital e pela ausência de parâmetros interpretativos, demandam atenção prioritária da ANPD. Cada termo ou conceito objeto de análise segue estrutura uniforme de contribuição composta por: problemática; esclarecimento; e justificativa. Os temas alvo de análise podem ser encontrados no Sumário acima.

Esta contribuição busca apoiar a ANPD na construção de uma regulamentação que ofereça segurança jurídica, facilite a implementação do ECA Digital e, em última análise, assegure sua efetividade na proteção de crianças e adolescentes. Colocamo-nos à disposição da Agência para aprofundar o debate técnico e contribuir com os próximos passos desse processo regulatório.

II. ACESSO PROVÁVEL POR CRIANÇAS E ADOLESCENTES

Dispositivo: art. 1º, parágrafo único, incisos I a III

Problemática

O art. 1º do ECA Digital estabelece que a lei "aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles". O parágrafo único define "acesso provável" através de três critérios: (i) "suficiente probabilidade de uso e atratividade" do produto ou serviço por crianças e adolescentes; (ii) "considerável facilidade ao acesso e utilização" por esse público; e (iii) "significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial".

A problemática central reside na indefinição dos conceitos estruturantes dessa definição. As expressões "suficiente probabilidade", "considerável facilidade" e "significativo grau de risco" são vagas e carecem de parâmetros orientativos para sua aplicação, gerando insegurança jurídica sobre o escopo de aplicabilidade da lei. Há risco de interpretações excessivamente amplas, que enquadrem praticamente qualquer serviço digital acessível pela internet como de "acesso provável" por crianças e adolescentes, assim como de interpretações excessivamente restritivas, que deixem de abranger serviços que efetivamente mereceriam atenção.

Ademais, há indefinição sobre a relação entre os três critérios. O parágrafo único utiliza a conjunção "e" ao final dos incisos I e II, sugerindo cumulatividade, mas não há clareza sobre se todos os três critérios devem de fato estar presentes simultaneamente para caracterizar "acesso provável" ou se a presença de qualquer um deles seria suficiente. Essa indefinição tem impactos significativos sobre a amplitude do escopo de aplicabilidade.

Esclarecimento

A ANPD deve trazer elementos suficientes para a adequada aplicação dos três critérios que compõem a definição de "acesso provável" estabelecida no parágrafo único do art. 1º, fornecendo parâmetros orientativos que permitam aos fornecedores avaliar se seus produtos ou serviços enquadram-se no escopo de aplicabilidade da lei.

É fundamental estabelecer que "acesso provável" não se confunde com "acesso possível" ou "acesso tecnicamente viável". Virtualmente todo serviço online é tecnicamente acessível por crianças e adolescentes, mas isso não significa que todos tenham acesso provável por esse público. A probabilidade deve ser avaliada com base em evidências



concretas de uso efetivo ou em características do serviço que indiquem atratividade e facilidade para esse público específico.

O regulamento - ou guia orientativo - deve explicitar o significado - ou ao menos fornecer orientações para sua interpretação - de cada um dos três critérios: (i) o que caracteriza "suficiente probabilidade de uso e atratividade"; (ii) o que constitui "considerável facilidade ao acesso e utilização"; e (iii) como avaliar se há "significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial".

Quanto à relação entre os critérios, o texto legal utiliza a conjunção "e" ao final dos incisos I e II, indicando que são cumulativos. Um serviço só estaria no escopo se apresentasse simultaneamente: probabilidade de uso E facilidade de acesso E risco significativo. Essa interpretação cumulativa é a mais coerente com a literalidade do dispositivo e com a necessidade de evitar escopo excessivamente amplo que alcance serviços sem probabilidade real de uso por crianças e adolescentes. A ANPD deve reconhecer expressamente a cumulatividade dos critérios.

Justificativa

A definição de “acesso provável” requer esclarecimento porque o parágrafo único utiliza expressões vagas que não oferecem parâmetros operacionais para que fornecedores determinem, com segurança, se estão sujeitos ao ECA Digital. Sem balizas claras, há risco especialmente de sobreenquadramento por excesso de cautela, comprometendo a proporcionalidade regulatória.

Considerando a amplitude dos termos empregados nos incisos do parágrafo único do artigo 1º, há risco concreto de interpretações excessivamente amplas que levem ao enquadramento de praticamente qualquer serviço online como de “acesso provável”, partindo da premissa de que crianças e adolescentes usam amplamente a internet, de que qualquer serviço é tecnicamente acessível a esse público e de que todo serviço pode apresentar algum grau de risco, mesmo que remoto. Essa leitura ampliaria indevidamente o escopo da lei e incluiria serviços que, embora eventualmente acessados por menores, não apresentam probabilidade real ou significativa de uso.

A experiência do ICO¹ demonstra a importância e a viabilidade de elucidar conceitos vagos relacionados a “acesso provável”. No Age Appropriate Design Code, que utiliza expressão similar (“likely to be accessed by children”), o ICO identificou que a falta de definição gerava insegurança jurídica e, para enfrentá-la, desenvolveu orientação detalhada com metodologia estruturada de avaliação de enquadramento.

¹<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/>



Esse guia orientativo fornece lista não exaustiva de fatores que devem ser considerados, como: evidências concretas (dados demográficos, padrões de acesso, reclamações, publicidade direcionada); características do serviço (conteúdo, design, gamificação, presença de influenciadores); pesquisas externas sobre serviços similares; e modelo de negócio.

O ICO também disponibilizou estudos de caso que demonstram a aplicação prática desses critérios (plataformas de namoro, sites de conteúdo adulto, jogos, redes sociais, sites de pequenas empresas) e criou ferramenta de autoavaliação que orienta fornecedores por meio de perguntas estruturadas, permitindo determinações fundamentadas e reduzindo custos de conformidade, especialmente para pequenos provedores.

A adoção de orientação semelhante no contexto do ECA Digital preserva a coerência regulatória, reduz incertezas e assegura que o escopo da lei seja direcionado aos serviços que representam risco real para o público infantojuvenil, evitando tanto lacunas quanto encargos desproporcionais.

III. PERFILAMENTO

Dispositivo: Art. 2º, V

Problemática

O ECA Digital define perfilamento como qualquer tratamento de dados destinado a classificar pessoas e produzir inferências, mas utiliza termos que exigem interpretação, como o alcance de “automatizado ou não”, o significado de “classificar em grupo ou perfil”, o conceito de “inferências” e a amplitude de “outras características assemelhadas”, o que gera incerteza sobre o alcance do conceito.

Soma-se a isso o risco de leitura excessivamente ampla das vedações dos arts. 22 e 26, que, cabe lembrar, se referem exclusivamente ao perfilamento para direcionamento de publicidade comercial. Caso interpretadas de forma expansiva, essas vedações poderiam atingir não só práticas legítimas, mas como aquelas necessárias para o próprio cumprimento do ECA Digital, prejudicando a eficácia das obrigações legais e, em última análise, o atingimento do melhor interesse da criança e do adolescente, apresentando ainda risco de incertezas, e erros materiais, na discussão de perfilamento no contexto da LGPD.



Esclarecimento

A ANPD deve esclarecer o escopo dos elementos do art. 2º, V, bem como reconhecer que as vedações dos arts. 22 e 26 se limitam ao uso de perfilamento para publicidade comercial, exclusivamente. Fora dessa hipótese, o perfilamento deve ser admitido sempre que estiver alinhado ao melhor interesse da criança e do adolescente, conceito que envolve proteção integral e abrange não apenas segurança, mas também desenvolvimento, participação, inclusão, acessibilidade, autonomia progressiva, fruição cultural e liberdade de expressão.

Assim, além das obrigações previstas pelo ECA Digital que dependem de técnicas de classificação e inferência, o perfilamento também pode ser empregado de forma legítima para finalidades que ampliam a experiência segura e inclusiva para crianças e adolescentes, como personalização de ambientes, adaptação gradual de interfaces à maturidade do usuário e recomendações de conteúdos adequados ao estágio de desenvolvimento. O perfilamento não é, por si só, prática negativa; seu risco decorre do contexto de uso. Desde que não sirva ao direcionamento de publicidade comercial e respeite o melhor interesse em sua dimensão ampla, ele é compatível com os objetivos do ECA Digital e tal reforço pela ANPD seria bastante importante.

Justificativa

O esclarecimento é essencial para compatibilizar as vedações com as obrigações previstas pela lei e evitar interpretação que impeça práticas imprescindíveis à proteção infanto-juvenil.

Diversas obrigações dependem de técnicas de classificação e inferência: o art. 8º, II e III exige adequação de conteúdo à faixa etária e bloqueio de materiais inadequados; o art. 6º demanda identificação de padrões de risco; o art. 27 envolve detecção de abuso sexual; o art. 17, § 4º, V, pressupõe sistemas de recomendação; e o art. 12 exige aferição de idade.

Além disso, a LGPD e diversas regulações internacionais não proíbem o perfilamento de forma absoluta, mas condicionam seu uso à finalidade legítima e a salvaguardas adequadas. Cabe à ANPD, portanto, reconhecer que a proibição se restringe ao uso para publicidade comercial e que o perfilamento é permitido - e necessário - nas demais circunstâncias compatíveis com o melhor interesse da criança e do adolescente.

IV. LOJA DE APLICAÇÕES DE INTERNET

Dispositivo: art. 2º, inciso VI



Problemática

O ECA Digital define “lojas de aplicações de internet” como sendo a aplicação “*que distribui e facilita o download, para usuários de terminais, de aplicações de internet disponibilizadas ou tornadas acessíveis por meio de sua plataforma*”. No entanto, essa conceituação, embora aparente descrever as lojas de aplicativos mais conhecidas (como as de celulares e tablets), acaba sendo ampla e gerando dúvidas importantes sobre quem exatamente se enquadraria nessa categoria e estaria sujeito às obrigações previstas na lei. O texto não esclarece o que significa exatamente “distribuir e facilitar o download”. Isso abre espaço para interpretar que uma loja seria tanto uma plataforma altamente controlada, com curadoria e regras próprias, quanto um simples ambiente que organiza links ou permite acesso indireto a softwares de terceiros. A referência às aplicações “disponibilizadas ou tornadas acessíveis” também traz incertezas, uma vez que também poderiam vir a ser incluídos no conceito extensões de navegador, miniaplicações em plataformas de jogos, plug-ins e add-ons, ainda que a plataforma não funcione como uma loja no sentido tradicional.

Ademais, o texto legal não deixa claro se sistemas operacionais, navegadores, plataformas de conteúdo ou ambientes corporativos internos poderiam ser interpretados como lojas, já que muitos deles também “facilitam downloads” de alguma maneira. Essa indefinição amplia excessivamente o alcance da lei e torna difícil identificar com precisão quem é o regulado. Nesse sentido, o conceito trazido atualmente pode vir a alcançar tanto serviços pensados para distribuição massiva de aplicativos quanto plataformas cujo foco principal não seja esse, se aplicado em sua literalidade, gerando insegurança jurídica e risco de imposição de obrigações excessivas ou inadequadas.

Esclarecimento

Tendo por base a problemática mencionada, entendemos que a ANPD deva esclarecer, de forma objetiva, o conceito detalhando os elementos e as características de lojas de aplicações de internet como um agente que efetivamente exerce o papel de distribuidora de aplicativos, influencia a segurança do ecossistema e pode impor padrões aos desenvolvedores.

Entendemos que também é necessário que o futuro regulamento determine de forma expressa quais plataformas não se enquadram no conceito legal. Nesse sentido, é fundamental diferenciar sistemas operacionais, navegadores, plataformas multimídia, ambientes corporativos fechados e outros serviços cujo foco não seja o de distribuir aplicativos das aplicações que, de fato, se caracterizam como “lojas”, o que pode se dar por meio do estabelecimento de critérios técnicos e funcionais, como ausência de



curadoria, inexistência de controle sobre o conteúdo de terceiros ou falta de mecanismos formais de publicação.

Justificativa

O conceito de “lojas de aplicações” do ECA Digital traz em seu bojo dois elementos de enquadramento: o ato de distribuir e o ato de facilitar o download de aplicações. No entanto, é possível considerar que o ato de distribuir, para alguns serviços, significa hospedar diretamente o aplicativo e permitir seu download; enquanto que, para outros, poderia-se dizer que a sua mera atuação como intermediário que disponibiliza um catálogo organizado de links ou um ambiente que apenas encaminha o usuário para outra fonte de instalação, por exemplo, já o incluiria nessa definição.

Com isso, verificamos que a ausência de critérios objetivos traz insegurança jurídica a medida em que permite, em tese, que tanto uma loja tradicional de aplicações quanto um serviço que agrega conteúdos de terceiros sejam tratados como equivalentes para a incidência das obrigações da lei, ainda que exerçam atividades com características e representem riscos completamente distintos. Desse modo, é necessário que haja uma delimitação clara para que empresas e desenvolvedores consigam saber, efetivamente, se estão ou não sujeitos às obrigações criadas pela lei, afastando, assim, incertezas que poderiam trazer prejuízos à inovação ou levar a interpretações excessivamente amplas por parte de órgãos públicos ou de concorrentes.

Além disso, a falta de clareza no conceito pode conduzir a uma aplicação desproporcional da norma, uma vez que o ECA Digital, em seu artigo 12, atribui às lojas diversas obrigações relacionadas à aferição de idade, mecanismos de supervisão parental e à privacidade que podem ser indevidamente estendidas a serviços que não possuem esse papel nem a capacidade técnica para cumpri-las, o que acabaria por criar barreiras para o desenvolvimento de novos modelos de negócios.

Importante ressaltar ainda outro aspecto de fundamental importância a ser obtido com o esclarecimento da norma, que é o referente à eficácia regulatória. Isto porque na hipótese de se considerar todas as aplicações como se loja fossem, a lei acabará por perder o foco de proteção a que ela se destina, deixando de atingir os agentes que realmente concentram os riscos inerentes a uma loja de aplicativos e à sua organização, controle e influência na distribuição de aplicativos a um grande número de usuários. Dessa forma, a falta de clareza e certeza quanto ao comando normativo acabará por dificultar a fiscalização e poderá gerar questionamentos quanto ao seu destinatário.

Nesse sentido, entendemos que a ANPD, ao esclarecer este conceito e definir limites claros para sua incidência, poderá adequar as obrigações aos seus reais destinatários,

garantindo proporcionalidade e incentivando a inovação tecnológica, o que se mostra essencial para que a aplicação da lei cumpra seu propósito que é o de proteger usuários menores de idade e garantir segurança no ecossistema digital sem, com isso, inviabilizar o desenvolvimento de aplicações que não foram concebidas nem funcionam como lojas de aplicativos.

V. MECANISMO DE SUPERVISÃO PARENTAL

Dispositivo: Art. 2º, inciso VIII

Problemática

O ECA Digital, em seu artigo 2º, inciso VIII conceitua os mecanismos de supervisão parental como sendo o “conjunto de configurações, de ferramentas e de salvaguardas tecnológicas (...) que possibilitem aos pais ou responsáveis legais supervisionar, limitar e gerenciar o uso do serviço, o conteúdo acessado e o tratamento de dados pessoais realizado”. No entanto, embora o texto legal busque contemplar a diversidade de soluções possíveis, a definição é excessivamente genérica e não faz distinção entre tipos de serviços, contextos de uso e níveis de risco e, por tal razão tem o potencial de gerar interpretações divergentes entre agentes do mercado, com risco de adoção de controles meramente pouco eficazes ou desproporcionais.

A diversidade de plataformas, arquiteturas tecnológicas e modelos de interação utilizados por crianças e adolescentes torna inviável o estabelecimento de um conjunto uniforme de mecanismos de supervisão parental para todos os serviços acessíveis a menores de idade. Aplicativos educativos, jogos online, plataformas de vídeo, redes sociais, televisões conectadas, assistentes virtuais e sistemas operacionais apresentam finalidades, fluxos de uso e superfícies de risco distintos, de modo que pode-se afirmar que um mecanismo adequado em determinado contexto pode ser tecnicamente inviável, economicamente desproporcional ou excessivamente intrusivo em outro. Adicionalmente, a determinação de mecanismos e controles inadequados ao tipo de aplicação em que ele será disponibilizado pode acabar trazendo problemas com a observância aos princípios de proteção de dados e o respeito à autonomia progressiva da criança e do adolescente.

Esclarecimento

Para assegurar a correta interpretação do conceito de mecanismos de supervisão parental e orientar sua implementação de modo proporcional ao risco envolvido, respeitando a autonomia progressiva do menor, é essencial que a ANPD apresente diretrizes que esclareça a importância da consideração do contexto específico, explicitando que a adoção desses mecanismos deve seguir uma abordagem baseada em risco, na qual as



exigências variam conforme a natureza do serviço, o tipo de interação oferecida, o potencial de exposição a conteúdo gerado por terceiros e a sensibilidade das funcionalidades envolvidas. Tais esclarecimentos permitiriam adequar o nível de proteção esperado sem impor soluções uniformes a serviços e aplicações que apresentem perfis de risco - e arquiteturas - muito distintos. Entendemos que diretrizes claras podem contribuir para uniformizar expectativas e prevenir abordagens inadequadas que possam comprometer direitos fundamentais.

É essencial, por fim, que tais esclarecimentos reforcem que o objetivo da norma não é padronizar ferramentas, mas assegurar que cada serviço implemente soluções adequadas ao seu contexto, ao seu modelo de risco e ao impacto potencial sobre crianças e adolescentes que possuem acesso às suas funcionalidades.

Justificativa

Os esclarecimentos pela ANPD em torno dos mecanismos de supervisão parental que deverão ser implementados e a flexibilidade na sua escolha por cada produto ou serviço de tecnologia da informação são fundamentais para assegurar que a proteção prevista no ECA Digital seja efetiva, tecnicamente consistente e compatível com direitos fundamentais, uma vez que sem tais parâmetros interpretativos, a amplitude do conceito legal pode levar à adoção tanto de mecanismos insuficientes quanto de soluções intrusivas que possam comprometer a privacidade, a dignidade e o desenvolvimento da autonomia da criança e do adolescente.

Desse modo, é necessário que a ANPD estabeleça diretrizes claras que irão favorecer a segurança jurídica, reduzir assimetrias entre fornecedores de atividades e portes diferentes e permitir a calibragem das exigências e obrigações conforme o risco real de cada serviço. Além disso, ao estabelecer princípios e critérios proporcionais, a ANPD irá contribuir para um ambiente regulatório que incentiva inovação responsável e evita a imposição de obrigações desnecessárias em serviços de menor impacto.

Por fim, entendemos que é essencial que a regulamentação a ser editada pela Agência não promova a definição taxativa dos mecanismos de supervisão parental em virtude da diversidade tecnológica e da constante evolução das formas de interação digital envolvidas, pois uma relação fechadas e rígida de ferramentas podem rapidamente se tornar obsoletas, além de impor soluções incompatíveis com determinados serviços ou, ainda, comprometer a adoção de novas tecnologias mais eficazes e menos invasivas. Desse modo, uma abordagem flexível, fundamentada em princípios e análise de risco é a que representa uma melhor garantia de proteção efetiva, proporcionalidade, viabilidade técnica e respeito aos direitos das crianças e adolescentes no ecossistema digital atual.

VI. MELHOR INTERESSE DA CRIANÇA E DO ADOLESCENTE

Dispositivo: Art. 5º, § 2º

Problemática

O ECA Digital estabelece o melhor interesse como parâmetro central (arts. 3º e 5º), definindo-o no § 2º do art. 5º como a proteção da privacidade, segurança, saúde física e mental, acesso à informação, liberdade de participação, acesso significativo às tecnologias digitais e bem-estar.

A problemática envolve três pontos. Primeiro, embora o § 2º liste elementos que compõem o melhor interesse, a lei não indica como ponderá-los quando entram em tensão. Medidas como verificação de idade (art. 9º), restrições de acesso a conteúdos (art. 8º, III) ou configurações protetivas por padrão (art. 7º) promovem certos direitos mas podem limitar outros, exigindo orientações para um balanceamento estruturado.

Segundo, há risco de interpretação abstrata e apriorística do melhor interesse. Nesse sentido, vale lembrar que o Comentário Geral da ONU nº 14 afirma que o conceito é flexível, adaptável e deve considerar a situação concreta da criança ou do grupo afetado. Avaliações rígidas e descontextualizadas contrariam essa diretriz.

Terceiro, apesar de o art. 4º reconhecer a condição peculiar de pessoa em desenvolvimento e a autonomia progressiva, esses elementos não são integrados explicitamente à definição do § 2º. Sem essa articulação, corre-se o risco de aplicar o mesmo padrão a crianças e adolescentes em estágios de desenvolvimento muito distintos.

Esclarecimento

É preciso reconhecer que o melhor interesse exige avaliação concreta, contextual e multidimensional, considerando a interação entre os elementos do § 2º e reconhecendo que não há hierarquia fixa entre eles.

A Agência pode oferecer metodologia orientativa para avaliação fundamentada (com espaço para adaptação a diferentes contextos), que considere, por exemplo: (i) o serviço ou produto ofertado; (iii) riscos concretos; (iv) salvaguardas implementadas; (v) a condição peculiar de pessoa em desenvolvimento e autonomia progressiva (art. 4º); (vi) balanceamento de direitos.

Ainda, é necessário que o melhor interesse não corresponda ao emprego tão somente de soluções restritivas: acesso à informação, participação e acesso significativo às

tecnologias são elementos positivos do melhor interesse, não exceções. Medidas excessivamente restritivas podem violá-lo, mesmo quando justificadas por interesse legítimos de proteger a segurança ou privacidade de crianças e adolescentes.

Justificativa

O esclarecimento é indispensável para dar concretude ao princípio, garantir segurança jurídica e evitar sua utilização como cláusula aberta sem conteúdo operacional. O melhor interesse permeia diversos dispositivos do ECA Digital (arts. 3º, 5º, 7º, 17 § 2º, 19 § 2º) e, sem critérios claros, há risco de que fornecedores deixem de implementar funcionalidades benéficas ou adotem medidas inadequadas por falta de orientação.

A interpretação unidimensional focada apenas em proteção pode prejudicar outros direitos fundamentais. Os Comentários Gerais da ONU nº 14² e nº 25³ reforçam que o melhor interesse é dinâmico, interage com vários direitos e exige avaliação equilibrada e baseada em contexto. Abordagens rígidas podem limitar oportunidades, participação e desenvolvimento integral.

A flexibilidade do princípio decorre da própria doutrina internacional e visa permitir respostas proporcionais às necessidades de cada faixa etária e a evolução do conhecimento científico. Integrar a condição peculiar de pessoa em desenvolvimento evita tanto excesso quanto insuficiência de proteção, impedindo que crianças e adolescentes sejam tratados como grupos homogêneos.

VII. CONTEÚDO PORNOGRÁFICO E MATERIAL PORNOGRÁFICO

Dispositivo: Art. 9º

Problemática

O Art. 9º, § 2º da Lei nº 15.211/2025 é um dispositivo fundamental no arcabouço protetivo que define o que se considera "impróprio ou inadequado" para crianças e adolescentes, listando explicitamente o "material pornográfico" e "quaisquer outros vedados pela legislação vigente". Este dispositivo é crucial, pois exige que os fornecedores de tecnologia adotem medidas eficazes para impedir o acesso a tais conteúdos, exigindo mecanismos confiáveis de verificação de idade a cada acesso e vedando a autodeclaração.

²<https://www.refworld.org/legal/general/crc/2013/en/95780>

³<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

No entanto, o ECA Digital ou ordenamento jurídico brasileiro não possui uma definição legal unificada e clara do que constitui "conteúdo pornográfico" ou "material pornográfico" para fins civis e regulatórios. A ausência de um conceito técnico-jurídico claro o abre espaço para uma leitura extensiva segundo a qual qualquer obra audiovisual que contenha representações de sexo e nudez – tratadas como eixo temático específico no sistema de Classificação Indicativa (CI) – possa ser enquadrada como “conteúdo pornográfico” para fins do art. 9º. Essa ausência conceitual tem potencial de equiparação indevida das obras classificadas como “não recomendadas para menores de 18 anos” em razão de sexo/nudez (dramas, séries, filmes de arte, documentários, biografias etc.) a serviços especializados em pornografia.

Esclarecimento

Para evitar a conflação e respeitar a natureza distinta das obras, sugerimos que a ANPD adote uma definição de "material pornográfico" que se concentre na finalidade produtiva principal do conteúdo, dissociando-o de obras audiovisuais onde o sexo ou a nudez são utilizados em contextos artísticos, narrativos ou ficcionais.

Justificativa

A adoção de uma definição restritiva de “material pornográfico”, centrada na finalidade principal de excitação sexual, é necessária para preservar a coerência entre o ECA Digital e a Política de Classificação Indicativa.

A experiência comparada mostra que esse risco de conflação é evitado por meio de conceitos normativos claros. A Ofcom, ao implementar a Parte 5 do Online Safety Act⁴ (Reino Unido), faz as seguintes distinções:

- o “conteúdo pornográfico regulado”, definido como conteúdo “produzido única ou principalmente com o propósito de excitação sexual”, sujeito a exigências reforçadas de garantia de idade altamente eficaz; e
- outras obras audiovisuais com forte conteúdo sexual ou nudez, que não são produzidas com essa finalidade principal e, por isso, são reguladas por outros regimes (como serviços on-demand) e não enquadradas automaticamente como pornografia.

⁴

<https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/guidance-on-highly-effective-age-assurance-and-other-part-5-duties.pdf?v=388810>

No contexto brasileiro, a Portaria 1048/2025 já regulamenta a Classificação Indicativa para produtos e serviços de tecnologia da informação, utilizando eixos temáticos (como “sexo e nudez”) para modular a faixa etária e a não recomendação, em chave pedagógica e informativa. Se a regulamentação da ANPD não diferenciar claramente o “material pornográfico” das obras classificadas pela CI, o ECA Digital acabará por criar um sistema paralelo, que desconsidera essa metodologia (eixos, agravantes, atenuantes) e converte um regime de informação e modulação etária em um regime único de bloqueio.

A diferenciação proposta permite calibrar adequadamente os instrumentos de proteção. O regime de impedimento categórico e verificação de idade a cada acesso, previsto no art. 9º, caput e § 1º, deve aplicar-se ao conteúdo genuinamente vedado, isto é, material produzido exclusiva ou principalmente com propósito de excitação sexual. Já para obras lícitas classificadas como “não recomendadas para menores de 18 anos”, o regime mais adequado é o de supervisão parental configurável e restrições graduadas por faixa etária, em consonância com o poder familiar de escolha, com os arts. 12 e 18 do ECA Digital e com a Portaria 1.048/2025.

Ao adotar um critério baseado na finalidade produtiva, a ANPD alinha o ECA Digital às boas práticas internacionais de segurança online, oferece um parâmetro objetivo e fiscalizável para diferenciar conteúdo vedado de conteúdo apenas inadequado, e evita que a noção de “pornografia” seja aplicada de forma excessivamente ampla ou subjetiva a obras audiovisuais lícitas.

VIII. CONTEÚDO IMPRÓPRIOS OU INADEQUADOS PARA CRIANÇAS E ADOLESCENTES

Dispositivo: Art. 9º, §2º

Problemática

Para apresentar a problemática do art. 9º, § 2º do ECA Digital é preciso fazer uma leitura combinada com os demais dispositivos do artigo. O art. 9º do ECA Digital estabelece um regime mais rígido para certos conteúdos: (i) o caput impõe a adoção de “medidas eficazes para impedir o acesso” de crianças e adolescentes a conteúdos, produtos ou serviços “impróprios, inadequados ou proibidos” para menores de 18 anos; (ii) o § 1º exige “mecanismos confiáveis de verificação de idade a cada acesso”, vedando expressamente a autodeclaração; (iii) o § 2º define que são “impróprios ou inadequados” os conteúdos com material pornográfico ou “quaisquer outros vedados pela legislação vigente”; (iii) o § 3º reforça, de forma específica, que provedores que disponibilizam conteúdo pornográfico devem impedir a criação de contas ou perfis por crianças e adolescentes.

Em resumo, lido em conjunto, o art. 9º orienta que determinados conteúdos são legalmente vedados a menores (tais como material pornográfico e outros expressamente proibidos por normas vigentes, tais como álcool)); e para esses conteúdos, exige-se um regime robusto de impedimento de acesso, com verificação de idade confiável e recorrente.

No entanto, a problemática do dispositivo surge ao utilizar os termos “impróprio” e “inadequado” que historicamente estão usados na Política de Classificação Indicativa, para designar conteúdos “não recomendados” a determinadas faixas etárias, possuindo natureza pedagógica e informativa, e não de proibitiva. Assim, no âmbito da Classificação Indicativa, “impróprio” ou “inadequado” para determinada faixa etária não significa vedação absoluta, mas apenas que aquele conteúdo não possui recomendação para determinada faixa etária, podendo exigir mediação e escolha responsável por parte das famílias e responsáveis.

Embora o § 2º faça um recorte objetivo (pornografia + demais conteúdos vedados pela legislação vigente), a combinação entre: (i) a redação ampla do caput (“impróprio, inadequado ou proibido para menores de 18 anos”); (ii) o histórico uso de “impróprio/inadequado” na Classificação Indicativa; e (iii) a exigência de verificação robusta “a cada acesso” (art. 9º, § 1º), pode levar, na prática, a interpretações segundo as quais obras classificadas como “não recomendadas para menores de 18 anos” pela Classificação Indicativa seriam tratadas como se fossem “impróprias ou inadequadas” em sentido proibitivo, sujeitas a: bloqueio absoluto para crianças e adolescentes; mecanismos intrusivos de verificação de idade a cada acesso; tratamento equiparado a material pornográfico ou a conteúdos ilícitos.

Ao empregar os mesmos termos (“impróprio/inadequado”) para se referir a conteúdos que devem ser impedidos nos termos do ECA Digital, a lei gerou um risco de fusão conceitual entre duas esferas distintas:

1. a esfera informativa, própria da Classificação Indicativa, em que conteúdos são rotulados como “não recomendados” para certas idades, sem proibição de exibição; e
2. a esfera proibitória, própria do ECA e do ECA Digital, em que determinados conteúdos são legalmente vedados (por exemplo, produtos alcançados pelo art. 81 do ECA ou materiais de natureza delituosa).

Essa sobreposição terminológica abre espaço para interpretações perigosas nas quais toda obra classificada pelo Ministério da Justiça como “não recomendada para menores de 18 anos” poderia ser tratada como “imprópria ou inadequada” em sentido proibitivo, sujeita a bloqueio ou a mecanismos de verificação de idade tão rígidos quanto aqueles



reservados a conteúdos ilícitos ou expressamente vedados, afastando, nesse caso, o dever compartilhado com a família constitucionalmente previsto. .

Esse cenário de iminente fusão conceitual pode levar a um deslocamento da natureza da Classificação Indicativa: de instrumento de informação e co-participação entre (Estado - família - sociedade) para um mecanismo indireto de censura ou de proibição de acesso, em tensão com a liberdade de expressão e com a vedação à censura prévia consagradas na Constituição Federal. Por isso, a regulamentação da ANPD precisa afastar essa confusão conceitual, preservando a distinção entre:

- conteúdos proibidos (ilícitos ou vedados pela legislação); e
- conteúdos não recomendados (que devem ser informados e sujeitos a mecanismos de supervisão e controle parental, mas não automaticamente bloqueados).

Esclarecimento

Sugere-se que a regulamentação da ANPD diferencie o tratamento entre os conteúdos que são legalmente vedados (proibidos) e aqueles que são apenas não recomendados (inadequados/impróprios) segundo a Política de Classificação Indicativa, harmonizando o Art. 9º do ECA Digital com a Política de Classificação Indicativa, estabelecendo:

1. Delimitação do alcance de “impróprio ou inadequado” para fins do art. 9º do ECA digital: A regulamentação deve esclarecer que, para os fins do art. 9º, § 2º, o conceito de “produtos, serviços ou conteúdos impróprios ou inadequados” se restringe a: conteúdos com material pornográfico, nos termos do § 2º; e “quaisquer outros vedados pela legislação vigente”, isto é, conteúdos cuja oferta a menores de idade seja expressamente proibida por normas legais (por exemplo, hipóteses equiparáveis às do art. 81 do ECA ou outros tipos penais e vedações específicas).
2. Diferenciação dos conteúdos apenas “não recomendados” pela Classificação Indicativa: A regulamentação deve deixar claro que conteúdos apenas “não recomendados” para determinadas faixas etárias, conforme a Política de Classificação Indicativa (ex.: “não recomendado para menores de 16 anos” ou “não recomendado para menores de 18 anos), não são automaticamente enquadrados como “impróprios ou inadequados” em sentido proibitivo, nem “vedados pela legislação vigente”, para fins de aplicação integral do art. 9º (bloqueio absoluto + verificação de idade forte a cada acesso).

Nesses casos, as obrigações dos serviços devem ser proporcionais e consistir



principalmente em: informação clara e destaque da faixa etária e dos descritores de conteúdo; oferta e efetividade de ferramentas de controle parental; desenho de produto que mitigue riscos específicos para crianças e adolescentes, sem equiparar tais conteúdos a material ilícito.

Justificativa

O art. 9º, §§ 1º a 3º do ECA Digital compõe um eixo normativo que responde a uma preocupação legítima da sociedade com conteúdos de alta nocividade (notadamente, pornografia e produtos/serviços explicitamente vedados a menores de idade); impondo um regime robusto de impedimento de acesso e verificação de idade, adequado a esse contexto de alta gravidade, ao mesmo tempo, utiliza terminologia (“impróprio”, “inadequado”) que já possui significado consolidado na política de Classificação Indicativa, onde designa conteúdos não recomendados para determinadas faixas etárias, mas não proibidos.

A atuação interpretativa da ANPD, é fundamental para afastar o cenário insegurança jurídica existente, esclarecendo eventuais interpretações divergentes sobre quais conteúdos, produtos ou serviços exigem mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo - nos termos do capítulo III do ECA Digital - daqueles mecanismos para proporcionar experiências adequadas à idade, nos termos deste Capítulo, respeitadas a autonomia progressiva e a diversidade de contextos socioeconômicos brasileiros, e incluindo mecanismos de informação e supervisão parental. Havendo a possibilidade de extensão do regime de verificação de idade a cada acesso (art. 9º, § 1º) a toda e qualquer obra rotulada como não recomendado para menores de 18 anos, tratando conteúdo lícito e culturalmente legítimo (filmes, séries, jogos) como se fossem equivalentes a material pornográfico ou ilícito; além de possível deslocamento do papel informativo e orientativo da Política de Classificação Indicativa para um papel de filtro de proibição, rompendo a lógica construída desde a Constituição de 1988, que substituiu a censura por um modelo de corresponsabilidade.

Diferenciar, de forma explícita, os conteúdos legalmente vedados (núcleo do art. 9º, § 2º) daqueles não recomendados segundo a Classificação Indicativa, preserva a coerência sistêmica entre ECA, ECA Digital e Política de Classificação Indicativa do MJSP; confere segurança jurídica a serviços e desenvolvedores quanto ao desenho de mecanismos de verificação de idade e controle parental e assegura que um regime mais robusto de verificação de idade (art. 9º, § 1º) seja aplicado de forma proporcional ao risco, concentrado em pornografia e conteúdos efetivamente proibidos, sem expandir indevidamente a esfera da proibição para todo o universo de obras classificadas como “não recomendadas” para determinadas faixas etárias.

IX. PUBLICIDADE COMERCIAL

Dispositivo: Arts. 22 e 26

Problemática

Os arts. 22 e 26 do ECA Digital vedam o uso de técnicas de perfilamento e a criação de perfis comportamentais para o direcionamento de publicidade comercial a crianças e adolescentes. Embora o texto seja específico, há receio de interpretações extensivas que concluam pela existência de uma proibição total de publicidade direcionada a esse público, interpretação que não encontra respaldo no ordenamento jurídico brasileiro.

O Código de Defesa do Consumidor (CDC) não proíbe publicidade direcionada, mas sim a publicidade abusiva, incluindo aquela que “se aproveite da deficiência de julgamento e experiência da criança”. Assim, a vedação legal recai apenas sobre publicidade que explora vulnerabilidades de crianças, não sobre toda e qualquer forma de publicidade dirigida a esse público.

O CONAR, referência em autorregulação publicitária, também não adota proibição absoluta. Seu Código⁵ prevê uma seção específica sobre publicidade para crianças e adolescentes que estabelece cuidados especiais e diretrizes, tais como: respeito à ingenuidade e inexperiência, proibição de apelos imperativos de consumo, observância de valores sociais positivos, vedação a mensagens que estimulem comportamentos socialmente condenáveis, e atenção às características psicológicas do público. Essas normas orientam como a publicidade deve ocorrer, e não que ela seja proibida.

Por fim, salienta-se que a vedação, prevista no artigo 22, ao uso de técnicas como análise emocional, realidade aumentada, realidade estendida e realidade virtual aplica-se exclusivamente quando utilizadas para fins de direcionamento publicitário, não impedindo seu uso para finalidades legítimas, como educação, segurança, acessibilidade e bem-estar.

Esclarecimento

A ANPD deve esclarecer que:

- A vedação dos arts. 22 e 26 recai exclusivamente sobre o uso de técnicas de perfilamento e a criação de perfis comportamentais para fins de direcionamento de publicidade comercial.

⁵ http://www.conar.org.br/pdf/codigo-conar-2021_6pv.pdf



- Publicidade que não utiliza perfilamento, inclusive aquela baseada apenas no conteúdo acessado (contextual) ou não direcionada (genérica), não é abrangida pela vedação, desde que observadas as regras do CDC.
- As tecnologias mencionadas no art. 22 são proibidas apenas quando empregadas para direcionamento publicitário, não impedindo seu uso para outras finalidades legítimas.
- A interpretação adequada deve harmonizar o ECA Digital com o CDC e o CONAR, prevenindo práticas manipulativas sem inviabilizar modelos de negócio legítimos.
- A publicidade para fins de políticas públicas, ainda que direcionada ao público infante juvenil, deverá ser permitida.

Justificativa

O esclarecimento é essencial para conferir segurança jurídica e evitar interpretações desproporcionais, especialmente porque o legislador fez uma escolha explícita: vedar apenas a publicidade baseada em perfilamento, não qualquer forma de publicidade direcionada a crianças e adolescentes.

Reitera-se que o ordenamento jurídico brasileiro não proíbe a publicidade dirigida a crianças e adolescentes, mas apenas aquela considerada abusiva. Interpretar o ECA Digital como uma vedação total à publicidade não apenas contraria sua própria redação, como também carece de qualquer fundamento legal. Além disso, é necessário considerar os efeitos concretos de uma interpretação tão ampla: a proibição geral de publicidade poderia restringir o acesso de crianças e adolescentes a serviços digitais gratuitos, em desacordo com o art. 5º, § 2º do ECA Digital.

É necessário ainda explicitar a diferença entre as modalidades de publicidade:

- Publicidade comportamental (vedada): baseada em perfilamento para direcionamento individualizado.
- Publicidade contextual (permitida): relacionada ao conteúdo acessado, sem emprego de perfilamento.
- Publicidade genérica (permitida): não direcionada a partir de dados ou comportamento.

A distinção é fundamental para garantir a proteção contra práticas manipulativas, sem inviabilizar atividades econômicas lícitas nem reduzir o acesso a conteúdos e serviços por crianças e adolescentes.

X. CONTEÚDOS VIOLADORES DE DIREITOS DE CRIANÇAS E ADOLESCENTES

Dispositivo: Art. 29, § 1º, com remissão ao art. 6º

Problemática

O ECA Digital, ao definir “conteúdos violadores de direitos de crianças e adolescentes” no art. 29, §1º, remete expressamente ao rol do art. 6º, estabelecendo um parâmetro objetivo para orientar plataformas e autoridades. Esse rol abrange conteúdos como exploração e abuso sexual, violência física ou psicológica, cyberbullying, indução à autolesão ou suicídio, promoção de jogos de azar ou produtos proibidos para crianças e adolescentes, práticas predatórias e material pornográfico — elementos que, por sua natureza, configuram violação direta de direitos fundamentais.

Ocorre que o §1º também menciona a classificação indicativa, o que pode gerar uma interpretação equivocada: a de que o enquadramento como “conteúdo violador” dependeria de um sistema classificatório que não tem caráter obrigatório, sendo sim indicativo..

Esclarecimento

Embora citado pelo §1º do art. 29, o sistema de classificação indicativa possui natureza informativa e orientadora, e não obrigatória ou censória, conforme previsto no marco jurídico brasileiro. Seu objetivo é auxiliar responsáveis e provedores na avaliação de adequação etária, e não definir o que é proibido por lei.

Assim, a identificação dos conteúdos do art. 6º como violadores de direitos decorre diretamente da lei, independentemente de eventual classificação.

Justificativa

Vincular a caracterização de “conteúdo violador de direitos” a um mecanismo não obrigatório, como a classificação indicativa, pode gerar insegurança interpretativa e distorções na aplicação da norma. Diante dessa redação já aprovada, caberá à ANPD esclarecer, na regulamentação, a necessária dissociação entre os institutos: a classificação indicativa não condiciona, relativiza ou integra o critério de definição dos conteúdos do art. 6º como violadores de direitos. Esse esclarecimento é essencial para preservar a coerência normativa, evitar interpretações que ampliem de forma indevida o alcance do sistema de classificação e assegurar que a lei não seja convertida, na prática, em um regime de classificação obrigatória.

XI. CONDIÇÃO PECULIAR DE PESSOA EM DESENVOLVIMENTO

Dispositivo: Art. 4º, Inciso III

Problemática

O art. 4º, III, do ECA Digital adota como fundamento “a condição peculiar de pessoa em desenvolvimento biopsicossocial” e, no art. 4º, V, prevê “o respeito à autonomia e ao desenvolvimento progressivo do indivíduo”. No entanto, embora o ECA diferencie crianças (até 12 anos incompletos) de adolescentes (12 a 18 anos) e determine, em seu art. 6º, que as normas devem considerar essa condição peculiar, o ECA Digital aplica suas obrigações a “crianças e adolescentes” de forma indistinta.

A ausência dessa diferenciação ao longo da lei gera falta de orientação sobre como operacionalizar tais princípios no ambiente digital.

Essa indiferenciação resulta em dois riscos: (i) adoção de medidas excessivamente restritivas a adolescentes, limitando indevidamente autonomia, liberdade de expressão e acesso à informação; e (ii) adoção de medidas insuficientemente protetivas para crianças menores, por não reconhecer vulnerabilidades específicas.

Um exemplo ilustrativo é o art. 2º, VIII, que define “mecanismo de supervisão parental” de forma ampla, combinado com os arts. 16, 17 e 18, que impõem obrigações sobre tais ferramentas sem diferenciar sua aplicação conforme idade, maturidade ou grau de autonomia. Esse tipo de tratamento uniforme demonstra como a ausência de reconhecimento da condição peculiar de desenvolvimento pode resultar em exigências inadequadas tanto para crianças quanto para adolescentes.

Esclarecimento

A ANPD deve esclarecer que a condição peculiar de pessoa em desenvolvimento exige tratamento diferenciado entre crianças e adolescentes, com abordagens que considerem idade, estágio de maturidade, evolução da autonomia e capacidades cognitivas. Isso inclui reconhecer expressamente que, nos termos do art. 2º do ECA, crianças e adolescentes constituem grupos distintos, e que essa distinção deve ser refletida na forma de implementação das obrigações previstas no ECA Digital.

Enquanto para crianças são adequadas medidas que permitam maior participação dos pais, para adolescentes, deve-se priorizar mecanismos que respeitem e promovam autonomia progressiva. Entende-se que a autonomia progressiva deve ser tratada como elemento estruturante e interpretativo do ECA Digital, implicando, por exemplo:



- (i) em transparência e comunicação adaptadas a diferentes idades;
- (ii) no exercício diferenciado de direitos;
- (iii) na possibilidade de adolescentes consentire ;
- (iv) na proporcionalidade na adoção de restrições e controles.

Nesse contexto, a ANPD pode considerar como exemplo útil o *Age Appropriate Design Code* (Reino Unido), que traduz princípios de desenvolvimento em parâmetros práticos. O Código organiza obrigações segundo faixas etárias e estágios de maturidade (0–5; 6–9; 10–12; 13–15; 16–17)⁶, orientando transparência, linguagem, limites de uso, proteção contra nudges, padrões de privacidade e interação com ferramentas parentais de forma graduada. Essa experiência demonstra como as normas podem reconhecer capacidades em evolução e ajustar salvaguardas conforme o desenvolvimento.

O esclarecimento deve reconhecer, ainda, que o princípio da condição peculiar de pessoa em desenvolvimento impõe ao ECA Digital não apenas a criação de restrições, mas também o gozo de direitos fundamentais no ambiente digital, incluindo acesso à informação, liberdade de expressão, participação social, educação e lazer.

Justificativa

Considerar as diferenças não apenas entre crianças e adolescentes, mas também entre as diferentes faixas etárias, é essencial para assegurar que o ECA Digital seja aplicado de forma coerente com os princípios que regem o direito da criança e do adolescente, como o princípio da autonomia progressiva e o do melhor interesse da criança e do adolescente. A ausência dessa diferenciação pode gerar tanto restrições excessivas para adolescentes quanto proteção insuficiente para crianças menores.

Instrumentos internacionais, especialmente a Convenção sobre os Direitos da Criança e os Comentários Gerais da ONU nº 14 e nº 25, reforçam a centralidade das capacidades em evolução e Experiências como o *Age Appropriate Design Code* (Reino Unido), os *Fundamentals* (Irlanda) e o *Children's Code* (Holanda) demonstram que calibrar obrigações conforme o estágio de desenvolvimento é uma prática consolidada e essencial para equilibrar proteção, participação e autonomia.

XII. VERIFICAÇÃO DE IDADE VS. AFERIÇÃO DE IDADE

Dispositivos: Arts. 9º e 15

Problemática

⁶<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>

O ECA Digital utiliza terminologias distintas em diferentes dispositivos: art. 9º, § 1º, refere-se a "mecanismos confiáveis de verificação de idade"; Capítulo IV intitula-se "Dos Mecanismos de Aferição de Idade"; art. 12, I, menciona "aferir a idade ou a faixa etária"; art. 13 refere-se a "verificação de idade"; e art. 24, § 3º, menciona "métodos complementares de verificação". A ausência de clareza sobre a relação conceitual entre esses termos gera incerteza sobre exigências, métodos admissíveis e alcance de obrigações.

Há um certo consenso internacional de que "age assurance" funciona como termo guarda-chuva que engloba diferentes mecanismos, dentre eles a verificação. Contudo, apesar desse consenso conceitual, a problemática central reside em: o ECA Digital efetivamente adotou essa diferenciação conceitual ao empregar "verificação" em alguns dispositivos e "aferição" em outros, ou utilizou os termos como sinônimos intercambiáveis? E, mais importante: quais são os impactos práticos de interpretar a lei em um sentido ou outro? A questão não é meramente semântica, tem consequências jurídicas e práticas.

A problemática se complica porque, embora haja certo consenso técnico sobre "assurance" como guarda-chuva, não há consenso sobre quais mecanismos específicos cada categoria abrange. Por exemplo: autodeclaração é forma de aferição ou não? Algumas entidades internacionais admitem a autodeclaração como um mecanismo de aferição ou ao menos como um método de triagem inicial.

Portanto, a questão fundamental que a ANPD deve enfrentar não é apenas "qual a definição técnica correta", mas sim: considerando como o ECA Digital efetivamente empregou esses termos em diferentes dispositivos, qual interpretação gera consequências práticas mais coerentes com o sistema da lei, com a proporcionalidade e com o melhor interesse de crianças e adolescentes?

Esclarecimento

A ANPD deve esclarecer como os termos "verificação de idade" e "aferição de idade" devem ser interpretados no contexto do ECA Digital, considerando que:

1. Os termos aparecem em dispositivos diferentes da lei, e a interpretação adotada poderá gerar consequências práticas distintas sobre obrigações e métodos permitidos.
2. A escolha entre tratá-los como conceitos tecnicamente distintos ou como sinônimos terá impactos práticos na implementação das obrigações de aferição



de idade.

3. Apesar de haver entendimento técnico de que “aferição” é um termo guarda-chuva que abrange “verificação”, não existe consenso internacional sobre quais mecanismos estão ou não abrangidos pelo termo aferição.
4. Não existe método perfeito de age assurance: todos apresentam trade-offs em termos de precisão, privacidade, inclusão e viabilidade técnica e econômica.
5. A experiência internacional recomenda abordagem baseada em risco, com maior rigor para serviços de alto risco e mais flexibilidade para contextos gerais, não havendo método único obrigatório.
6. Métodos de age assurance têm impactos significativos sobre outros direitos fundamentais, como privacidade, proteção contra vigilância, inclusão digital, liberdade de expressão e anonimato.
7. A implementação de mecanismos de age assurance nos termos exigidos pelo ECA Digital terá impactos não só em crianças e adolescentes, mas nos usuários de produtos ou serviços de tecnologia da informação de forma geral.
8. Todos os mecanismos são falíveis, o que reforça que a lei exige medidas proporcionais e tecnicamente seguras, e não infalibilidade absoluta.

Justificativa

O esclarecimento é necessário porque a indefinição terminológica no ECA Digital produz incertezas regulatórias que afetam diretamente a implementação prática das obrigações. A interpretação adotada pela ANPD influenciará:

- quais métodos são admitidos como válidos em diferentes contextos;
- o nível de rigor esperado de cada contexto;
- a compatibilidade entre proteção, privacidade, inclusão e proporcionalidade;
- a viabilidade da implementação das obrigações impostas, especialmente para agentes de menor porte.

A ausência dessa definição pode gerar interpretações desproporcionais, como a exigência de métodos uniformes, altamente intrusivos ou economicamente inviáveis, em desacordo com os arts. 5º, § 3º, e 34, § 2º, que determinam abordagens graduais e responsivas, ajustadas ao porte do agente e aos riscos envolvidos.



Por fim, definir a relação entre “aferição” e “verificação” é essencial para assegurar coerência normativa, alinhamento com práticas internacionais e previsibilidade regulatória. Somente com clareza conceitual será possível equilibrar proteção efetiva, viabilidade de implementação e respeito aos direitos fundamentais de crianças e adolescentes no ambiente digital.



OFÍCIO Nº ED-0030/2025



São Paulo, 12 de dezembro de 2025.

Autoridade Nacional de Proteção de Dados (ANPD)
Aos cuidados da Coordenação-Geral de Normatização

Assunto: Tomada de Subsídios - Conceitos previstos no ECA Digital - ANPD

Prezados,

1 A Federação Brasileira de Bancos (“FEBRABAN”) e Associação Brasileira das Empresas de Cartões de Crédito e Serviços (“ABECS”), associações civis sem fins lucrativos representativas do setor financeiro, vêm apresentar suas contribuições acerca da tomada de subsídios relacionada aos conceitos previstos na Lei 15211 de 17 de setembro de 2025 (“ECA Digital”).

2 Esperamos que nossas contribuições possam auxiliar qualitativamente no desenvolvimento das atividades da ANPD.

3 Permanecemos à disposição para quaisquer esclarecimentos ou contribuições que se façam necessários.

Respeitosamente,

Federação Brasileira de Bancos


D4Sign

Luís Vicente Magni De Chiara
Diretor-executivo de Assuntos Jurídicos


D4Sign

Roberta Gaspar Buso
Gerente Jurídica

Associação Brasileira das Empresas de Cartões de Crédito e Serviços


D4Sign

Marcelo Takeyama
Diretor Jurídico, Autorregulação e Compliance

Tomada de Subsídios conceitos previstos no ECA Digital - ANPD

Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Dentre os principais pontos que demandam esclarecimento, estão:

I. Aplicabilidade do ECA Digital (arts.1º e 2º):

Produto e serviço de tecnologia da informação direcionado a criança e adolescentes: é necessário que sejam publicados esclarecimentos adicionais sobre a aplicabilidade da norma, visto que esta foi constituída com foco nas plataformas digitais - onde há maior interação do público infanto-juvenil (como redes sociais e jogos eletrônicos). A norma traz um conceito de “produto ou serviço de tecnologia da informação” extremamente amplo, gerando dúvidas sobre a aplicação para outros segmentos do mercado.

Neste sentido, dentre os exemplos de produtos e serviços de tecnologia da informação contemplados pela norma estão as “aplicações de internet” – conceito definido pelo Marco Civil da Internet como “o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”.

Pela redação do ECA Digital, qualquer aplicativo, ainda que não seja construído para interação social por crianças e adolescentes, mas que simplesmente esteja disponível ao público, que tenham ou não funcionalidades que possam ser acessadas por elas, seria considerado no conceito, o que parece desviar da finalidade inicial da aplicação da lei.

A título de exemplo, considerando a natureza e a finalidade dos serviços prestados pelas instituições financeiras, a aplicação das normas do ECA Digital a esses serviços, tal como publicada, não estaria em linha com os objetivos da lei de proteção às crianças e adolescentes em ambiente digital. Isto porque, o setor financeiro não atua como provedor de conteúdo digital ou ambiente de entretenimento, mas sim como executor de operações reguladas, voltadas principalmente a pessoas com capacidade civil plena ou representadas, conforme a legislação vigente. O fato de os serviços serem oferecidos por aplicativos ou pela

internet não implica, necessariamente, acesso por menores de idade, e, quando há produtos específicos para esse público, a contratação é feita pelo responsável legal.

Nesse sentido, os seguintes parâmetros ou definições poderiam ser considerados para delimitação dos conceitos: (i) tipo de serviço (interação social, comunicação, compartilhamento, monetização, publicidade etc.); (ii) modelo de uso (se há conta individual, conta individual aberta pelos responsáveis ou vinculada aos responsáveis legais); (iii) público alvo do serviço – se o serviço se destina explicitamente ao público infantil ou adolescentes; (iv) grau de risco associado ao uso por menores: como, por exemplo, a possibilidade de assédio, exposição a conteúdos impróprios etc.

Acesso provável: os conceitos utilizados para caracterizar o “acesso provável” não trazem a completude necessária para garantir compreensão sobre aplicabilidade da lei. A definição de “acesso provável” fundada em critérios amplos e subjetivos, como: (i) “suficiente probabilidade de uso”; (ii) “atratividade”; (iii) “considerável facilidade ao acesso e utilização”; e (iv) “significativo grau de risco à privacidade, segurança ou desenvolvimento biopsicossocial” sem definição específica de tais termos, produz um nível considerável de incerteza jurídica.

Sobre esse ponto, é importante considerar que, apesar de os serviços financeiros serem oferecidos digitalmente por meio de aplicativos, estes são concebidos para um público amplo, majoritariamente adulto, com foco em segurança e eficiência, não podendo a adoção de uma interface moderna, intuitiva e acessível ou o fato de poder ser acessado pela internet, por si só, ser interpretada como um elemento de atratividade ou facilidade de acesso por menores de idade.

É fundamental, portanto, distinguir com precisão os serviços financeiros de uso geral, que podem eventualmente ser acessados por jovens, mas não são direcionados a eles, daqueles produtos efetivamente voltados ao público infantil ou adolescente. Inclusive, é válido destacar que os produtos e serviços oferecidos por instituições financeiras somente podem ser contratados por meio dos responsáveis legais destes menores, nos termos do Código Civil, de modo que não há apelo de consumo ou atrativo de marketing direcionado a eles. Além disso, ao se tratar deste segmento, não há interação de menores de idade com outros usuários, como acontece em redes sociais e plataformas de jogos online.

Além disso, a “atratividade” atrelada ao “acesso provável” deve ser analisada com cautela, posto que do modo em que se encontra, gamificações usadas em

OFÍCIO Nº ED-0030/2025

iniciativas de educação financeira, por exemplo, poderiam ser indevidamente classificadas como "atrativas" para crianças. Tal atratividade deve ser vinculada a uma estratégia deliberada de marketing e design para o público infantil, e não a elementos isolados que visam tornar a experiência financeira mais amigável e até mesmo mais segura para todos os públicos. Deste modo, eventual presunção de "acesso provável" deveria estar atrelada apenas aos produtos e serviços comercializados como "infantis" ou "juvenis".

Acesso possível: O termo "acesso possível", embora não definido explicitamente na lei em contraste com "acesso provável", permeia a interpretação da norma e gera incerteza. Observa-se uma confusão recorrente, inclusive em veículos de imprensa, consultorias e pareceres técnicos, entre o que é "acesso possível" (qualquer serviço pode, em tese, ser acessado por uma criança) e o que é "acesso provável" (quando o acesso se mostra previsível, frequente ou atraído por elementos do serviço). Essa confusão conceitual tem levado à interpretação equivocada de que qualquer serviço acessível via internet estaria automaticamente sujeito ao regime mais rígido da lei, o que desvirtua o critério de proporcionalidade previsto no próprio texto legal. No contexto do setor financeiro, isso significaria aplicar o regime mais estrito a todas as plataformas bancárias apenas por serem tecnicamente acessíveis, o que seria desproporcional.

Deste modo, a ANPD deve esclarecer que "Acesso possível" é um conceito amplo e irrestrito, reconhecendo que qualquer serviço conectado está potencialmente ao alcance de uma criança e "Acesso provável" demanda previsibilidade, indícios concretos e evidências objetivas de que crianças e adolescentes, na prática: (a) acessam com frequência; (b) procuram aquele tipo de serviço; (c) são atraídos por elementos temáticos, estéticos ou funcionais; (d) formam uma parte relevante da audiência; e (e) são alvo direto de estratégias de comunicação.

Considerações finais sobre aplicabilidade da norma:

Diante do cenário descrito acima, os conceitos de "produto ou serviço de tecnologia da informação direcionado" e "acesso provável" precisam ser melhor definidos pela ANPD, mediante critérios objetivos e específicos de modo a garantir a assertividade quanto à aplicabilidade da norma aos setores que de fato se pretende regular, sob pena de toda e qualquer plataforma, mesmo que não tenha foco na interação infantil, possa estar sujeita às obrigações e penalidades trazidas pela lei.

Neste sentido, cabe destacar que as instituições financeiras já seguem um conjunto robusto de normas para proteção de dados, canais de denúncia e transparência, sob a regulação do Banco Central e do Conselho Monetário Nacional. A inclusão do setor financeiro na nova legislação, sem uma delimitação clara, pode gerar sobreposição de obrigações, insegurança jurídica e conflitos regulatórios, além de dificultar o uso dos produtos e serviços por menores de idade.

II. Mecanismos de supervisão parental (art. 3º, Parágrafo Único e arts. 16 a 18)

A norma prevê que fornecedores de produtos ou serviços de tecnologia da informação devem disponibilizar configurações e ferramentas acessíveis que apoiem a supervisão parental pelos pais e/ou responsáveis legais, considerando a tecnologia disponível, a natureza e o propósito do produto ou serviço.

O texto é abrangente e não delimita as características mínimas desses mecanismos de supervisão parental, não definindo até que ponto essa supervisão pode ou deve interferir na autonomia do usuário jovem. Também não há clareza sobre o que deve ser considerado ao se tratar do “propósito do produto”, tais fatores geram incerteza e insegurança jurídica, uma vez que não há diretriz clara sobre a forma de aplicação da supervisão parental.

Dito isto, para o setor financeiro, a representação legal exercida pelos responsáveis no momento da contratação deve ser considerada como uma forma de supervisão parental, dado que é neste momento que o responsável pode avaliar as condições de contratação do produto e/ou serviço que poderá ser utilizado pelo menor. Para outros contextos além do setor financeiro, além desta forma de supervisão, há outras formas válidas como por meio de controles que permitam limitar o uso (de tempo, contatos, compras etc.), a depender do tipo de serviço ou produto em questão.

Neste sentido, cabe destacar que a depender da natureza do produto e/ou serviço direcionado ao menor de idade, da faixa etária e maturidade, deve ser suficiente para fins de supervisão parental, que as informações sejam divulgadas de forma clara e transparentes, no início da jornada do produto e/ou serviços, aos responsáveis legais, observando a autonomia progressiva do menor, principalmente dos adolescentes.

Além disso, é importante considerar que o intuito do mecanismo de supervisão parental não é inviabilizar ou impedir o uso do aplicativo pelo menor de idade, mas

sim garantir que o uso seja compatível e adequado. Por esta razão, sempre deve ser considerada a finalidade de uso do respectivo produto e/ou serviço.

III. Mecanismos confiáveis de verificação de idade (Art. 9º)

Para impedir acesso de menores a conteúdos impróprios, o art. 9º da lei exige mecanismos confiáveis de verificação de idade a cada acesso, vedando a simples autodeclaração.

Para o setor financeiro, a adoção da aferição de idade é importante para garantir que os produtos e serviços sejam oferecidos de forma adequada e compatível ao público menor de idade. Neste sentido, o setor financeiro já possui mecanismos confiáveis de verificação de idade utilizados antes da contratação de produtos e serviços financeiros, podendo o setor, inclusive, colaborar nas discussões de soluções confiáveis de verificação de idade.

De forma exemplificativa, podem ser considerados como mecanismos confiáveis a: solicitação de documento de identificação e verificação automática ou manual; validação de dados com base em bancos de dados oficiais; mecanismos de dupla verificação (idade + vínculo familiar/responsável) etc. Destaca-se que a verificação de idade feita no início do relacionamento com as instituições financeiras é suficiente e confiável, e uma vez realizada, se torna desnecessária a aferição da idade à cada transação/atividade realizada pelo menor.

IV. “Perfilamento”, “direcionamento de publicidade” e “proibição de criação de perfis comportamentais para fins de publicidade” (arts. 22 e 26)

A lei veda a criação de perfis comportamentais de crianças e adolescentes com base na coleta/tratamento de seus dados pessoais para fins de publicidade comercial. Além disso, proíbe técnicas invasivas como análise emocional, realidade aumentada, realidade virtual ou estendida para esse fim.

No entanto, a norma não define o que configura “perfil comportamental” ou quais dados seriam utilizados para criação/formação de referidos perfis comportamentais vedados pela norma. Neste sentido, pode haver confusões entre “perfil comportamental” e a coleta/obtenção de perfil demográfico simples, segmentação contextual, dados de uso, preferências, histórico de navegação etc.

É necessário sopesar o risco de interpretação restritiva desarrazoada, que pode prejudicar o acesso à cultura, educação, comunicação, por exemplo.

Deste modo, seria importante esclarecer que o perfilamento vedado pela norma está relacionado as publicidades comerciais, e não se confunde com a possibilidade de tratamento de dados pessoais das crianças e adolescentes, com fundamento nas bases legais da LGPD, para perfilamentos no melhor interesse do menor, inclusive para evitar o direcionamento de publicidades para este público e a oferta inadequada de produtos e serviços.

Diante das dúvidas atreladas à norma, é importante que a ANPD publique esclarecimentos para delimitar sua aplicação, especialmente em relação aos segmentos que já são regulados por outras legislações, como o setor financeiro. Essa definição é essencial para evitar sobreposição de obrigações, insegurança jurídica e conflitos regulatórios, garantindo que a norma seja aplicada de forma adequada apenas aos setores que realmente necessitam de proteção adicional.

V. “Medidas técnicas adequadas” (arts. 3 e 5º. §1º), “medidas razoáveis” (art.6º) e “configuração padrão mais protetiva disponível” (art. 7º)

A Lei exige que fornecedores de produtos ou serviços adotem, desde a concepção e ao longo da operação, medidas técnicas adequadas para prevenir riscos e garantir um padrão protetivo de privacidade, segurança e tratamento de dados.

A definição de quais seriam as “medidas técnicas adequadas”, qual nível de segurança, mecanismos e/ou padrões mínimos devem ser adotados é imprecisa. Além disso, a expressão “mais protetiva disponível” depende do que está tecnicamente disponível no mercado, o que pode variar.

O setor financeiro já opera sob um rigoroso arcabouço regulatório do Banco Central que exige altíssimos padrões de segurança, devendo os termos "razoáveis" e "adequadas" dialogar com as normas setoriais já existentes.

Deste modo, sugere-se que a conformidade com as normas de segurança cibernética e prevenção a fraudes do Banco Central e do Conselho Monetário Nacional seja considerada um forte indicativo de cumprimento das "medidas razoáveis e adequadas", criando um mecanismo de "safe harbor" para as instituições reguladas, considerando parâmetros amplamente utilizados, como: criptografia, anonimização ou minimização de dados; avaliações de segurança; relatórios de impacto de proteção de dados etc.

VI. Exploração comercial (Art. 4º, VI), Desenvolvimento progressivo (Art. 7º):



OFÍCIO Nº ED-0030/2025

É importante distinguir "exploração comercial" de conceitos relacionados a "inclusão e educação financeira". A oferta de produtos como contas correntes, de poupança, planos de previdência privada e/ou outros produtos financeiros para crianças e adolescentes são ferramentas legítimas para o desenvolvimento da autonomia e responsabilidade financeira dos jovens.

Deste modo, o conceito de “exploração” deve ser restrito a práticas predatórias destinadas a este público. A oferta de produtos financeiros adequados à faixa etária, com controles parentais e limites apropriados, deve ser explicitamente resguardada como legítima.

Neste sentido, o setor financeiro já aplica a autonomia e o desenvolvimento progressivo, com produtos que acompanham a maturidade do cliente: produtos para menores exigem a representação legal; produtos para crianças oferecem controle parental, enquanto para adolescentes mais velhos é possível disponibilizar maior autonomia de forma gradual.

Logo, a observância da autonomia e desenvolvimento progressivo da criança e adolescente pode estar diretamente atrelada a disponibilização de ferramentas de apoio ao uso consciente e à saúde financeira, como painéis de gastos, alertas de orçamento e conteúdo de educação financeira.

Considerações finais:

Esperamos que as indicações acima contribuam de forma concreta para o trabalho da ANPD, oferecendo referências claras que permitam a compreensão adequada da norma. Reafirmamos o nosso compromisso com a proteção integral de crianças e adolescentes no ambiente digital, alinhado às melhores práticas de governança, segurança e responsabilidade no setor financeiro. Permanecemos à disposição para colaborar na construção de um ambiente regulatório sólido, equilibrado e aderente às dinâmicas que estruturam o sistema nacional de pagamentos.

ED-0030 - Manifestação Febraban e Abecs - Tomada subsídios
Conceitos ECA rev jur 002 pdf

Código do documento 4b80625b-9ef6-4719-9426-eebdaecce2b7

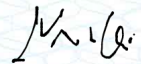


Assinaturas



Luis Vicente Magni De Chiara

Assinou



ROBERTA GASPAR BUSO

Assinou



Marcelo Takeyama

Assinou



Eventos do documento

12 Dec 2025, 16:15:18

Documento 4b80625b-9ef6-4719-9426-eebdaecce2b7 **criado** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). - DATE_ATOM: 2025-12-12T16:15:18-03:00

12 Dec 2025, 16:16:46

PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). Email: paula.mesquita@febraban.org.br. **REMOVEU** o signatário - DATE_ATOM: 2025-12-12T16:16:46-03:00

12 Dec 2025, 16:18:18

Assinaturas **iniciadas** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b).

- DATE_ATOM: 2025-12-12T16:18:18-03:00

12 Dec 2025, 16:19:21

LUIS VICENTE MAGNI DE CHIARA **Assinou** - IP: 54.207.243.177

(ec2-54-207-243-177.sa-east-1.compute.amazonaws.com porta: 44336) - Documento de identificação informado: 293.346.478-09 - DATE_ATOM: 2025-12-12T16:19:21-03:00

12 Dec 2025, 16:31:05

ROBERTA GASPAR BUSO **Assinou** (5ddc9e9a-9c5d-493b-92ca-05a9e2f52f9c) -

- IP: 54.207.205.207 (ec2-54-207-205-207.sa-east-1.compute.amazonaws.com

porta: 29094) - Documento de identificação informado: 306.633.378-79 - DATE_ATOM: 2025-12-12T16:31:05-03:00

12 Dec 2025, 16:40:40

MARCELO TAKEYAMA **Assinou** - [REDACTED] - IP: 186.204.63.68 (bacc3f44.virtua.com.br porta: 28026) - **Geolocalização:** -23.594860199911377 -46.64366189593837 - Documento de identificação informado: 255.964.638-25 - DATE_ATOM: 2025-12-12T16:40:40-03:00

Hash do documento original

(SHA256):1981938b2d9eb39fe7be5b2bbaed03ed43d00771a36cc642375b9b6e011fb8e2

(SHA512):f2e224c156db5cb436d8dcdae4d65c64a6c9eef8b935f8a489b199fe7a5741ede69ce0fbd034a0c0574f8dd2436ac1799b23df5f30c79f88f3476bb884145a7

Esse log pertence **única e exclusivamente** aos documentos de HASH acima**Esse documento está assinado e certificado pela D4Sign****Integridade certificada no padrão ICP-BRASIL**Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.

Contribuições à Tomada de Subsídios para esclarecer conceitos do ECA Digital

I. Introdução e apresentações

A Telefônica Brasil S.A, detentora da marca “Vivo”, oferece aos seus clientes um completo portfólio de produtos, incluindo serviços de voz (fixos e móveis), dados móveis, ultra banda larga, TV por assinatura, tecnologia da informação e serviços digitais (como, por exemplo, serviços financeiros, e-commerce, casa conectada, de nuvem, de entretenimento e segurança). Nosso propósito é “Digitalizar para aproximar”, o que reforça nosso compromisso de levar conexão de qualidade e inclusão digital para pessoas e empresas em todo o território nacional, pois acreditamos que a conectividade é a porta de entrada para o mundo digital e pode gerar muitas oportunidades para todos.

A Vivo se preocupa com a proteção de crianças e adolescentes em ambientes digitais, bem como com a segurança no tratamento dos dados pessoais de seus clientes e se pauta em três pilares fundamentais: a confidencialidade, a integridade e a disponibilidade das informações que gerimos.

O presente documento apresenta considerações da Vivo sobre as discussões promovidas pela ANPD acerca dos conceitos trazidos pelo recém-aprovado ECA Digital.

Congratulamos o Conselho Diretor da ANPD pela promoção do diálogo diante de temas importantes e de fundamental atenção para que todas as partes interessadas possam apresentar suas considerações visando contribuir para as premissas estabelecidas pelo ECA Digital, buscando sempre a proteção das crianças e adolescentes no ambiente digital.

II. Contribuições

Pergunta: Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

Com base no ECA Digital e na Nota Técnica disponibilizada, entendemos que diversos termos e conceitos carecem de maior precisão e critérios objetivos para aplicação prática. Expressões como “acesso provável”, “suficiente probabilidade de uso e atratividade”, “facilidade de acesso” e “grau significativo de risco” são imprecisas, pois não existem parâmetros claros para definir quando um serviço deve ser considerado acessível a menores ou quando apresenta risco relevante. Para trazer maior segurança jurídica aos entes regulados e para correta aplicação da nova lei, é necessário estabelecer conceitos concretos que reduzam interpretações subjetivas. Da mesma forma, conceitos como “mecanismos confiáveis de verificação de idade” e “mais alto nível de proteção disponível” precisam de definições detalhadas para orientar de maneira eficaz os entes regulados.

Aos seguintes conceitos apresentados no ECA Digital, sugerimos que sejam definidos de forma clara e objetiva, com parâmetros que facilitem a aplicação prática e reduzam divergências:

- **Acesso provável por crianças e adolescentes (art. 1º, parágrafo único):** entendemos que esse conceito deve ser mais bem delineado pela ANPD, levando em consideração, especialmente, que diferentes serviços apresentam níveis de risco distintos. A falta de clareza resulta em uma abordagem uniforme que trata serviços com perfis de risco completamente diferentes da mesma maneira, fazendo com que serviços comuns tenham as mesmas obrigações que serviços que oferecem conteúdo ou interação direta com menores de idade. Uma abordagem mais adequada seria seguir o modelo da Lei de Serviços Digitais da UE, que exige avaliação baseada no risco, considerando fatores como finalidade, tipo de conteúdo, funcionalidades, público-alvo e medidas de proteção.
- **Suficiente probabilidade de uso e atratividade e considerável facilidade ao acesso e utilização (Art. 1º, parágrafo único, I e II):** recomenda-se que seja orientada por critérios claros e proporcionais ao risco, evitando subjetividade e interpretações amplas. É essencial considerar a natureza e o contexto do serviço, o público-alvo e as funcionalidades oferecidas, em vez de aplicar regras uniformes que não refletem a realidade operacional dos diferentes agentes. Recomenda-se utilizar indicadores como a análise contextual do serviço, incluindo fatores como atratividade para menores e funcionalidades interativas. Essa abordagem deve ser complementada por princípios de proporcionalidade, garantindo que obrigações mais rigorosas sejam aplicadas apenas a serviços que apresentem riscos concretos e elevados. Além disso, é importante reconhecer a diversidade de modelos de negócio e evitar encargos desnecessários para agentes que não oferecem conteúdo ou interação direta com menores. A definição deve ser clara e compatível com boas práticas internacionais, assegurando previsibilidade regulatória e equilíbrio entre proteção, inclusão e inovação.
- **Significativo grau de risco (Art. 1º, parágrafo único, III):** A caracterização de risco significativo deve seguir o princípio da proporcionalidade e o melhor interesse da criança e do adolescente. A regulamentação deve considerar não apenas a natureza do conteúdo, mas também o contexto do serviço, suas funcionalidades e o grau de interação oferecido. É fundamental evitar critérios rígidos ou genéricos que possam gerar sobrecarga regulatória para serviços de baixo risco. Recomenda-se uma abordagem sistêmica, com matriz de risco alinhada às práticas de Relatórios de Impacto à Proteção de Dados (RIPD), considerando fatores como tipo de interação entre usuários, presença de funcionalidades abertas, mecanismos de moderação, modelo de negócios e práticas de monetização. Essa análise deve ser dinâmica e contextual, permitindo calibrar as obrigações conforme o risco efetivo. Para serviços que não oferecem conteúdo ou interação direta com menores, como empresas de telecomunicações, as obrigações devem ser claramente delimitadas. Além disso, os critérios devem ser transparentes, auditáveis e compatíveis com boas práticas internacionais, garantindo segurança jurídica e previsibilidade.
- **Medidas adequadas e proporcionais (art. 3º), medidas razoáveis desde a concepção (art. 6º) e medidas eficazes (art. 9º):** ao longo da lei, é exigido que os agentes regulados adotem medidas “adequadas”, “razoáveis”, “eficazes” e “proporcionais” para garantir a proteção e a segurança dos menores. No entanto, esses termos são genéricos e carecem de definição prática, o que gera insegurança jurídica e risco de interpretações divergentes. É fundamental que a ANPD estabeleça diretrizes claras sobre quais medidas são consideradas suficientes para atender às exigências legais. Essas orientações devem indicar parâmetros objetivos, como exemplos de medidas técnicas e organizacionais e, critérios de proporcionalidade, garantindo que serviços de baixo risco não sejam onerados com exigências desnecessárias.

- **Configuração do modelo mais protetivo disponível (art. 7º) e mais alto nível de proteção disponível (art. 17, § 4º):** Os termos utilizados nos arts. 7º e 17, § 4º carecem de definição objetiva, o que gera insegurança jurídica para os agentes regulados. A ausência de parâmetros claros dificulta a implementação adequada das exigências, podendo levar a interpretações divergentes e à adoção de medidas desproporcionais. Recomendamos que a ANPD publique orientações regulatórias detalhadas, especificando quais medidas e controles são esperados para garantir conformidade com a lei. Essas diretrizes devem indicar, por exemplo, práticas relacionadas à configuração padrão de privacidade, restrições de publicidade e marketing para menores, e critérios para compartilhamento de dados com terceiros. Além disso, é essencial que as orientações considerem a proporcionalidade, evitando sobrecarga regulatória para serviços de baixo risco. A abordagem deve ser baseada em risco, permitindo que empresas adotem medidas compatíveis com a natureza e funcionalidades do serviço, garantindo proteção efetiva sem comprometer a inovação ou a experiência do usuário.
- **Metadados (art. 27, § 2º, II):** O conceito de metadados é extremamente amplo, pois se refere a dados que descrevem outros dados. Essa abrangência pode gerar dúvidas sobre quais informações devem ser armazenadas pelos agentes regulados para atender à lei. Recomenda-se para a ANPD publicar orientações específicas definindo quais metadados devem ser armazenados, considerando a finalidade legal e evitando exigências desproporcionais.

De forma geral, sugerimos tornar os conceitos mais objetivos, claros e auditáveis, evitando detalhamento excessivo ou subjetividade que gere complexidade regulatória. As obrigações devem ser proporcionais ao risco e ao tipo de serviço, evitando impacto indevido em empresas que não ofertam produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes. É fundamental priorizar conformidade com normas existentes, como LGPD e Marco Civil da Internet, além de boas práticas internacionais, e incluir orientações claras sobre escopo para que empresas de infraestrutura, como telecomunicações, não sejam indevidamente enquadradas.



b/luz

B/LUZ

R. Ramos Batista, 444, Vila Olímpia

04552-020, São Paulo – SP

baptistaluz.com.br

/ Assunto: **Anexo à Tomada de Subsídios – Conceitos Previstos na Lei nº 15.211/2025 (ECA Digital)**

/ Para: **Agência Nacional de Proteção de Dados ("ANPD")**

/ De: **b/luz**
Fernando Bousso
Felipe Gabriades
Matheus B. Kasputis
Thiago Peregrino
Vitor Delafina

/ Data: 12 de dezembro de 2025

Sumário

1. Produto ou Serviço de Tecnologia da Informação.....	3
2. Acesso Provável	4
3. Produto ou Serviço Direcionado a Crianças e Adolescentes	6
4. Serviço com Controle Editorial	7
5. Provedores de Conteúdos Protegidos por Direitos Autorais	8
6. Conteúdo Impróprio, Inadequado ou Proibido.....	8
7. Interação entre Usuários.....	Error! Bookmark not defined.
8. Funcionalidades não Essenciais ao Funcionamento Básico dos Sistemas.....	Error! Bookmark not defined.

Introdução: Este Anexo tem como objetivo complementar a contribuição registrada na Tomada de Subsídios sobre conceitos do ECA Digital disponibilizada na plataforma Brasil Participativo. Aqui são apresentados, de forma organizada, os motivos pelos quais determinados termos demandam maior precisão conceitual, bem como os riscos práticos de definições excessivamente amplas, vagas ou inconsistentes para a interpretação e a aplicação do futuro instrumento regulatório. Além de justificar a necessidade de detalhamento, o documento consolida parâmetros que podem orientar a construção das definições, com foco em segurança jurídica, proporcionalidade, aplicabilidade técnica e aderência ao regime de proteção de dados pessoais de crianças e adolescentes. A intenção é apoiar a ANPD na formulação de conceitos operacionais, verificáveis e compatíveis com diferentes contextos de uso, reduzindo ambiguidades e favorecendo a harmonização entre atores regulados, sociedade civil e órgãos de controle.

1. Produto ou Serviço de Tecnologia da Informação

Art. 2º Para os fins desta Lei, considera-se:

I – **produto ou serviço de tecnologia da informação:** produto ou serviço fornecido a distância, por meio eletrônico e provido em virtude de requisição individual, tais como aplicações de internet, programas de computador, softwares, sistemas operacionais de terminais, lojas de aplicações de internet e jogos eletrônicos ou similares conectados à internet ou a outra rede de comunicações.

A locução “outra rede de comunicações” amplia deliberadamente o alcance do conceito de “produto ou serviço de tecnologia da informação” para além da internet, mas o faz de maneira aberta, sem indicar quais redes são abrangidas e quais ficam excluídas. Essa abertura cria incerteza estrutural de enquadramento, uma vez que produtos e serviços podem operar em diversos tipos de redes, como redes de telefonia móvel, intranets, redes de TV por assinatura, redes satelitais, redes de radiocomunicação, redes privadas corporativas, redes locais, entre outras.

Sem parâmetros, agentes econômicos tendem a adotar estratégias opostas e igualmente problemáticas, incluindo: **(a)** sobreinclusão, aplicando o ECA Digital a qualquer software com conectividade mínima, com custos de conformidade desproporcionais; ou **(b)** subinclusão, restringindo o conceito apenas à *world wide web*, gerando lacunas de proteção em serviços entregues por redes alternativas, como serviços interativos em *set-top boxes* ou aplicações distribuídas em ambientes controlados.

A expressão “outra rede de comunicações” deve receber interpretação restritiva, sob pena de o conceito de “produto ou serviço de tecnologia da informação” tornar-se excessivamente elástico e, na prática, passar a abranger qualquer serviço entregue mediante algum tipo de infraestrutura de telecomunicações. A redação legal, ao mencionar produtos “conectados à internet ou a outra rede de comunicações”, sugere a intenção de capturar ambientes digitais conectados que, embora não sejam a internet pública, reproduzem a mesma lógica funcional de conectividade remota e interação digital. Se a expressão for lida como sinônimo de “qualquer rede de telecomunicações”, haveria risco real de deslocar o escopo do ECA Digital para o plano da mera infraestrutura de conectividade, produzindo sobreinclusão e insegurança jurídica para empresas que não detêm controle sobre o serviço digital final.

É recomendável que a ANPD delimite o alcance de “outra rede de comunicações” para significar, exclusivamente, redes que viabilizem a prestação de um serviço de TI a distância, por meio eletrônico e sob requisição individual, em regime funcionalmente semelhante ao acesso via internet. O núcleo da expressão deve ser a existência de conectividade de dados apta a permitir funcionalidades típicas de serviços digitais, e não a simples circunstância de o usuário estar conectado a alguma rede em sentido amplo. Em outras palavras, a incidência deve recair sobre o produto ou serviço digital, e não sobre a rede enquanto infraestrutura.

2. Acesso Provável

Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de **acesso provável** por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.

Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações:

I – suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes;

II – considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes; e

III – significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital.

2.1. Suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes

O termo demanda critérios objetivos para reduzir a subjetividade na avaliação de enquadramento ao ECA Digital e evitar insegurança jurídica. Se interpretado de forma ampla, pode configurar praticamente qualquer serviço como “provável” de ser acessado, esvaziando a utilidade do critério e dificultando a conformidade por parte dos fornecedores de serviços ou produtos de tecnologia da informação.

Para fins de clareza e precisão jurídica, é necessário que haja uma melhor definição de limiares e evidências mínimas para caracterizar “suficiente probabilidade” e “atratividade”, com base em dados observáveis e atualizáveis, como métricas de audiência por faixa etária, direcionamento de conteúdo e linguagem, elementos de design e funcionalidades tipicamente atraentes para menores, canais de aquisição e publicidade, categorias de conteúdo e finalidades do serviço, além de fatores de contexto como barreiras de acesso, mecanismos de verificação etária e classificação indicativa.

Ademais, é importante prever exemplos de aplicação e de não aplicação, além de diferenciar situações de acesso incidental de uso recorrente ou intencional.

2.2. Considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes

A expressão “considerável facilidade ao acesso e utilização” é ampla e subjetiva, o que dificulta que provedores de produtos ou serviços de tecnologia da informação compreendam quando estão submetidos às obrigações específicas previstas na lei. Termos como “considerável” e “facilidade” carecem de critérios objetivos, podendo gerar interpretações divergentes e insegurança sobre o alcance das disposições. Assim, é necessário que a regulamentação estabeleça parâmetros claros para caracterizar essa condição.

Os parâmetros a serem formalmente definidos na regulamentação devem considerar, principalmente, a existência ou ausência de barreiras técnicas ou práticas que limitem o acesso por crianças e adolescentes. Para tanto, podem ser considerados critérios como: **(a)** simplicidade de navegação e linguagem; **(b)** características de design que favoreçam o uso por menores; **(c)** natureza e atratividade do conteúdo; e **(d)** evidências de utilização desse público na prática.

2.3. Significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital.

A expressão “significativo grau de risco” é central para que empresas consigam determinar se estão sujeitas ao ECA Digital e quais obrigações devem observar. Entretanto, a lei não explicita critérios objetivos para aferição desse grau de risco, o que

tende a gerar assimetria interpretativa, variações entre setores e insegurança jurídica relevante para empresas que precisam priorizar investimentos em compliance, desenho de produtos, engenharia e governança de dados. Além disso, o termo agrega três dimensões distintas – privacidade, segurança e desenvolvimento biopsicossocial –, cada qual com naturezas de risco próprias. Sem clarificação regulatória, empresas podem enfrentar dificuldades para integrar tal conceito em seus modelos de risco, avaliações internas, relatórios de impacto, documentação de conformidade e mecanismos de auditoria.

Sugere-se que a ANPD estabeleça critérios objetivos para identificar quando um risco se torna “significativo”. No que diz respeito especialmente ao grau de risco à privacidade, a ANPD deveria esclarecer como metodologias já regulamentadas no âmbito da LGPD – como os critérios de classificação de risco para agentes de tratamento de pequeno porte (Resolução CD/ANPD nº 2/2022, art. 4º) e de notificação de incidentes de segurança (Resolução CD/ANPD nº 15/2024, art. 5º) – podem ser aproveitadas no contexto de aplicação do ECA Digital, indicando em que medida tais parâmetros podem servir de referência ou quando são insuficientes para caracterizar risco “significativo”. Essa harmonização é essencial para que empresas evitem interpretações fragmentadas entre regimes normativos conectados.

3. Produto ou Serviço Direcionado a Crianças e Adolescentes

Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo **produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes** no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.

Embora a ideia de direcionamento pareça intuitiva, o termo não indica de forma precisa quais características levam um produto ou serviço a ser considerado “direcionado” ao público infantil ou adolescente. A ausência de critérios objetivos abre espaço para interpretações inconsistentes, especialmente em setores onde diferentes faixas etárias utilizam os mesmos serviços. A regulamentação deve esclarecer quais elementos determinam o direcionamento, evitando incertezas quanto às obrigações decorrentes.

Nesse cenário, a regulamentação deve incluir, de forma expressa, critérios objetivos para a identificação de produtos ou serviços “direcionados” a crianças e adolescentes. Essa definição deve considerar a finalidade declarada e as características práticas do serviço, como:

- **Conteúdo disponibilizado:** temas, linguagens, personagens, formatos ou narrativas compatíveis com os interesses típicos de crianças ou adolescentes.

- **Design e usabilidade:** recursos visuais, gráficos, elementos interativos ou outras formas de engajamento que sejam claramente voltadas a esse público.
- **Comunicação e marketing:** campanhas, publicidade, materiais promocionais ou linguagem institucional que tenham como foco esse público, diretamente ou por meio de familiares/responsáveis.
- **Configurações padrão e funcionalidades:** opções predefinidas que favorecem o uso infantil, como ativação automática de interações, personalizações lúdicas e ausência de mecanismos de controle etário.
- **Segmentação intencional de público:** evidências de que o serviço foi concebido para atingir crianças ou adolescentes.

4. Serviço com Controle Editorial

Art. 2º Para os fins desta Lei, considera-se:

IX – **serviço com controle editorial:** aplicação de internet que tem como finalidade principal a disponibilização de conteúdos previamente selecionados, sem o uso de meios automatizados de seleção, por agente econômico responsável;

O ECA Digital utiliza o conceito de “serviços com controle editorial” para diferenciar, dentro do ecossistema digital, aqueles serviços cuja seleção, organização e disponibilização de conteúdos são determinantes para a imposição de obrigações especiais relacionadas à proteção de crianças e adolescentes. Contudo, a legislação não explicita critérios objetivos que permitam distinguir, de forma clara, serviços baseados em controle editorial ativo daqueles estruturados predominantemente como plataformas intermediárias, que apenas hospedam, organizam ou recomendam conteúdo gerado por terceiros.

Tal lacuna interpretativa gera dificuldades significativas para empresas reguladas, sobretudo em ambientes digitais caracterizados por modelos híbridos, nos quais coexistem elementos editoriais (curadoria humana, seleção de catálogos, promoção de coleções etc.) e funções típicas de plataformas. Sem parâmetros claros, empresas enfrentam incertezas quanto à correta classificação de seus serviços, o que impacta a identificação das obrigações aplicáveis, o desenho e o registro das salvaguardas técnicas, a avaliação de riscos e a alocação de recursos e a previsibilidade regulatória.

Além disso, a ausência de delimitação clara pode gerar assimetria competitiva na medida em que empresas com modelos semelhantes podem ser tratadas de maneira desigual a depender da interpretação mais ou menos extensiva adotada em cada caso concreto.

A diretriz da ANPD deve considerar parâmetros objetivos que permitam avaliar, de forma verificável, se o provedor exerce controle editorial. Entre eles, podem ser considerados

aspectos como: **(a)** existência de seleção ativa e curadoria prévia de conteúdos, com critérios editoriais definidos pelo provedor; **(b)** intervenção humana relevante no processo de escolha, organização ou priorização de conteúdos disponibilizados aos usuários; **(c)** responsabilidade direta pela produção, encomenda ou licenciamento de conteúdos, ainda que parcialmente; **(d)** capacidade de determinar a linha editorial, estética ou temática do catálogo; e **(e)** distinção entre moderação reativa e decisões editoriais proativas que moldem o conjunto de conteúdos oferecidos. Também é relevante considerar fatores contextuais, como a predominância de conteúdo profissional vs. conteúdo de usuários, a existência de áreas segregadas com controle editorial, o grau de automatização na seleção de conteúdos e a finalidade principal do serviço.

5. Conteúdo Impróprio, Inadequado ou Proibido

Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja **impróprio, inadequado ou proibido** para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos.

Apesar de o art. 9º, § 2º, incluir referência expressa a material pornográfico, a expressão “quaisquer outros vedados pela legislação vigente” permanece aberta e pode gerar incerteza sobre o universo de conteúdos abrangidos, com risco de interpretações divergentes, obrigações de bloqueio excessivas ou insuficientes e dificuldades de implementação consistente entre diferentes serviços. Assim, vê-se como essencial indicar, de forma taxativa ou por remissão objetiva, quais categorias normativas compõem o universo de “vedado pela legislação vigente”.



AMOBITEC

Associação Brasileira de Mobilidade e Tecnologia

OF/AMOBITEC N. 107/2025

São Paulo, 12 de dezembro de 2025.

Ref.: Sugestões à Tomada de Subsídios para esclarecimento de conceitos críticos do recém-sancionado Estatuto Digital da Criança e do Adolescente (ECA Digital)

Senhor Diretor,

A **Associação Brasileira de Mobilidade e Tecnologia ("AMOBITEC")**, entidade representante das empresas que prestam serviços tecnológicos relacionados à mobilidade de pessoas ou bens, como aplicativos de delivery e intermediação de viagens de transporte individual privado de mobilidade urbana, vem, respeitosamente, **EXPOR SEU POSICIONAMENTO** na Tomada de Subsídios voltada ao esclarecimento de conceitos críticos do recém-sancionado Estatuto Digital da Criança e do Adolescente (ECA Digital), iniciativa destinada a eliminar dúvidas e ambiguidades terminológicas e a assegurar a aplicação segura, uniforme e efetiva da lei em favor da proteção de crianças e adolescentes no ambiente digital.

André Alencar Porto

Diretor-Executivo



I. BREVES CONSIDERAÇÕES

A Lei nº 15.211/2025 (ECA Digital) inaugurou um regime próprio de proteção de crianças e adolescentes no ambiente digital, alinhado às diretrizes constitucionais da proteção integral e às normas infraconstitucionais correlatas, como o ECA, o CDC, o Marco Civil da Internet e a LGPD. O diploma introduziu definições essenciais para compreender a dinâmica das atividades digitais contemporâneas, especialmente aquelas baseadas no tratamento intensivo de dados pessoais e que impactam diretamente a privacidade e os direitos fundamentais de crianças e adolescentes.

A correta aplicação dessas definições depende de atuação regulatória consistente, cabendo à autoridade competente esclarecer conceitos, orientar agentes regulados e detalhar obrigações legais por meio de manifestações interpretativas, regulamentos e guias. Entre os pontos que demandam precisão destacam-se o escopo de incidência da lei, como os conceitos de produto ou serviço de tecnologia da informação (art. 2º, I); acesso provável (art. 1º, parágrafo único); provedores com controle editorial e provedores de conteúdo protegido por direitos autorais (art. 39, § 1º), além dos deveres de prevenção, proteção, informação e segurança (art. 5º, caput).

Nesse contexto, e em atenção à Tomada de Subsídios¹ atualmente em andamento, esta manifestação se propõe a responder às questões formuladas pela autoridade, identificando (i) os principais conceitos, termos e expressões do ECA Digital que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei e (ii) os parâmetros que podem ser considerados para tornar tais conceitos mais precisos, proporcionais e operacionalizáveis. Busca-se, com isso, contribuir para a construção de um ambiente regulatório estável e coerente, que reduza incertezas para os agentes

¹ <https://brasilparticipativo.presidencia.gov.br/processes/conceitosecadigital/f/1912/>



AMOBITEC

Associação Brasileira de Mobilidade e Tecnologia

regulados e assegure que o Estatuto Digital alcance plena efetividade na proteção de crianças e adolescentes no ambiente digital.

II. QUESTÕES NORTEADORAS

A seguir, apresentamos quadro consolidado com os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que, em nossa avaliação, demandam esclarecimentos adicionais para assegurar sua adequada compreensão e aplicação.

O referido quadro reúne respostas fundamentadas para cada ponto, estruturadas com foco em precisão técnica, coerência regulatória, proporcionalidade e alinhamento às melhores práticas internacionais de proteção infantil em ambientes digitais.



ARTIGO QUE CONTÉM OS CONCEITOS QUE DEMANDAM ESCLARECIMENTOS	CONCEITOS QUE DEMANDAM ESCLARECIMENTOS	JUSTIFICATIVA
Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.	“DE ACESSO PROVÁVEL”	Recomendamos que sejam introduzidas orientações regulamentares adicionais para esclarecer que apenas os serviços que representam um risco significativo de danos para menores estão abrangidos. Ao determinar se um serviço representa um risco significativo de dano aos menores, devem ser considerados os fatores: 1) a finalidade principal do serviço; 2) a natureza e os tipos de conteúdo disponibilizados através do serviço; 3) as características e funcionalidades do serviço, incluindo, mas não se limitando a: (i) capacidades de comunicação direta entre usuários; (ii) recursos de interação social; (iii) funcionalidade que permite o compartilhamento em grande escala de conteúdo gerado pelo usuário final; 7) barreiras de acesso projetadas para impedir que crianças acessem conteúdo potencialmente prejudicial; e 8) se o conteúdo fornecido pelo serviço é normalmente acessado por meio de dispositivos compartilhados. As orientações regulamentares devem também esclarecer que os serviços necessitam de flexibilidade para desenvolver medidas de proteção que sejam razoavelmente proporcionais ao seu perfil de risco específico, tendo em conta a natureza do seu serviço. Isto deve incluir o reconhecimento de que nem todos os requisitos são adequados para todos os serviços (por exemplo, os limites de tempo de ecrã fazem pouco sentido para serviços que não se destinam a uma utilização contínua ou que se destinam a uma utilização prolongada, como os serviços de streaming de música). As orientações devem também centrar-se na obtenção de resultados de proteção, em vez de prescrever abordagens técnicas específicas, permitindo que os serviços implementem soluções que se alinhem com os seus casos de utilização reais e perfis de risco.



		As orientações regulamentares devem, ainda, considerar a clarificação de que este termo se aplica apenas a serviços que se destinam diretamente a menores ou, se se tratar de um serviço para o público em geral, apenas às partes do serviço dirigidas a menores (ou seja, perfis específicos de crianças), obedecidos os riscos significativo de danos aos menores. Isto garantiria que os produtos e serviços se concentrassem na sua conformidade apenas para os produtos ou serviços, ou partes dos mesmos, que são realmente suscetíveis de serem acessados por crianças e adolescentes. Diante disso, recomenda-se que a aplicação do ECA Digital adote abordagem baseada em risco, alcançando apenas serviços que representem risco significativo a crianças e adolescentes, considerados sua finalidade, conteúdo, funcionalidades e barreiras de acesso. Tal interpretação assegura medidas proporcionais ao perfil de risco e concentra as obrigações apenas nos serviços ou funcionalidades efetivamente direcionados a menores, privilegiando resultados de proteção sem impor exigências desproporcionais.
O Art. 1º do ECA Digital demanda esclarecimentos adicionais especificamente quanto aos critérios definidores de “acesso provável por crianças e adolescentes”. O parágrafo único apresenta três elementos: (I) suficiente probabilidade de uso e atratividade; (II) considerável facilidade	“SUFICIENTE PROBABILIDADE DE USO E ATRATIVIDADE” “CONSIDERÁVEL FACILIDADE DE ACESSO E UTILIZAÇÃO” “SIGNIFICATIVO GRAU DE RISCO” “COMPARTILHAMENTO DE INFORMAÇÕES EM LARGA ESCALA”	Sugere-se interpretação que prestigie o princípio da razoabilidade, garantindo a efetividade da proteção sem impor tratamento regulatório desproporcional a produtos ou serviços cujo público-alvo não é infantojuvenil e cujo modelo de operação não implica exposição significativa de dados. Essa interpretação confere previsibilidade jurídica às empresas e evita que atividades orientadas ao público adulto, mas tecnicamente acessíveis a menores, sejam tratadas como intrinsecamente arriscadas sem fundamento técnico ou fático. Parâmetros interpretativos para cada termo: “Suficiente probabilidade de uso e atratividade”: recomenda-se que essa probabilidade seja aferida com base em parâmetros mensuráveis que permitam aplicação uniforme e verificável da norma, garantindo segurança jurídica aos entes



de acesso e utilização; e (III) significativo grau de risco à privacidade, segurança ou desenvolvimento biopsicossocial, especialmente em produtos voltados à interação social e compartilhamento em larga escala		privados – tais como conteúdo explícito direcionado a crianças, que não envolvam campanhas educacionais sobre adesão a produtos e serviços direcionados cujos parâmetros de controle e proteção por supervisão de adulto são maiores do que o produto ou serviço para o público em geral Além disso, é necessário considerar que o conceito legal de “crianças e adolescentes” abrange faixa etária bastante ampla. Indivíduos situados no limite superior dessa faixa, por exemplo, entre 16 e 18 anos incompletos, podem possuir interesses e comportamentos significativamente próximos aos de adultos, especialmente jovens adultos, de modo que a aplicação deste conceito deve ser razoável, sob pena do quesito ser satisfeito por grande parte, senão todos, produtos e serviços disponíveis online. “Considerável facilidade de acesso e utilização”: sugere-se que o critério seja vinculado a funcionalidades projetadas especificamente para crianças (por exemplo, interfaces lúdicas e pedagógicas) e não à mera possibilidade de acesso por ausência de barreiras tecnológicas. “Significativo grau de risco”: recomenda-se que o risco seja aferido de forma objetiva e mensurável, com base no tipo de dado tratado, natureza do serviço, modelo de interação entre usuários, finalidade do produto ou serviço e existência de monitoramento. “Compartilhamento de informações em larga escala”: recomenda-se interpretação que restrinja este conceito a plataformas cujo propósito central seja a interação social massiva, não alcançando aplicações cujo fluxo de dados é estritamente funcional, transacional ou restrito à prestação de serviços. Essa interpretação confere previsibilidade jurídica às empresas e evita que atividades orientadas ao público adulto, mas tecnicamente acessíveis a menores, sejam tratadas como intrinsecamente arriscadas sem fundamento técnico ou fático. Dessa forma, recomenda-se que a interpretação dos conceitos analisados seja



		orientada pelos princípios da razoabilidade e da proporcionalidade, com a adoção de parâmetros objetivos, verificáveis e compatíveis com o perfil de risco efetivamente associado a cada produto ou serviço. Tal abordagem permite assegurar a proteção adequada de crianças e adolescentes em ambientes digitais sem impor tratamento regulatório desproporcional a aplicações cujo público-alvo não é infantojuvenil e cujo modelo de operação não implica exposição significativa de dados ou riscos relevantes. Ao conferir maior precisão aos conceitos de “acesso provável”, “probabilidade de uso e atratividade”, “facilidade de acesso”, “grau de risco” e “compartilhamento em larga escala”, a autoridade reguladora promove previsibilidade jurídica, evita enquadramentos excessivamente amplos e garante que atividades legítimas, voltadas predominantemente ao público adulto, não sejam indevidamente tratadas como intrinsecamente arriscadas, sem fundamento técnico ou fático.
Art. 7º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo mais protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerados a autonomia e o desenvolvimento progressivo do indivíduo e justificado o melhor interesse da criança e	“DE ACESSO PROVÁVEL “ E “ O GRAU MAIS ELEVADO DE PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS” E “ DISPONIBILIZAÇÃO DE INFORMAÇÕES CLARAS, ACESSÍVEIS E ADEQUADAS”	No que concerne à aplicabilidade do artigo aos serviços “de acesso provável por crianças e adolescentes”, são aplicáveis as considerações pontuadas com relação ao Artigo 1. O Artigo 7 e outros artigos semelhantes exigem que as empresas operem com “o grau mais elevado de proteção da privacidade e dos dados pessoais”. No entanto, o que constitui “o grau mais elevado de proteção da privacidade e dos dados pessoais” não está definido, deixando as empresas com muita incerteza sobre como operar seus serviços e produtos. Recomendamos que as orientações regulatórias definam explicitamente o que constitui “o grau mais elevado de proteção da privacidade e dos dados pessoais”, indicando principalmente os controles em mente (ou seja, publicidade, marketing, compartilhamento de dados com terceiros) e como esses controles devem ser definidos por padrão para menores de idade. O Artigo 7 e outros artigos semelhantes exigem que as empresas forneçam informações claras, acessíveis e adequadas para que os menores e seus responsáveis possam fazer escolhas informadas. Recomendamos uma orientação regulatória que



do adolescente. § 1º O produto ou serviço referido no caput deste artigo deverá, por padrão, operar com o grau mais elevado de proteção da privacidade e dos dados pessoais, observado que será obrigatória a disponibilização de informações claras, acessíveis e adequadas para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à eventual adoção de configurações menos protetivas.		estabeleça que uma seção sobre menores na política de privacidade da empresa ou nos Termos & Condições (T&Cs) é satisfaz o critério de informação “clara, acessível e adequada”, conforme exigido pelo Artigo 7. Nesse contexto, recomenda-se que as orientações regulatórias esclareçam, de forma objetiva e operacional, o alcance das obrigações previstas no art. 7º do ECA Digital, especialmente quanto ao conteúdo do “grau mais elevado de proteção da privacidade e dos dados pessoais” e aos critérios para o fornecimento de informações “claras, acessíveis e adequadas”.
Art. 7º (...) § 2º Os fornecedores de que trata o caput deste artigo deverão abster-se de realizar o tratamento dos dados pessoais de crianças e de adolescentes de forma que cause, facilite ou contribua para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei,	“CAUSEM, FACILITEM OU CONTRIBUAM”	O art. 7º, §2º, do ECA Digital proíbe tratamento dos dados pessoais de crianças e de adolescentes de forma que “cause, facilite ou contribua” para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei. No entanto, a leitura literal do dispositivo, na prática, implicaria em óbice intransponível à maioria das atividades de tratamento. Isso porque a expressão “cause, facilite ou contribua” é abrangente e, se interpretada literalmente, acaba por vedar, na prática, qualquer atividade de tratamento de dados envolvendo menores de idade. Isso ocorre porque os verbos “facilitar” e “contribuir” sugerem que estariam proibidas as atividades capazes de gerar ou contribuir com resultado danoso – ou seja



observados os princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e o melhor interesse da criança e do adolescente.		quaisquer atividades que envolvam riscos aos direitos legais dos menores. Como o dispositivo é silente quanto ao grau de risco, sua redação abarca indistintamente todos os tratamentos, já que toda atividade de tratamento envolve algum nível de risco aos titulares. É precisamente por essa razão que legislações modernas de proteção de dados, como a Lei Geral de Proteção de Dados, adotam abordagens baseadas em risco. Deste modo, previsão genérica de proibição a atividades que envolvam riscos aos direitos do titular, na prática, proíbe todas as atividades de tratamento. Diante desse contexto, recomenda-se que o art. 7º, §2º, do ECA Digital seja interpretado de forma sistemática e alinhada ao regime de proteção de dados vigente, de modo a compreender que a vedação ali prevista incide apenas sobre atividades de tratamento que gerem riscos desproporcionais aos direitos e às liberdades de crianças e adolescentes, ou que sejam, em si mesmas, incompatíveis ou violadoras desses direitos. Tal leitura preserva a finalidade protetiva da norma sem inviabilizar, de forma automática, atividades legítimas de tratamento de dados necessárias à prestação de serviços e à implementação de medidas de segurança no ambiente digital.



Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos. § 1º Para dar efetividade ao disposto no caput, deverão ser adotados mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração.	"A CADA ACESSO"	À luz da LGPD, em especial dos princípios da necessidade e da minimização de dados (art. 6º, III), uma leitura literal que exigisse verificação de idade sempre que o usuário simplesmente abrisse o aplicativo, mesmo sem interação relevante, conduziria a um cenário de tratamento excessivo e desnecessário de dados pessoais, em aparente desconformidade com a própria LGPD. No contexto internacional, instrumentos como o Age Appropriate Design Code da ICO (Reino Unido) e análises sobre "age assurance" no âmbito europeu adotam, de forma consistente, uma abordagem baseada em risco, em que os mecanismos de verificação/asseguramento de idade são calibrados conforme: • a natureza do conteúdo ou serviço; • a probabilidade de acesso por crianças e adolescentes; • o grau de risco associado; • e o impacto na privacidade e na experiência do usuário. Essas referências, embora não utilizem a expressão "a cada acesso", reconhecem que: • os mecanismos de idade podem ser aplicados em pontos específicos da jornada (ponto de acesso ao serviço, acesso a determinada funcionalidade, momento da transação etc.); • e que reavaliações periódicas ou em marcos relevantes (como mudança de faixa etária) são mais compatíveis com proporcionalidade do que uma verificação reiterada a cada interação meramente técnica. Diante disso, propõe-se que a ANPD esclareça que a expressão "a cada acesso" é : 1. Material, e não meramente técnica "Acesso" não deve abarcar indiscriminadamente todos os eventos técnicos (como simples abertura do aplicativo, carregamento de tela ou realização de login), mas sim momentos relevantes da jornada em que haja efetivo risco de exposição da criança ou adolescente a conteúdo ou produto restrito. No caso de marketplaces, por exemplo, a verificação de idade poderia ser exigida,



		prioritariamente: • no cadastro ou criação de conta; • no acesso a categorias de produtos sujeitas a restrição etária; OU • no momento de checkout ou conclusão da transação relativa a tais produtos. 2. Com validade temporal razoável, e revalidação em casos excepcionais A idade é um dado que se altera apenas uma vez por ano e sempre se atualizado de forma previsível, de modo que, sabendo-se a data de nascimento do titular, pode ser atualizada de forma automatizada. A experiência internacional em proteção de crianças no ambiente digital indica a adoção de novas verificações em marcos relevantes da idade ou em intervalos razoáveis, em vez de revalidações constantes a cada uso cotidiano da mesma conta. Assim, a verificação de idade, uma vez realizada por meio de mecanismo confiável (conforme parâmetros que venham a ser definidos pela ANPD), deveria: • manter sua eficácia para acessos subsequentes do mesmo usuário; e • ser renovada apenas: (a) de forma periódica, em intervalo compatível com a mudança efetiva do dado (por exemplo, anual ou atrelado à mudança de faixa etária), quando não verificada a data de nascimento; ou (b) em situações excepcionais, como indícios concretos de uso indevido da conta por menores, alteração relevante do contexto de risco ou mudança significativa da jornada de uso. 3. Considerando custos econômicos e viabilidade prática A exigência de verificação plena de idade em absolutamente todos os acessos técnicos implicaria: • custos operacionais e tecnológicos elevados, sobretudo quando envolvem integrações com terceiros, biometria ou outros métodos robustos; • aumento substancial de fricção na experiência do usuário, com impacto na concorrência e na inovação;



		e um volume de tratamento de dados pessoais (inclusive sensíveis, em alguns modelos) manifestamente desproporcional aos objetivos perseguidos. Em setores de uso recorrente, isso poderia inviabilizar economicamente determinadas aplicações, especialmente para pequenos e médios agentes econômicos, contrariando o equilíbrio entre proteção de crianças e adolescentes e a livre iniciativa. Assim, recomenda-se que a interpretação seja baseada em materialidade e risco, segundo a qual a exigência de verificação de idade se concentre em momentos relevantes da jornada do usuário, nos quais haja efetivo potencial de exposição a conteúdo ou produto restrito. A verificação, uma vez realizada por meio de mecanismo confiável, deve produzir efeitos para acessos subsequentes, admitindo-se sua renovação apenas em intervalos razoáveis ou em situações excepcionais, em consonância com os princípios da LGPD e com a viabilidade técnica e econômica dos serviços.
Art. 9º (...) § 1º Para dar efetividade ao disposto no caput, deverão ser adotados mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração.	"VEDADA AUTODECLARAÇÃO"	A O art. 9º, §1º da Lei dispõe que deverão ser adotados "mecanismos confiáveis de verificação de idade (...) vedada a autodeclaração". A Lei, contudo, não define "autodeclaração" em seu art. 2º, nem em qualquer outro dispositivo, o que gera incerteza quanto ao alcance da proibição. 1. Interpretação proposta: sentido estrito A finalidade da vedação, à luz do contexto protetivo do ECA Digital, é impedir mecanismos manifestamente ineficazes, em que: - o usuário informa sua idade sem qualquer respaldo, ou - a plataforma apenas pergunta a idade e confia cegamente na resposta. Assim, a proibição deve ser entendida como vedação ao ato unilateral e não validado pelo qual o usuário declara sua idade, sem elemento externo de confiabilidade. Esse entendimento está alinhado ao Radar Tecnológico nº 5 da ANPD, que destaca a baixa confiabilidade da autodeclaração e sua inadequação como mecanismo exclusivo de aferição etária.



		2. O que NÃO é autodeclaração (portanto, não deve ser vedado) É importante diferenciar a “autodeclaração pura” de procedimentos estruturados que, embora possam envolver uma etapa de interação do usuário, não são autodeclaração no sentido vedado pela lei, porque incorporam elementos de confirmação ou vinculação seguros. Exemplos que não devem ser proibidos (por não serem autodeclaração pura): • Inclusão de data de nascimento associada a método de autenticação forte (ex.: login federado, identidade verificada); • Validação de idade por meio de cadastro pré-existente em app store, operadora, instituição financeira ou serviço confiável; • Verificação documental assistida por algoritmos, com extração de metadados; • Serviços de verificação etária baseados em integrações confiáveis (identity providers). Nesses casos, a declaração não é autônoma; ela está ancorada em processo confiável. 3. Por que a interpretação restritiva é coerente com a LGPD Uma interpretação que proibisse qualquer declaração do usuário, mesmo quando acompanhada de mecanismo de validação, resultaria em: • coleta adicional desnecessária de dados biométricos, documentais ou comportamentais; • maior risco de violação de privacidade; • tratamento excessivo de dados sensíveis. Isso contraria a LGPD (art. 6º, III – necessidade). Por isso, a sugestão seria incluir dispositivo que veda a autodeclaração como ato unilateral de verificação para que a interpretação do mesmo seja a de que: • a legislação proíbe processos de verificação de idade baseados exclusivamente em autodeclaração;



		• mas não proíbe mecanismos de verificação de idade que envolvam a autodeclaração, somada a mecanismos robustos a ela complementares. Desta forma, a título meramente exemplificativo, e sem prejuízo de outras soluções tecnicamente adequadas, a validação de eventual declaração inicial do usuário pode ocorrer por meio de mecanismos complementares, tais como: (i) validação documental ou em bases de dados oficiais ou confiáveis; (ii) utilização de sinais técnicos ou estimativas etárias proporcionais ao risco; (iii) confirmação ou autorização inequívoca realizada por responsável legal devidamente identificado (verificação parental).
Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos. § 2º Para os fins desta Lei, consideram-se impróprios ou inadequados para crianças e adolescentes os produtos,	CONTEÚDO IMPRÓPRIO PARA MENORES	O artigo 9º inclui referência a conteúdo que seja “impróprio, inadequado ou proibido para menores de 18 anos”. Essa abordagem é ambígua e pode criar desafios significativos para serviços de conteúdo literário. Sem limites de definição claros, esses descritores subjetivos poderiam abranger praticamente qualquer tema adulto na literatura, incluindo obras com significado educacional, histórico ou cultural significativo. A orientação deve enfatizar que o escopo do conteúdo “impróprio, inadequado ou proibido” se aplica apenas ao conteúdo de natureza pornográfica ou explicitamente proibido pela legislação brasileira vigente para menores de idade. Além disso, no que diz respeito ao Artigo 9 §2, a orientação deve ser precisa na definição de conteúdo “pornográfico” para distinguir entre material explícito destinado principalmente à excitação sexual e obras literárias que incluem temas sexuais adultos como parte de contextos narrativos, educacionais, históricos ou culturais mais amplos. Sem esse esclarecimento, existe o risco de que obras literárias legítimas e valiosas possam ser indevidamente classificadas como materiais pornográficos. Diante disso, recomenda-se interpretação restritiva do art. 9º do ECA Digital, de modo que o conceito de conteúdo “impróprio, inadequado ou proibido” se limite àquele de natureza pornográfica ou expressamente vedado pela legislação brasileira



serviços ou conteúdos de tecnologia da informação que contenham material pornográfico, ou quaisquer outros vedados pela legislação vigente.		para menores, distinguindo-se material explicitamente voltado à excitação sexual de obras literárias com contextos educacionais, históricos ou culturais. Tal entendimento evita enquadramentos excessivos e preserva o acesso a conteúdos legítimos, sem prejuízo da proteção de crianças e adolescentes.
Art. 12. Os provedores de lojas de aplicações de internet e de sistemas operacionais de terminais deverão: III – possibilitar, por meio de Interface de Programação de Aplicações (Application Programming Interface – API) segura e pautada pela proteção da privacidade desde o padrão, o fornecimento de sinal de idade aos provedores de aplicações de internet, exclusivamente para o cumprimento das finalidades desta Lei e com salvaguardas técnicas adequadas.	"SINAL DE IDADE"	O "sinal de idade" é um atributo derivado de processo prévio de aferição, realizado pelo provedor de loja de aplicativos ou do sistema operacional. Trata-se de um marcador mínimo de idade, cujo propósito é informar o provedor da aplicação acerca da adequação do usuário a determinadas funcionalidades, conteúdos ou produtos. 1. Informações mínimas que o sinal de idade deve conter A interpretação coerente com os princípios da LGPD (necessidade, minimização e limitação da finalidade) e com o § 1º do art. 12 leva à conclusão de que o "sinal de idade" deve conter apenas aquilo que permita ao provedor de aplicação: (i) associar o sinal a um usuário específico na sua plataforma, e (ii) assumir a postura regulatória adequada, nos termos do ECA Digital. Para que tal associação seja possível – e sem fornecer dados excessivos – o sinal de idade deve incluir: (i) a informação etária em si, representada de forma estruturada, por exemplo: data de nascimento (preferível quando necessária para limites etários objetivos), ou faixa etária (ex.: "< 13", "13 a 17", "≥ 18"), quando tecnicamente suficiente. (ii) Um identificador mínimo e pseudonimizado, para permitir a vinculação ao usuário da aplicação, como por exemplo: • um token persistente; • device ID pseudonimizado;



		• identificador criptografado. 2. Necessidade de padronização e interoperabilidade A ausência de especificação técnica pode gerar riscos concretos: • inconsistência entre sinais de diferentes plataformas; • interpretação divergente do conteúdo do sinal; • assimetria competitiva caso determinados provedores priorizem clientes “mais relevantes”; • tratamento excessivo ou insuficiente dependendo do formato adotado. Por isso, a ANPD deveria: • definir formato mínimo interoperável do sinal de idade; • padronizar o conteúdo obrigatório (por exemplo, faixa etária + identificador pseudonimizado); • permitir graus opcionais, se necessários em determinados contextos de risco (ex.: produtos regulados). Desta forma, recomenda-se que as orientações regulatórias esclareçam o conteúdo mínimo e o formato interoperável do “sinal de idade”, limitado à informação etária necessária e a identificador pseudonimizado, em observância aos princípios da LGPD. Tal definição promove uniformidade regulatória, evita tratamento excessivo de dados e assegura o uso proporcional do sinal de idade para a proteção de crianças e adolescentes.



Art. 13. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito.	“VEDADO SEU TRATAMENTO PARA QUALQUER OUTRO PROPÓSITO”	É importante que seja oferecida interpretação restritiva ao art. 13 do ECA Digital, de modo que ele se limite à reutilização de dados pessoais, quando coletados específica e exclusivamente para fins de verificação de idade. Em seus processos de negócio, em especial aqueles voltados à prevenção de fraudes e a realização de cadastros, as organizações tendem a coletar dados pessoais que podem ser úteis para procedimentos de verificação de idade, tais como informações biométricas, documentos de identificação, datas de nascimento, CPF, telefone e demais dados correlatos. Para evitar a coleta duplicada desses elementos, o que violaria o princípio da necessidade (art. 6º, III, da LGPD) e poderia gerar riscos adicionais desnecessários aos titulares, é recomendável que a interpretação a ser dada ao referido artigo não inviabilize o reaproveitamento nos processos de verificação de idade de dados previamente tratados para outras finalidades legítimas. Para tanto, a ANPD deve disponibilizar meios razoáveis e dotados de segurança jurídica para que as organizações possam demonstrar que referidos dados, embora utilizados para fins de validação de idade, não foram coletados para esse fim – de modo que a sua utilização nos processos ordinários de negócio não configuram violação ao disposto no art. 13. Nesse sentido, sugere-se que a ANPD esclareça o alcance do art. 13 do ECA Digital, inclusive mediante a previsão de parágrafo único interpretativo, a fim de explicitar que a vedação ao tratamento para outras finalidades não obsta a utilização, nos procedimentos de verificação de idade, de dados pessoais previamente coletados para finalidades legítimas e compatíveis, desde que observados os princípios da LGPD. Tal esclarecimento contribui para evitar a coleta duplicada de dados, reduzir riscos à privacidade e conferir maior segurança jurídica aos agentes regulados.



Art. 15. O cumprimento das obrigações previstas neste Capítulo não exime os demais agentes da cadeia digital das suas responsabilidades legais, cabendo a todos os envolvidos garantir de forma solidária a proteção integral de crianças e de adolescentes.	RESPONSABILIDADE DE CADA AGENTE NA CADEIA DIGITAL	Esclarecer os limites de responsabilidade de cada agente na cadeia digital. A lei aplica-se de forma ampla aos “sistemas operacionais” e impõe obrigações específicas ao serviço (por exemplo, Art. 12) e obrigações gerais ao provedor de conteúdo a esses serviços, sem distinguir adequadamente entre as diferentes funções que esses serviços desempenham na pilha tecnológica. Os sistemas operacionais fornecem infraestrutura técnica para facilitar o acesso à internet — eles não fornecem conteúdo diretamente nem têm visibilidade ou controle sobre o conteúdo que os usuários podem acessar em seus serviços. Eles também não podem realizar moderação de conteúdo para o conteúdo de outro serviço. Assim, as obrigações dirigidas aos provedores de conteúdo não são tecnicamente viáveis nem razoavelmente praticáveis para serviços que operam no nível da infraestrutura do dispositivo. Recomendamos que sejam introduzidas orientações adicionais para estabelecer limites definidores claros e obrigações proporcionais entre os provedores de conteúdo (ou seja, serviços que hospedam, selecionam ou disponibilizam conteúdo diretamente aos usuários finais) e intermediários técnicos, como sistemas operacionais, que facilitam o acesso geral à Internet sem controle ou visibilidade específicos do conteúdo. Recomenda-se, portanto, a inclusão de orientações adicionais assegurando que a solidariedade prevista no art. 15 se restrinja às obrigações do Capítulo IV relativas aos mecanismos de aferição de idade, evitando interpretações que ampliem indevidamente o escopo de deveres para atores que não controlam conteúdo. No direito brasileiro, é pacífico que regimes de responsabilidade solidária podem coexistir com excludentes legais específicas, como: • inexistência de defeito no produto ou serviço; • culpa exclusiva do consumidor; • culpa exclusiva de terceiro; • inexistência de ato ou tratamento.



		Tais excludentes: • integram o Código de Defesa do Consumidor (arts. 12, §3º e 14, §3º), • integram a LGPD (art. 43), • e não foram afastadas expressamente pelo ECA Digital. Portanto, a interpretação sistemática exige que o art. 15 seja compreendido como cláusula de cooperação solidária, e não como cláusula absoluta de responsabilidade objetiva universal. O ecossistema digital envolve agentes distintos, com deveres e riscos distintos. Provedores de aplicação, lojas de aplicativos, sistemas operacionais, provedores de identidade e prestadores de serviço de aferição desempenham: • funções diferentes, • com graus de controle distintos, • e obrigação legal diversa. A interpretação do art. 15 não pode ignorar essa assimetria técnica – sobretudo porque o próprio texto da Lei reconhece que cada agente possui obrigações específicas (e.g., art. 12 – obrigação exclusiva das lojas de apps e sistemas operacionais). Aplicação das excludentes do CDC Nas relações envolvendo oferta de produtos e serviços digitais a usuários finais, incidem as excludentes de responsabilidade previstas nos arts. 12, §3º e 14, §3º do CDC. Em especial: • Culpa exclusiva do consumidor ou de terceiro (arts. 12, §3º, III e 14, §3º, II); • Inexistência de defeito no produto/serviço (arts. 12, §3º, II e 14, §3º, I). Essas excludentes: • evitam responsabilização automática; • preservam a proporcionalidade e o equilíbrio da cadeia digital;



		• evitam responsabilização objetiva indevida. Aplicação das excludentes da LGPD (art. 43) Quando o tratamento envolver dados pessoais – o que ocorrerá em parte significativa dos casos regulados pela Lei – incidem também as excludentes previstas no art. 43 da LGPD, notadamente: • ausência de tratamento (art. 43, I); • realização de tratamento por terceiro (art. 43, III); • responsabilidade exclusiva de outro agente (art. 43, III). Assim, não é juridicamente sustentável impor responsabilidade solidária a agentes que não realizaram o tratamento ou que o realizaram com diligência e conformidade. Recomenda-se interpretação do art. 15 do ECA Digital que reconheça as diferenças funcionais e o grau de controle de cada agente da cadeia digital, compreendendo a responsabilidade solidária como mecanismo de cooperação proporcional e não como responsabilização objetiva universal. Tal leitura, em consonância com o CDC e a LGPD, preserva as excludentes legais, evita a imposição de deveres inexecutáveis a intermediários técnicos e reforça a segurança jurídica e o equilíbrio regulatório.
Art. 16. (...) Parágrafo único. Na hipótese de tratamento de dados de crianças e de adolescentes, sobretudo quando realizado para fins que não os estritamente necessários para a operação do produto ou serviço, o controlador a que se refere o inciso VI do art. 5º da	“RELATÓRIO DE IMPACTO, DE MONITORAMENTO E DE AVALIAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS”	O legislador introduziu no ECA Digital a nova expressão “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”, sem trazer o conceito do que se deve entender sobre esse documento. A Lei Geral de Proteção de Dados, baseada na regulação europeia, já introduziu ao ordenamento jurídico nacional o Relatório de Impacto à Proteção de Dados (“RIPD”), documentação apropriada e suficiente para a demonstração e gestão de riscos à privacidade nas atividades de tratamento que possam afetar direitos e liberdades fundamentais dos titulares. Assim, não obstante a imprecisão redacional do ECA Digital, a melhor interpretação



Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverá: (...) II – elaborar relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais, a ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital, na forma de regulamento.á:		ao texto é considerar que o “<i>relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais</i>” diz respeito ao próprio RIPD previsto na LGPD, e não a um novo documento. A adoção de entendimento diverso levaria a alocação ineficiente de recursos, já que a elaboração de RIPD exige alta complexidade técnica e significativo emprego de tempo das áreas de negócio, equipes técnicas e especialistas em privacidade. Produzir relatório adicional duplicará esse consumo de recursos escassos, afastando-os de atividades relevantes à proteção de crianças e adolescentes, como a correção de vulnerabilidades e a implementação dos controles apontados no próprio RIPD. Em essência, recursos que poderiam mitigar riscos aos titulares seriam desviados para criar novo documento provavelmente redundante e sem benefício efetivo, atendendo apenas a formalidade regulatória. Diante disso, recomenda-se interpretação segundo a qual a expressão “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais” se refere ao Relatório de Impacto à Proteção de Dados previsto na LGPD. Tal entendimento evita a duplicação de obrigações documentais, assegura o uso eficiente de recursos e direciona os esforços regulatórios para medidas efetivas de proteção dos direitos de crianças e adolescentes.
Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão: (...) IV – oferecer funcionalidades que permitam limitar e monitorar o tempo de uso	LIMITAR E MONITORAR O TEMPO DE USO	Esclarecer os parâmetros do que se espera com a oferta de funcionalidades que permitam limitar e monitorar o tempo de uso dos produtos ou serviços, além da compatibilização de interesses de agentes privados. A sugestão é que a limitação não incorra em incapacidade técnica de realização do serviço contratado para resolver uma necessidade logística, por exemplo. Nesse caso, a limitação é incompatível com a natureza utilitária do serviço e compromete a funcionalidade essencial da aplicação. Nesse contexto, recomenda-se que a ANPD esclareça, em sede interpretativa, que a obrigação de ofertar funcionalidades de limitação e monitoramento do tempo de uso deve ser aplicada de forma proporcional à natureza e à finalidade do serviço, não



do produto ou serviço.		alcançando aplicações cuja funcionalidade principal seja a contratação ou operacionalização de serviços a serem prestados no mundo físico, aquelas de natureza estritamente transacional ou de mobilidade, bem como aplicações voltadas à segurança pessoal ou familiar do titular . Nessas hipóteses, a imposição de limites artificiais de tempo de uso mostra-se incompatível com a função essencial da aplicação e pode comprometer a adequada prestação do serviço, sem ganho efetivo à proteção de crianças e adolescentes.
Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão: (...) § 4º As configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo: (...) V – controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação	"DE ACESSO PROVÁVEL" E "SISTEMAS RECOMENDAÇÃO PERSONALIZADOS " DE	No que concerne à aplicabilidade do artigo aos serviços "de acesso provável por crianças e adolescentes", são aplicáveis as considerações pontuadas com relação ao Artigo 1. A lei exige que os serviços ofereçam controles para "sistemas de recomendação personalizados", presumindo que tais sistemas de recomendação sejam inerentemente arriscados para menores. No entanto, os sistemas de recomendação personalizados servem a diferentes propósitos em diferentes tipos de serviços e não devem ser caracterizados como uniformemente arriscados. O contexto e a finalidade de um sistema de recomendação afetam significativamente seu perfil de risco. Por exemplo, um sistema de recomendação personalizado que ajuda os clientes a navegar com eficiência por vastos catálogos de conteúdo e encontrar conteúdo adequado à idade tem uma finalidade fundamentalmente diferente daquele projetado para maximizar o envolvimento contínuo do usuário. No primeiro caso, o sistema realmente melhora a experiência do usuário, reduzindo o tempo de pesquisa, em vez de tentar manter os usuários no serviço por mais tempo. É uma parte inerente do serviço e não algo que pode ser ativado ou desativado. Recomendamos que as orientações regulatórias distingam entre diferentes tipos de sistemas de recomendação personalizados com base em sua finalidade e risco potencial para menores. Os sistemas projetados principalmente para aumentar o tempo de engajamento do usuário ou amplificar a viralidade do conteúdo devem estar



		sujeitos a controles mais rígidos. No entanto, os sistemas que simplesmente ajudam os usuários a navegar por catálogos de conteúdo ou encontrar materiais adequados à idade devem ser reconhecidos como recursos benéficos que melhoram a experiência e protegem o usuário, em vez de comprometer. O racional deve focar na diferença entre recomendação de conteúdo e sugestão de interface e logística com resultados em utilidade e/ou segurança. Se a lei obrigar a desligar sistemas de recomendação em transporte individual de passageiros, por exemplo, o app pode perder a capacidade de sugerir destinos rápidos (ex: "Casa" ou "Escola") ou rotas otimizadas, piorando a experiência e até a segurança (ao obrigar a digitação manual de endereços). A orientação deve se concentrar em práticas prejudiciais específicas no design do sistema de recomendação — como recursos que promovem tempo excessivo de tela ou conteúdo potencialmente prejudicial — em vez de tratar todos os recursos de personalização como inerentemente problemáticos. Essa abordagem diferenciada alinharia melhor os requisitos regulatórios com os riscos reais, preservando os recursos de recomendação benéficos que ajudam os usuários a acessar conteúdo apropriado com eficiência. Diante disso, recomenda-se que as orientações regulatórias esclareçam que não se enquadram no conceito de sistemas de recomendação personalizados sujeitos a restrições aquelas funcionalidades de caráter estritamente operacional, logístico ou de segurança, indispensáveis à adequada prestação do serviço. Incluem-se nesse escopo, exemplificativamente, funcionalidades necessárias à viabilização de serviços de transporte, mobilidade urbana ou entregas, à facilitação da interface do usuário com vistas à redução de fricção ou erro na contratação, bem como à proteção da integridade física do titular, como a sugestão de rotas seguras ou de destinos frequentemente utilizados.



Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão: (...) § 4º As configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível, assegurados, no mínimo: (...) VIII – revisão regular das ferramentas de inteligência artificial, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas;	“ DE ACESSO PROVÁVEL” E “INTELIGÊNCIA ARTIFICIAL”	No que concerne à aplicabilidade do artigo aos serviços “de acesso provável por crianças e adolescentes”, são aplicáveis as considerações pontuadas com relação ao Artigo 1. Temos preocupações quanto à inclusão de requisitos específicos de inteligência artificial nesta lei, pois essa abordagem interpreta erroneamente tanto a natureza onipresente da tecnologia de IA quanto suas diversas aplicações na segurança online. A IA não é inerentemente prejudicial; é uma tecnologia usada para muitos fins legítimos, incluindo a moderação eficaz de conteúdo em grande escala. As ferramentas de IA podem ser usadas para identificar e remover conteúdo prejudicial de forma rápida e consistente em grandes volumes de interações de usuários. Muitos recursos de segurança que protegem as crianças online, desde a filtragem de conteúdo até a detecção de possíveis comportamentos predatórios, dependem da tecnologia de IA. Além disso, adicionar requisitos específicos de IA não melhora significativamente os objetivos de proteção da lei. Conteúdos inadequados para crianças se enquadram no âmbito das medidas de segurança exigidas, independentemente de serem gerados por IA ou criados por humanos. O método de criação de conteúdo não altera a forma como um serviço deve ser moderado e regulamentado. Além disso, exigir uma revisão externa dos sistemas de IA pode comprometer a segurança, expondo informações confidenciais sobre os sistemas de moderação de conteúdo a terceiros. Recomendamos que as orientações regulatórias se concentrem em práticas ou resultados prejudiciais específicos que a lei busca prevenir, em vez de regulamentar a tecnologia de IA como um todo. As orientações devem reconhecer explicitamente que as ferramentas de IA podem aumentar a segurança online quando implementadas adequadamente e que os serviços devem ter flexibilidade para desenvolver e revisar sistemas de IA internamente, desde que incorporem princípios adequados de segurança desde a concepção. Essa abordagem atenderia melhor aos objetivos de proteção da lei, evitando consequências indesejadas para aplicações benéficas de IA que ajudam a manter as crianças seguras online.



		Nesse sentido, recomenda-se que as orientações regulatórias esclareçam que a possibilidade de desabilitação de funcionalidades não deve alcançar sistemas de inteligência artificial ou mecanismos automatizados que sejam essenciais à segurança e à proteção dos usuários, especialmente quando desempenhem funções de moderação de conteúdo nocivo, monitoramento de segurança física ou operacional (safety), bem como proteção contra acessos não autorizados e garantia da segurança da informação. Tais sistemas constituem instrumentos fundamentais para a prevenção de riscos e a efetividade da proteção de crianças e adolescentes no ambiente digital, de modo que sua desativação compulsória poderia, paradoxalmente, fragilizar os níveis de segurança que a própria norma busca assegurar.
Art. 22. Para além das demais disposições desta Lei, é vedada a utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e a adolescentes, bem como o emprego de análise emocional, de realidade aumentada, de realidade estendida e de realidade virtual para esse fim.	“ TÉCNICAS DE PERFILAMENTO PARA DIRECIONAMENTO DE PUBLICIDADE COMERCIAL ” E “DIRECIONAMENTO DE PUBLICIDADE COMERCIAL A CRIANÇAS E A ADOLESCENTES ”	O artigo 22 da lei proíbe a criação de “perfis comportamentais” de menores para fins de publicidade comercial; no entanto, ao fazer isso, ela não define o que constitui “publicidade comercial”. Existem várias formas de “publicidade comercial”, como anúncios baseados em interesses, anúncios comportamentais contextuais cruzados, marketing e até mesmo publicidade contextual e educativa. Sem definições mais claras sobre o significado de “publicidade comercial”, os serviços enfrentam incertezas sobre como adaptar adequadamente seus sistemas de publicidade. Recomendamos orientações mais claras que estabeleçam que “publicidade comercial” inclui anúncios baseados em interesses e publicidade comportamental contextual cruzada, mas não inclui publicidade contextual ou educacional. Além disso, essa orientação deve esclarecer que “publicidade comercial” não inclui recomendações de conteúdo sobre itens como histórico de visualizações ou interações com um produto ou serviço. Além disso, recomendamos uma orientação que estabeleça que as empresas relevantes podem continuar a exibir “publicidade comercial” de qualquer forma em suas plataformas, a menos que tenham um sinal claro de que o usuário é menor de idade.



		Além disso, é importante distinguir a proibição da “publicidade comercial” do Artigo 22 das ferramentas do Artigo 17 para permitir o controle sobre “recomendações personalizadas”. É necessário definir o que constitui “recomendações personalizadas” — que são claramente permitidas com controles limitantes — em oposição à “publicidade comercial” — que é claramente proibida. Caso contrário, não seria possível que o Artigo 22 e o Artigo 17 coexistissem na lei. Recomendamos deixar claro que “publicidade comercial” não inclui recomendações de produtos em lojas virtuais e formas semelhantes de priorização de produtos em sites de varejo comercial. Em um aplicativo de mobilidade ou marketplace, a recomendação de um serviço específico (ex: uma categoria de veículo mais confortável ou uma rota promocional) não constitui publicidade no sentido estrito, mas sim a apresentação do catálogo de serviços. Interpretar essas funcionalidades como 'publicidade comercial' prejudicaria a navegabilidade e a capacidade do usuário de encontrar o serviço que melhor atende à sua necessidade imediata. Ademais, cabe salientar que o enfoque da regulação é a proteção de menores de idade a conteúdos impróprios que possam causar danos significativos ao seu desenvolvimento e vivência. Conforme os exemplos já pontuamos acima, o uso de publicidade comercial também viabiliza o acesso deste público a conteúdo adequado à sua faixa etária, conciliando a proteção de crianças e adolescentes com o desenvolvimento econômico e a livre iniciativa. Uma vez que o uso de publicidade comercial se dá em variados locais e formatos, a verificação etária anterior à exposição torna-se inviável. Dessa forma, entende-se que o escopo da vedação deveria ser justamente a publicidade direcionada e relacionada a produtos e serviços impróprios, mediante um sinal claro de que o usuário é menor de idade. Pedido de esclarecimento recomendado, a ANPD deve especificar: • Distinção clara entre publicidade direcionada proibida e curadoria/recomendações de conteúdo permitidas, inclusive mecanismos de exibição e organização de ofertas (merchandising digital) essenciais para o



		funcionamento de plataformas transacionais. • Se a publicidade contextual (baseada no conteúdo que está sendo visualizado, não no perfil do usuário) é permitida • Padrões e necessidade de verificação de idade exigidos antes de veicular qualquer conteúdo comercial • Período de carência para implementar a filtragem de anúncios em perfis infantis existentes Nesse contexto, recomenda-se que as orientações regulatórias esclareçam que não se enquadram no conceito de publicidade comercial, para os fins do art. 22 do ECA Digital, as práticas estritamente vinculadas à apresentação e organização do próprio catálogo de produtos ou serviços disponibilizados na plataforma. Incluem-se nesse escopo, de forma exemplificativa, a exibição, organização, priorização ou recomendação de produtos e serviços passíveis de contratação ou aquisição direta no ambiente digital (vitrine virtual), bem como as sugestões de funcionalidades, modalidades ou opções de serviço inerentes ao portfólio do próprio controlador ou de seus parceiros comerciais diretos em contextos transacionais. Tal esclarecimento é essencial para diferenciar publicidade direcionada baseada em perfil — objeto legítimo da vedação legal — de mecanismos operacionais de curadoria e navegação, indispensáveis ao funcionamento eficiente e seguro das plataformas digitais.
O ECA Digital emprega os conceitos de “ verificação de idade ” e “ aferição de idade ” de forma reiterada, mas sem definição explícita. Considerando a relevância desses termos para a operacionalização da Lei, solicita-se que a ANPD esclareça seu sentido e	“VERIFICAÇÃO DE IDADE” “AFERIÇÃO DE IDADE”	À luz do Radar Tecnológico nº 5 – Mecanismos de Aferição de Idade em Ambientes Digitais (“Radar”), publicado pela ANPD, entende-se que: 1. Aferição de idade (conceito gênero) O Radar trata a aferição como o processo primário pelo qual a idade do usuário é determinada ou confirmada mediante mecanismos tecnicamente seguros, auditáveis e proporcionais. Diversas tecnologias podem compor essa etapa – como validação documental, integração com fontes confiáveis, biometria ou métodos criptográficos – todas abrangidas pelo conceito gênero “aferição de idade”. 2. Verificação de idade (espécie da aferição) A “verificação” é etapa que se insere dentro do gênero aferição, mas destinada à



extensão.		confirmação da idade para determinado acesso, etapa, funcionalidade ou contexto. A verificação: • é confirmatória e contextual; • pode ocorrer com menor invasividade do que a aferição inicial; • pode recair sobre dados previamente aferidos; • sem excluir a possibilidade de coleta limitada adicional, desde que: 1. o proporcional à finalidade; 2. o estritamente necessária; 3. o em conformidade com a minimização de dados prevista na LGPD. Essa interpretação está em linha com o Radar, que destaca a existência de diferentes níveis de robustez e intrusividade técnica ao longo do ciclo de aferição etária. Assim, a distinção conceitual não é abstrata, ela serve justamente para calibrar as obrigações, evitando que todos os agentes econômicos tenham que implementar mecanismos complexos idênticos em todos os contextos, o que seria contrário a lógica de regulações e sistemas de governança baseados em riscos que regem o universo digital. Diante disso, recomenda-se que as obrigações relacionadas à idade do usuário observem a distinção entre aferição e verificação de idade, conforme o Radar Tecnológico nº 5 da ANPD, permitindo a calibração das exigências segundo o contexto e o risco. Tal abordagem viabiliza o uso proporcional de mecanismos menos invasivos, o reaproveitamento de dados previamente aferidos e a conformidade com a LGPD, evitando a imposição uniforme de soluções complexas.

A partir da análise sistemática dos dispositivos do ECA Digital, o quadro apresentado demonstra que diversos conceitos centrais da Lei nº 15.211/2025 – tais como “de acesso provável”, “suficiente probabilidade de uso e atratividade”,



AMOBITEC

Associação Brasileira de Mobilidade e Tecnologia

“considerável facilidade de acesso e utilização”, “significativo grau de risco”, “grau mais elevado de proteção da privacidade e dos dados pessoais”, “informações claras, acessíveis e adequadas”, “a cada acesso”, “vedada a autodeclaração”, “conteúdo impróprio, inadequado ou proibido”, “sinal de idade”, “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”, bem como as noções de responsabilidade solidária e de sistemas de recomendação personalizados, inteligência artificial e publicidade comercial – carecem de maior densificação normativa e interpretativa para viabilizar sua aplicação coerente, proporcional e tecnicamente exequível.

As respostas ao questionário da Tomada de Subsídios buscam justamente suprir essa lacuna, ao identificar, para cada expressão, parâmetros objetivos de interpretação (finalidade do serviço, natureza do conteúdo, funcionalidades, público-alvo, perfil de risco, contexto de uso, tipo de dado tratado, modelo de negócio, presença de barreiras de acesso, critérios de aferição e verificação de idade, entre outros), em alinhamento com a LGPD, o CDC, o princípio da proteção integral e as melhores práticas internacionais de regulação baseada em risco. Essa abordagem evita que a mera possibilidade técnica de acesso por crianças e adolescentes converta todos os produtos e serviços digitais em “serviços de risco”, ao mesmo tempo em que preserva um alto nível de tutela para situações em que haja, de fato, exposição relevante a danos.

Em síntese, as contribuições apresentadas respondem às duas questões norteadoras da Tomada de Subsídios: (i) ao mapear, de forma minuciosa, os conceitos, termos e expressões do ECA Digital que demandam esclarecimentos adicionais; e (ii) ao propor critérios e balizas interpretativas concretas para torná-los mais precisos, proporcionais e operacionalizáveis. Com isso, pretende-se colaborar para que a regulamentação a ser editada pela autoridade competente promova, simultaneamente, a proteção efetiva de crianças e adolescentes em ambientes digitais, a segurança jurídica dos agentes



AMOBITEC

Associação Brasileira de Mobilidade e Tecnologia

envolvidos na cadeia digital e a preservação da inovação e da livre iniciativa em um ecossistema regulatório racional e equilibrado.

III. CONSIDERAÇÕES FINAIS

Ante o exposto, as contribuições apresentadas refletem o compromisso do setor em colaborar para uma regulamentação equilibrada, capaz de proteger crianças e adolescentes sem comprometer a privacidade, a inovação e o acesso digital da população.

Reafirmamos nosso compromisso em contribuir continuamente para o aprimoramento do marco regulatório. Agradecemos a atenção dispensada e permanecemos à disposição para aprofundar o diálogo e avançar, de forma conjunta, na construção de políticas públicas sólidas e sustentáveis. Renovamos, por fim, nossos votos de estima e consideração.

André Alencar Porto | Diretor Executivo – AMOBITEC

diretoriaexecutiva@amobitec.org | 

Contribuição da Associação Latino-Americana de Internet (ALAI) – Tomada de Subsídios conceitos previstos no ECA Digital (ANPD)

1. Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos? Justifique sua resposta separadamente para cada conceito, termo ou expressão indicado. (2000 caracteres)

A Associação Latino-Americana de Internet (ALAI) considera que as diretrizes gerais do ECA Digital são pertinentes diante do atual contexto, marcado por rápidas transformações tecnológicas, pela ampliação do acesso digital por grupos vulneráveis e pelos riscos inerentes às fases específicas de desenvolvimento de crianças e adolescentes. Reconhecemos como legítimo o propósito de garantir a proteção integral e prevenir danos.

Por essa razão, ressaltamos a necessidade de esclarecimentos técnicos e normativos que permitam a plena efetividade do objetivo protetivo da lei. Essa necessidade se evidencia diante da persistência de conceitos indefinidos, de obrigações que demandam elevado esforço interpretativo e de situações que requerem regulamentação complementar para assegurar a correta aplicação da norma, bem como segurança jurídica e proporcionalidade regulatória.

Torna-se, portanto, imprescindível que a regulamentação posterior estabeleça critérios técnicos e objetivos para suprir as definições em aberto, levando em consideração as particularidades de cada setor e os diferentes níveis de risco associados a cada modelo de serviço. Esse é um requisito fundamental para garantir que a implementação do ECA Digital seja efetiva, proporcional, alinhada aos princípios da proteção integral e harmonizada com o ordenamento jurídico brasileiro e com os atos normativos da Agência Nacional de Proteção de Dados (ANPD). Ressaltamos, ainda, a importância de evitar a imposição de obrigações uniformes a serviços que apresentam características e graus de risco substancialmente distintos.

Por fim, em razão da limitação de caracteres deste formulário, apresentamos em anexo as necessidades específicas de esclarecimento sobre conceitos, termos e expressões do texto legislativo, objeto desta Tomada de Subsídios. A ALAI permanece à disposição para contribuir com o avanço do escopo regulatório aplicável ao ambiente digital.

2. Anexo.

Referência	Texto	Comentário/Recomendação

Art. 1º	Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.	Consideramos que o ECA Digital adota uma aplicação abrangente a qualquer serviço considerado “de acesso provável por crianças e adolescentes”, mas sem levar em conta que distintos serviços apresentam níveis de risco muito diferentes para esse público. Essa formulação resulta em um tratamento uniforme que impõe as mesmas obrigações a serviços com perfis de risco completamente distintos. Por exemplo, plataformas educacionais voltadas ao público infantil, com conteúdo curado e sem interação entre usuários, e sistemas operacionais de dispositivos domésticos inteligentes acabam sujeitos às mesmas exigências que redes sociais onde crianças podem ter contato com conteúdo prejudicial ou interações inadequadas. Um caminho mais adequado seria adotar um modelo semelhante ao previsto no Artigo 28 da Lei de Serviços Digitais (DSA) da União Europeia, que estabelece uma abordagem efetivamente baseada em risco. Esse modelo exige que os serviços analisem não apenas a possibilidade de serem acessados por menores, mas também o seu risco global, considerando finalidade, características, funcionalidades e medidas de segurança existentes. Sugerimos que sejam emitidas orientações regulamentares que esclareçam que somente serviços que representem risco significativo de danos a menores devem ser incluídos no escopo. Para avaliar se um serviço apresenta tal risco, devem ser observados fatores como: 1. a finalidade principal do serviço; 2. a natureza e o tipo de conteúdo disponibilizado; 3. as características e funcionalidades da plataforma, incluindo: (i) ferramentas de comunicação direta entre usuários; (ii) mecanismos de interação social; (iii) recursos que permitam amplo compartilhamento de conteúdo gerado por usuários; 4. o público-alvo pretendido; 5. a presença expressiva de usuários menores; 6. estratégias de marketing ou direcionamento específico ao público infantil; 7. barreiras de acesso voltadas a impedir que crianças acessem conteúdo potencialmente nocivo; e 8. o fato de o serviço ser utilizado, com frequência, em dispositivos compartilhados.

I	suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes;	Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o significado de "suficiente probabilidade de uso e atratividade".
II	considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes; e	Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o significado de "facilidade de acesso e utilização", levando em consideração ferramentas disponíveis por padrão e/ou de controle parental para restrição ao acesso por crianças e adolescentes.
III	significativo grau de risco à privacidade , à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital.	Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o significado de "significativo grau de risco à privacidade", especialmente levando em conta a Resolução 15 da ANPD que tratou de risco e dano como a mesma coisa. Também, recomendamos esclarecer, com critérios técnicos e objetivos, o significado de "permitir interação social" e "compartilhamento de informações em larga escala".
Art. 2º	Para os fins desta Lei, considera-se:	Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o que não é considerado perfilamento [ex. classificação indicativa].

V	perfilamento: qualquer forma de tratamento de dados pessoais, automatizada ou não, para avaliar certos aspectos de uma pessoa natural, com o objetivo de classificá-la em grupo ou perfil de modo a fazer inferências sobre seu comportamento, situação econômica, saúde, preferências pessoais, interesses, desejos de consumo, localização geográfica, deslocamentos, posições políticas ou outras características assemelhadas;	
Art. 4º	A utilização de produtos ou serviços de tecnologia da informação por crianças e adolescentes tem como fundamentos:	Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o significado de "exploração comercial".
VI	a proteção contra a exploração comercial;	

Art. 5º	Os produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão observar os deveres de prevenção, de proteção, de informação e de segurança previstos neste Capítulo e nas Leis nºs 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), em conformidade com o princípio do melhor interesse da criança e do adolescente e da sua proteção integral, especial e prioritária.	
§ 1º	Os fornecedores dos produtos ou serviços de tecnologia da informação de que trata o caput deste artigo deverão adotar as medidas técnicas adequadas , inclusive mecanismos de segurança amplamente reconhecidos , que possibilitem à família e aos responsáveis legais prevenir o acesso e o uso	Recomendamos que seja considerada a diferenciação por risco e segmento de empresas para adoção de medidas técnicas mínimas exigidas. Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o significado, ou trazer parâmetros do que é “amplamente reconhecido”. Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o nível de controle parental exigido. Recomendamos que seja esclarecido, com critérios técnicos e objetivos, o significado de “uso inadequado”

	inadequado por crianças e adolescentes.	
Art. 6º	Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão tomar medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo de prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com os seguintes conteúdos , produtos ou práticas:	Consideramos que o artigo 6º abrange um conjunto excessivamente amplo de tipos de conteúdo, sem apresentar as qualificações necessárias. Isso faz com que materiais legítimos possam ser indevidamente incluídos. Por exemplo, reportagens jornalísticas podem abordar casos de abuso sexual com finalidade informativa e de interesse público; filmes de ação apropriados para menores podem conter representações de violência; e conteúdos educacionais podem mencionar temas como uso de substâncias ou automutilação em contextos preventivos e pedagógicos. Sugerimos a criação de orientações que incluam isenções explícitas para conteúdos legítimos, tais como matérias jornalísticas, obras literárias e artísticas, conteúdos educacionais e científicos, bem como materiais cujo contexto revele um uso apropriado. Além disso, várias categorias previstas necessitam de definições mais específicas para que possam ser aplicadas de forma prática. Referências a violência física, automutilação, suicídio ou uso de substâncias, por exemplo, deveriam ser qualificadas para abranger apenas conteúdos que “promovam, instruem ou incitem” tais comportamentos, e não qualquer menção a eles. Da mesma forma, expressões genéricas como “outras práticas conhecidas por causar danos financeiros a crianças e adolescentes” devem ser delimitadas para focar em situações concretas, como jogos de azar.
III	indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e	Essas classificações são fundamentais para garantir uma moderação de conteúdo que seja consistente, objetiva e efetiva. Recomenda-se ainda a adoção de critérios diferenciados por risco e segmento empresarial, de modo a assegurar que as obrigações impostas sejam razoáveis e proporcionais.

	automedicação, automutilação e suicídio;	
IV	promoção e comercialização de jogos de azar, apostas de quota fixa, loterias, produtos de tabaco, bebidas alcoólicas, narcóticos ou produtos de comercialização proibida a crianças e a adolescentes;	
V	práticas publicitárias predatórias, injustas ou enganosas ou outras práticas conhecidas por acarretarem danos financeiros a crianças e a adolescentes; e	
VI	conteúdo pornográfico.	

§ 2º	Entre as medidas de prevenção previstas no caput deste artigo, incluem-se políticas claras, eficazes e adequadas à legislação brasileira de prevenção à intimidação sistemática virtual e a outras formas de assédio na internet, com mecanismos de apoio adequado às vítimas, bem como o desenvolvimento e a disponibilização de programas educativos de conscientização direcionados a crianças, adolescentes, pais, educadores, funcionários e equipes de suporte sobre os riscos e as formas de prevenção e de enfrentamento dessas práticas, nos termos de regulamento.	Recomendamos que seja estabelecida a diferenciação por risco e segmento de empresas para aplicação de medidas previstas no artigo, objetivando entender se a aplicação de todos os requisitos é obrigatória a todo e qualquer modelo de negócio.
Art. 7º	Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo mais	Recomendamos que sejam estabelecidos critérios objetivos que esclareçam o significado de “modelo mais protetivo disponível”, considerando que tal padrão pode evoluir rapidamente em função das inovações tecnológicas. Além disso, recomenda-se a adoção de critérios de proporcionalidade baseados no nível de risco e no tipo de serviço, garantindo que as obrigações impostas sejam adequadas ao contexto e à natureza de cada atividade.

	protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerados a autonomia e o desenvolvimento progressivo do indivíduo e justificado o melhor interesse da criança e do adolescente.	
§ 1º	O produto ou serviço referido no caput deste artigo deverá, por padrão, operar com o grau mais elevado de proteção da privacidade e dos dados pessoais, observado que será obrigatória a disponibilização de informações claras, acessíveis e adequadas para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à eventual adoção de configurações menos protetivas.	Consideramos que o Artigo 7º e dispositivos correlatos determinam que as empresas devem disponibilizar informações de forma clara, acessível e adequada, para permitir que crianças, adolescentes e seus responsáveis tomem decisões informadas. Contudo, a legislação não define o que exatamente se enquadra como informação “clara, acessível e adequada”, o que gera incertezas significativas sobre como as empresas devem estruturar suas mensagens e materiais informativos. Sugerimos que as orientações regulatórias esclareçam que a inclusão de uma seção específica sobre crianças e adolescentes na política de privacidade da empresa seria suficiente para atender ao requisito de fornecer informações “claras, acessíveis e adequadas”, conforme previsto no Artigo 7º. Além disso, recomenda-se definir, com critérios técnicos e objetivos, o que se entende por “grau mais elevado” e por “configuração mais protetiva da aplicação”, considerando que tais parâmetros devem ser aplicáveis, verificáveis e compatíveis com diferentes tipos de serviços e contextos tecnológicos.

Art. 9º	Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos.	Consideramos que o artigo 9º menciona conteúdo “impróprio, inadequado ou proibido para menores de 18 anos”, mas essa formulação é vaga e pode gerar dificuldades relevantes para serviços que disponibilizam obras literárias. Sem delimitações claras, esses termos subjetivos podem abranger praticamente qualquer tema adulto presente na literatura, inclusive obras com relevância educacional, histórica ou cultural. As orientações regulatórias devem deixar explícito que o escopo de conteúdo “impróprio, inadequado ou proibido” deve se restringir a materiais de natureza pornográfica ou expressamente vedados pela legislação brasileira para crianças e adolescentes.
§ 1º	Para dar efetividade ao disposto no caput, deverão ser adotados mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração.	Consideramos que exigir a verificação da idade em todos os serviços digitais “provavelmente acessados por crianças” representa desafios operacionais e de privacidade significativos, sem necessariamente melhorar os resultados de segurança para menores. As tecnologias atuais de verificação de idade demonstraram limitações em termos de precisão e confiabilidade, com estudos mostrando vieses demográficos e taxas de erro que poderiam restringir injustamente o acesso legítimo (Veja, por exemplo, o relatório Age Assurance Technology Trial (Teste da Tecnologia de Garantia da Idade), financiado pelo Departamento Australiano de Infraestrutura, Transporte, Desenvolvimento Regional, Comunicações, Esporte e Artes.) Além disso, exigir a verificação de idade para todos os serviços não reconhece que diferentes serviços apresentam perfis de risco muito diferentes. É importante ressaltar que, nos casos em que os serviços já implementaram controles parentais robustos e restrições de acesso, conforme exigido por lei, a verificação adicional de idade se torna redundante, uma vez que esses controles existentes já permitem que os pais gerenciem efetivamente o acesso de seus filhos ao conteúdo com base em suas circunstâncias individuais e níveis de maturidade. A exigência e a robustez dos métodos de verificação de idade devem ser diretamente proporcionais ao risco que o produto ou serviço digital representa. Portanto, recomendamos que as orientações regulatórias adotem uma abordagem genuinamente baseada no risco para os requisitos de verificação de idade, concentrando medidas rigorosas em serviços nos

		quais as crianças enfrentam os maiores riscos de danos graves e permitindo opções mais flexíveis para serviços que não apresentam esses riscos. Sugere-se considerar a flexibilização na adoção de mecanismos de idade e que o regulador esclareça (i) critérios sobre parâmetros considerados suficientes à luz do risco trazido por cada serviço e considerando os mecanismos de proteção por padrão e de supervisão parental oferecidos; e (ii) como realizar verificações “a cada acesso” sem gerar coleta massiva de dados pessoais, sem conflitar com os princípios da LGPD, e considerando a inexistência de base de dados oficial do governo para checagem de informações. Por fim, o ECA Digital dispõe que os dados coletados para verificação de idade devem ser utilizados exclusivamente para essa finalidade, vedado seu uso para qualquer outro propósito. Isso implica que informações sobre a verificação da idade não podem ser compartilhadas, reutilizadas ou integradas a outros fluxos de tratamento. Em contraste, a LGPD, combinada com o Enunciado nº 1 da ANPD, admite que dados pessoais desse público alvos sejam tratados com base nas hipóteses legais dos artigos 7º e 11, desde que prevaleça o melhor interesse do menor e haja autorização parental, conforme o artigo 14. Essa divergência entre os dois regimes reforça a necessidade de harmonização regulatória.
§ 2º	Para os fins desta Lei, consideram-se impróprios ou inadequados para crianças e adolescentes os produtos, serviços ou conteúdos de tecnologia da informação que contenham material pornográfico, ou quaisquer outros vedados pela legislação vigente.	Consideramos que é fundamental que as orientações definam com precisão o que caracteriza conteúdo “pornográfico”, distinguindo entre material explicitamente voltado à excitação sexual e obras literárias que incluem elementos sexuais adultos dentro de um contexto narrativo, educacional, histórico ou cultural mais amplo. A definição apresentada pelo § 2º utiliza conceitos excessivamente amplos, o que provoca insegurança jurídica. A classificação precisa ser restritiva e focar em serviços que ignoram a lei, que não oferecem controles parentais e/ou experiências apropriadas à idade. Sem essa diferenciação, existe o risco de que obras literárias legítimas, e culturalmente relevantes, sejam classificadas indevidamente como pornografia.

Art. 13.	Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito.	Recomendamos que seja considerada a possibilidade de utilizar os dados coletados para a verificação de idade de crianças e adolescentes em outras finalidades que estejam diretamente vinculadas ao seu melhor interesse, incluindo ações de prevenção e combate a fraudes. Essa prática é compatível com a LGPD e com o Enunciado nº 1 da ANPD, que admite o tratamento de dados desse grupo etário com base nas hipóteses legais dos artigos 7º e 11, desde que o melhor interesse da criança ou adolescente seja prioridade e que exista consentimento dos responsáveis, conforme exige o artigo 14. Além disso, a oferta de “experiências adequadas à idade” depende justamente do uso dos dados obtidos no processo de verificação etária.
Art.14	Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar medidas técnicas e organizacionais para garantir o recebimento das informações de idade de que trata o art. 12 desta Lei.	Entendemos que o Artigo 14 determina que desenvolvedores de aplicativos com probabilidade de serem utilizados por crianças e adolescentes devem incorporar os sinais de idade disponibilizados pelas lojas de aplicativos, conforme o Artigo 12, além de implementar mecanismos próprios para evitar que menores tenham acesso a conteúdos inadequados à sua faixa etária. No entanto, alguns pontos ainda carecem de detalhamento. Em primeiro lugar, seria importante esclarecer que essa exigência não recai sobre todos os desenvolvedores, mas apenas sobre aqueles cujos aplicativos tenham probabilidade razoável de serem acessados por menores de idade.
Art. 16.	Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar a pais, responsáveis legais, crianças e adolescentes, com acesso de forma independente da aquisição do produto, informações sobre os riscos e as medidas de segurança adotadas para esse público,	Consideramos que o Artigo 16 estabelece que, caso uma empresa realize o tratamento de dados além do que seria “estritamente necessário” para o funcionamento do produto ou serviço, ela deve identificar os riscos envolvidos, adotar medidas de mitigação e elaborar um relatório de impacto. Contudo, a lei não especifica o que se entende por “estritamente necessário”, o que gera incerteza para as empresas quanto às situações em que esse relatório seria obrigatório. Seria importante que qualquer definição desse termo previsse exceções relativas à prevenção de fraude, segurança e cumprimento de obrigações legais. Também seria útil que ficasse claro que uma Avaliação de Impacto à Proteção de Dados, nos moldes da LGPD, é suficiente para atender ao relatório exigido pelo Artigo 16. Além disso, o texto atual apresenta possíveis conflitos com a LGPD. É necessário esclarecer a redação do parágrafo único, especialmente a expressão “sobretudo quando não realizados para fins que não os estritamente necessários para a operação”, uma vez que podem existir tratamentos adicionais legítimos, como aqueles voltados à prevenção de fraude. Também é importante definir se o Relatório de Impacto mencionado na lei é o mesmo previsto pela LGPD e se o tratamento

	incluídas a privacidade e a proteção de dados, em conformidade com o disposto no art. 14 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).	realizado para finalidades que não sejam estritamente necessárias à operação poderia ser interpretado como ausência de finalidade ou falta de adequação, abrindo margem para fiscalização com base na LGPD.
Parágrafo único	Na hipótese de tratamento de dados de crianças e de adolescentes, sobretudo quando realizado para fins que não os estritamente necessários para a operação do produto ou serviço, o controlador a que se refere o inciso VI do art. 5º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverá:	
I	mapear os riscos e envidar esforços para mitigá-los; e	
II	elaborar relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais, a ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente	

	digital, na forma de regulamento.	
Art. 17.	Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão:	Recomendamos que sejam especificadas de forma clara as situações em que o monitoramento do tempo de uso deve ser aplicado, levando em conta as funcionalidades do serviço e os riscos efetivamente envolvidos. Por exemplo, aplicativos do setor financeiro não são concebidos para que crianças ou adolescentes permaneçam navegando por longos períodos, sua finalidade é a realização de transações, cuja gestão já é regulada pelo próprio ECA.
IV	oferecer funcionalidades que permitam limitar e monitorar o tempo de uso do produto ou serviço.	
§ 2º	O desenvolvimento e o uso de mecanismos de supervisão parental deverão ser orientados pelo melhor interesse da criança e do adolescente, considerando o desenvolvimento progressivo de suas capacidades.	Recomendamos que sejam consideradas as funcionalidades e riscos concretos do serviço para o desenvolvimento do mecanismo de supervisão.

V	controle sobre sistemas de recomendação personalizados , inclusive com opção de desativação;	Consideramos que a Lei determina que os serviços disponibilizam controles para “sistemas de recomendação personalizados”, pressupondo que esses mecanismos representam, por si só, um risco para crianças e adolescentes. Contudo, sistemas de recomendação personalizados têm finalidades distintas dependendo do tipo de serviço e, portanto, não devem ser tratados como uniformemente arriscados. O contexto e o propósito de uso influenciam diretamente o perfil de risco. Por exemplo, um sistema que auxilia usuários a navegar por grandes catálogos e localizar conteúdo adequado à idade cumpre uma função totalmente diferente de um sistema voltado a maximizar engajamento contínuo. No primeiro caso, o recurso melhora a experiência do usuário ao reduzir o tempo de busca e integra a lógica essencial do serviço, não sendo algo que possa simplesmente ser desligado. Recomendamos que as orientações regulatórias diferenciam os tipos de sistemas de recomendação personalizados com base em sua finalidade e no risco potencial para crianças e adolescentes. Já aqueles que apenas auxiliam usuários a navegar por catálogos ou a identificar conteúdo adequado à idade devem ser reconhecidos como ferramentas positivas, que aprimoram a experiência do usuário em vez de representarem ameaças. As orientações devem concentrar-se em práticas de design nocivas, como mecanismos que induzem uso excessivo ou promovem conteúdo potencialmente prejudicial, em vez de assumir que toda forma de personalização é problemática. Além disso, é fundamental estabelecer critérios técnicos e objetivos para definir o que constitui um “sistema de recomendação personalizado”.
VI	restrição ao compartilhamento da geolocalização e fornecimento de aviso prévio e claro sobre seu rastreamento;	Recomendamos que seja esclarecido em quais hipóteses deve ocorrer a restrição de geolocalização, considerando funcionalidades e riscos concretos do serviço. Por exemplo, aplicações do setor financeiro utilizam geolocalização para fins de combate e prevenção à fraude.

IX	disponibilização, sempre que tecnicamente viável , de recursos ou de conexões a serviços de suporte emocional e de bem-estar, com conteúdo adequado à faixa etária e orientações baseadas em evidências, especialmente nos casos de interações com riscos psicossociais identificados.	Recomendamos que seja definido, com critérios técnicos e objetivos, o termo "tecnicamente viável".
§ 4º	As configurações-padrão das ferramentas de supervisão parental deverão adotar o mais alto nível de proteção disponível , assegurados, no mínimo:	Consideramos que o artigo 17 explica que as empresas devem fornecer “configurações padrão” que garantam “o mais alto nível de proteção” e, em seguida, fornece uma lista de nove medidas que as empresas podem tomar. Contudo, a lei não esclarece o que exatamente configura esse “nível mais elevado”, o que gera incertezas significativas sobre como os serviços e produtos devem ser implementados na prática. Seria importante fornecer orientações de que nem todas as nove medidas são necessárias e que as empresas têm discricionariedade para decidir com base no risco apresentado por seus produtos e serviços. Sugerimos que as orientações regulatórias definam de forma explícita o que se entende por “modelo mais protetivo disponível”, especificando os principais controles relevantes (por exemplo, práticas de publicidade, marketing e compartilhamento de dados com terceiros) e indicando como esses controles devem ser configurados por padrão para usuários menores de idade.

V	controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação;	Recomendamos que fique claramente estabelecido que o “controle sobre sistemas de recomendação personalizada” previsto no Art. 17, §4º, V deve ter como foco a proteção de crianças e adolescentes contra conteúdos e experiências potencialmente prejudiciais. Exigir controles universais e irrestritos sobre qualquer tipo de recomendação personalizada pode ser tecnicamente inadequado, uma vez que esses sistemas são, em muitos serviços, elementos fundamentais para fornecer conteúdos adequados à idade e melhorar a segurança online. Uma obrigação ampla e absoluta poderia gerar o efeito contrário ao pretendido pela Lei: em vez de restringir a exposição a material sensível e permitir que adolescentes ajustem suas próprias preferências de recomendação, a remoção completa da personalização pode levar à exibição de conteúdos totalmente desconectados da faixa etária, interesses ou nível de maturidade do usuário.
VIII	revisão regular das ferramentas de inteligência artificial, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas;	Consideramos crítico quanto à inclusão de exigências específicas relacionadas à inteligência artificial na Lei, pois essa abordagem parte de uma compreensão equivocada tanto sobre a natureza amplamente difundida da Inteligência Artificial quanto sobre a diversidade de suas aplicações em segurança online. A IA não é, em si, um elemento nocivo; trata-se de uma tecnologia empregada em diversas finalidades legítimas, incluindo a moderação eficiente de conteúdo em larga escala. Ferramentas de IA permitem identificar e remover rapidamente conteúdos prejudiciais em meio a grandes volumes de interações, sendo fundamentais para recursos de proteção infantil, como filtros de conteúdo e detecção de comportamentos potencialmente predatórios. Além disso, a imposição de requisitos específicos para IA não contribui de maneira significativa para os objetivos de proteção previstos na lei. Conteúdos inapropriados para crianças já estão contemplados nas medidas de segurança obrigatórias, independentemente de terem origem humana ou terem sido gerados por IA, o método de criação não altera as obrigações de moderação. Exigir revisão externa dos sistemas de IA, inclusive, pode gerar riscos adicionais ao expor informações sensíveis sobre mecanismos internos de moderação para terceiros. Recomendamos que as orientações regulatórias priorizem práticas, riscos e resultados concretos que a lei busca evitar, em vez de focar na regulação da tecnologia de IA em si. As orientações também devem reconhecer que ferramentas de IA podem fortalecer a segurança online quando bem implementadas, permitindo que os serviços mantenham autonomia para desenvolver e revisar internamente seus sistemas, desde que adotem princípios robustos de segurança desde a concepção. Essa abordagem atenderia de forma mais eficaz aos objetivos de proteção, ao mesmo tempo evitando impactos negativos sobre aplicações benéficas de IA que contribuem para a segurança de crianças e adolescentes.

		Por fim, é importante esclarecer o que seriam “funcionalidades não essenciais ao funcionamento básico dos sistemas”, apresentando exemplos concretos. Entendemos que os sistemas de inteligência artificial integram o próprio desenho do produto ou serviço e que ferramentas destinadas a garantir experiências apropriadas à idade, segurança e integridade devem ser consideradas elementos essenciais.
Art. 18	Art. 18. As ferramentas de supervisão parental deverão permitir aos pais e responsáveis legais:	Entendemos que o artigo 18 estabelece que as ferramentas parentais devem permitir que os responsáveis controlem ou restrinjam compras realizadas por crianças e adolescentes. Contudo, o dispositivo não esclarece o que exatamente se enquadra como “compra”. Por exemplo, prévias ou amostras de livros seriam consideradas compras? Empréstimos digitais se enquadram nessa categoria? Jogos gratuitos podem ser tratados como compras? E, caso não haja qualquer valor monetário envolvido, ainda assim haveria uma “compra”?
II	restringir compras e transações financeiras;	Diante dessas ambiguidades, seria importante que o regulador fornecesse definições mais precisas sobre o que configura uma “compra” para fins do artigo 18.
Art. 28	Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar aos usuários mecanismos de notificações acerca de violações aos direitos de crianças e de adolescentes.	Consideramos que a Lei mistura duas esferas que deveriam ser tratadas separadamente: a proteção contra danos graves a crianças (tema de segurança infantil) e a gestão de acesso a conteúdo inadequado para a idade (tema de moderação de conteúdo). O Artigo 28, por exemplo, impõe obrigações de notificação a qualquer serviço acessível por crianças, ainda que o serviço não ofereça funcionalidades ou riscos que possam efetivamente gerar danos graves. De modo semelhante, o Artigo 29 determina a remoção de conteúdo considerado “ofensivo” quando reportado pelas vítimas.
Parágrafo único	Notificados acerca de violações aos direitos de crianças e de adolescentes no âmbito de seus serviços, os	Como o Artigo 28 trata de comunicação às autoridades competentes para investigação e o Artigo 29 menciona especificamente “vítimas”, compreendemos que a intenção é abordar situações de risco grave à segurança de crianças, e não reclamações genéricas sobre conteúdo inadequado. Porém, a redação atual não define de forma precisa quais tipos de danos acionariam essas obrigações.
		Recomendamos, portanto, que as orientações regulatórias diferenciem claramente o conteúdo que causa prejuízo a crianças reais e identificáveis, exigindo intervenção urgente, daquele que é apenas impróprio para determinadas faixas etárias, devendo ser tratado por meio de mecanismos de moderação de conteúdo. As orientações deveriam estabelecer que os

	fornecedores deverão, quando for o caso, oficiar às autoridades competentes para instauração de investigação, nos termos de regulamento.	Artigos 28 e 29 se aplicam exclusivamente a conteúdos que causem ou ameacem causar danos graves a uma criança identificável ou que representem risco iminente à sua vida, segurança ou bem-estar (incluindo casos de cyberbullying ou assédio).
Art. 29.	Para atender ao princípio da proteção integral, é dever dos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles proceder à retirada de conteúdo que viola direitos de crianças e de adolescentes assim que forem comunicados do caráter ofensivo da publicação pela vítima, por seus representantes, pelo Ministério Público ou por entidades representativas de defesa dos direitos de crianças e de adolescentes, independentemente de ordem judicial.	Esse esclarecimento ajudaria a garantir que os esforços de investigação se concentrem em ameaças concretas à segurança infantil, enquanto questões gerais de conteúdo continuam a ser tratadas pelos fluxos regulares de moderação. Também permitiria definir parâmetros mais objetivos para identificar quando o conteúdo exige remoção imediata nos termos do Artigo 29.
§ 1º	Serão considerados violadores de direitos de crianças e de adolescentes os conteúdos referidos no art. 6º desta Lei, nos termos da classificação indicativa.	

§ 2º	A notificação prevista no caput deste artigo deverá conter, sob pena de nulidade, elementos que permitam a identificação técnica específica do conteúdo apontado como violador dos direitos de crianças e de adolescentes e do autor da notificação, vedada a denúncia anônima.	
§ 3º	Os provedores de aplicação deverão tornar público e de fácil acesso o mecanismo pelo qual a notificação prevista no caput deste artigo deverá ser encaminhada pelo notificante.	
§ 4º	Não estarão sujeitos ao procedimento de retirada de que trata o caput deste artigo os conteúdos jornalísticos e os submetidos a controle editorial.	
Art. 31.	Os provedores de aplicações de internet direcionadas a crianças e a adolescentes ou de acesso provável por eles que possuírem mais de 1.000.000 (um milhão) de usuários nessa faixa etária registrados, com conexão de	Tendo em vista que o relatório deve ser disponibilizado no site institucional, a exigência de divulgar informações como: a obrigação de disponibilizar os sistemas e processos de apuração (I), os aprimoramentos técnicos para a proteção de dados pessoais e privacidade (V), aprimoramentos técnicos para aferição do consentimento parental (V), bem como o detalhamento dos métodos utilizados (VII), pode tornar pública diversas informações internas e estratégia da empresa, torna-se necessário esclarecer: - se provedores com até 1 milhão de cadastros dentro dessa faixa etária estão dispensados da elaboração do relatório ou se há algum tipo de modulação das obrigações e, em caso afirmativo, quais seriam essas obrigações reduzidas;

	internet no território nacional, deverão elaborar relatórios semestrais, em língua portuguesa, a serem publicados no sítio eletrônico do provedor, que contenha:	- se o limite de 1 milhão de cadastros deve ser aferido por produto/serviço individualmente, e não pelo grupo econômico, uma vez que um mesmo grupo pode possuir diferentes empresas e produtos, cada qual com CNPJ e operações próprias.
I	os canais disponíveis para recebimento de denúncias e os sistemas e processos de apuração;	
II	a quantidade de denúncias recebidas;	
III	a quantidade de moderação de conteúdo ou de contas, por tipo;	
IV	as medidas adotadas para identificação de contas infantis em redes sociais, conforme o disposto no § 3º do art. 24, e de atos ilícitos, conforme o disposto o art. 27 desta Lei;	
V	os aprimoramentos técnicos para a proteção de dados pessoais e da privacidade das crianças e dos adolescentes;	
VI	os aprimoramentos técnicos para aferir consentimento parental conforme o disposto no § 1º do art. 14 da Lei nº 13.709, de 14 de agosto de	

	2018 (Lei Geral de Proteção de Dados Pessoais); e	
VII	o detalhamento dos métodos utilizados e a apresentação dos resultados das avaliações de impacto, identificação e gerenciamento de riscos à segurança e à saúde de crianças e de adolescentes.	
Parágrafo único	Os provedores de aplicações de internet deverão viabilizar, de forma gratuita, o acesso a dados necessários à realização de pesquisas sobre os impactos de seus produtos e serviços nos direitos de crianças e de adolescentes e no melhor interesse deles, por parte de instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas, conforme critérios e requisitos definidos em regulamento, vedada a utilização desses dados para quaisquer finalidades comerciais e assegurado o cumprimento dos princípios da finalidade, da necessidade, da segurança e da	Recomendamos que seja esclarecido o termo "dados necessários". Recomendamos que seja incluído que os dados compartilhados podem ser anonimizados Recomendamos que seja incluído a proteção ao segredo comercial.

	confidencialidade das informações.	
Art. 33.	Os provedores de aplicações de internet direcionadas a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar aos usuários informações claras e acessíveis sobre as hipóteses de uso indevido dos instrumentos de denúncia, bem como sobre as sanções cabíveis, observado o devido processo interno.	Recomendamos que seja esclarecido o termo "usuários" aqui, refere-se a usuários logados na plataforma.
Art. 35.	Sem prejuízo das demais sanções cíveis, criminais ou administrativas, em caso de descumprimento das obrigações previstas nesta Lei, assegurados o devido processo legal, a ampla defesa e o contraditório, os infratores estarão sujeitos às seguintes penalidades:	Recomendamos que seja esclarecido se as sanções poderão ser aplicadas de forma cumulativa ou isolada.
I	advertência, com prazo para adoção de medidas corretivas de até 30 (trinta) dias;	

II	multa simples, de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício ou, ausente o faturamento, multa de R\$ 10,00 (dez reais) até R\$ 1.000,00 (mil reais) por usuário cadastrado do provedor sancionado, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;	
III	suspensão temporária das atividades;	
IV	proibição de exercício das atividades.	
§ 1º	Para fixação e gradação da sanção, deverão ser observadas, além da proporcionalidade e da razoabilidade, as seguintes circunstâncias:	Recomendamos avaliar a possibilidade de incluir, como critério para definição e graduação das sanções, as medidas de proteção implementadas pelo agente para resguardar os dados pessoais e a privacidade de crianças e adolescentes, em observância ao princípio da boa-fé. Além disso, sugerimos considerar fatores como a extensão do dano, o nível de cooperação do agente, a existência de políticas e estruturas de governança adequadas e a adoção de medidas corretivas.
I	a gravidade da infração, considerados os seus motivos e a extensão do dano nas esferas individual e coletiva;	
II	a reincidência na prática de infrações previstas nesta Lei;	

III	a capacidade econômica do infrator, no caso de aplicação da sanção de multa;	
IV	a finalidade social do fornecedor e o impacto sobre a coletividade no que se refere ao fluxo de informações no território nacional.	
§ 3º	O processo de apuração das infrações ao disposto nesta Lei e de aplicação das sanções cabíveis reger-se-á pelas disposições relativas à apuração de infrações administrativas às normas de proteção da criança e do adolescente e à imposição das respectivas penalidades previstas na Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).	

Reconhecemos que a ANPD passou a exercer as competências de fiscalização e sanção previstas no ECA Digital. No entanto, o próprio ECA Digital determina que o processo de apuração e aplicação de penalidades siga as regras da Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente). Isso cria uma assimetria: a fiscalização será conduzida por uma autoridade especializada, com regulamentos atuais e alinhados às práticas modernas, enquanto o procedimento sancionatório estaria vinculado a um rito processual de 1990.

Diante disso, é necessário esclarecer, ou ajustar, o texto legal, de modo a garantir que o processo de aplicação de sanções seja efetivo, atualizado e coerente com as práticas regulatórias contemporâneas. Também é importante indicar como se dará a aplicação da Lei nº 9.784/1999 no âmbito dos processos conduzidos pela ANPD.

Art. 39.	As obrigações previstas nos arts. 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 desta Lei aplicar-se-ão conforme as características e as funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o grau de interferência do fornecedor do produto ou serviço sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor.	Recomendamos que seja esclarecido parâmetros técnicos e objetivos para: • Grau de interferência, definindo como deve ser mensurado e em quais situações se considera maior ou menor impacto; • Número de usuários, com faixas classificatórias (baixo, médio ou alto alcance) e critérios explícitos que indiquem quando um serviço se enquadra em cada categoria; • Porte do fornecedor, com distinção entre micro ou pequeno, médio e grande porte, alinhando-se, sempre que possível, às métricas já adotadas pela ANPD para agentes de pequeno porte; • Características e funcionalidades do serviço, que constituem um dos critérios mais relevantes ainda sem definição clara. O próprio ECA Digital, no art. 1º, III, menciona a necessidade de avaliar se o produto ou serviço representa “risco significativo à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e adolescentes, especialmente quando destinado à interação social e ao compartilhamento de informações em larga escala”. Esses elementos precisam ser detalhados de forma objetiva para assegurar segurança jurídica e coerência na aplicação das obrigações regulatórias.

§ 1º	Os provedores dos serviços com controle editorial e os provedores de conteúdos protegidos por direitos autorais previamente licenciados de agente econômico responsável que não se confunda com usuário final estarão dispensados do cumprimento das obrigações previstas nos artigos referidos no caput deste artigo, desde que:	Consideramos que embora a Lei dispense serviços com controle editorial de diversas obrigações, o alcance real dessa exceção permanece pouco definido. A norma parece presumir que tais serviços apresentam menor risco, mas baseia essa distinção no método de seleção do conteúdo, e não no aspecto mais relevante, que é a origem desse conteúdo. O fator determinante de risco é se o serviço disponibiliza, predominantemente, conteúdo gerado por usuários finais; quando isso ocorre, a isenção não deveria ser aplicada. Além disso, para plataformas que oferecem conteúdo produzido profissionalmente, e não conteúdo criado pelos usuários, o exercício do “controle editorial” deve abranger a moderação proativa em escala para garantir o cumprimento dos critérios de curadoria e das políticas internas de conteúdo. Como esses serviços recebem obras de diferentes fontes (licenciadores, distribuidores, agregadores etc.), o uso de processos automatizados na seleção não deve excluir sua qualificação para a isenção, desde que esses processos filtrem e rejeitem materiais que não estejam em conformidade com os padrões editoriais do serviço. Recomendamos, portanto, que as orientações regulatórias esclareçam dois pontos essenciais: (i) a isenção se aplica a serviços cujo conteúdo principal não é gerado por usuários finais; (ii) “controle editorial” abrange a moderação e curadoria proativas, independentemente de a seleção ser manual ou automatizada. Adicionalmente, a isenção destinada a serviços editoriais deve reconhecer que determinados tipos de conteúdo, como obras literárias, nunca foram submetidos a sistemas formais de classificação indicativa no Brasil. Assim, as orientações devem esclarecer que serviços literários enquadrados no art. 39 não precisam adotar classificações etárias tradicionais inexistentes para o setor. Em vez disso, podem utilizar categorias já consolidadas na indústria e mecanismos eficazes de controle parental como alternativas de conformidade. Esse ajuste preservaria a liberdade editorial e literária, ao mesmo tempo em que asseguraria a proteção de crianças e adolescentes por meio de ferramentas apropriadas de supervisão.
III	disponibilizem mecanismos técnicos de mediação parental de acesso facilitado que permitam aos pais ou responsáveis legais exercer o	Recomendamos que seja esclarecido se por “mediação parental” entende-se o mesmo que supervisão parental, uma vez que o termo “mediação parental” não está definido na Lei.

	controle sobre a forma com que crianças e adolescentes usam o serviço, a fim de possibilitar a restrição de:	

TOMADA DE SUBSÍDIOS CONCEITOS PREVISTOS NO ECA DIGITAL - ANPD

1. Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

(Parágrafo)

O Comitê Gestor da Internet no Brasil – CGI.br vem, por meio desta Tomada de Subsídios promovida pela Agência Nacional de Proteção de Dados (ANPD), oferecer contribuições para o esclarecimento adicional de termos, conceitos e expressões previstas no Estatuto Digital da Criança e Adolescente – Lei n. 15.211/2025.

No exercício de suas atribuições, o CGI.br¹ tem desempenhado papel central na promoção do diálogo multissetorial e na construção de consensos para o desenvolvimento de políticas públicas e marcos regulatórios relacionados à governança da Internet no país. Essa atuação histórica se materializa em contribuições fundamentais para o ecossistema regulatório brasileiro, como o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e, mais recentemente, o próprio Estatuto Digital da Criança e do Adolescente² (Lei nº 15.211/2025).

Saudamos a iniciativa da Agência Nacional de Proteção de Dados (ANPD) ao realizar esta Tomada de Subsídios voltada ao aprimoramento e esclarecimento de termos, conceitos e expressões previstos no ECA Digital. Trata-se de oportunidade relevante para que sociedade civil, especialistas, setor público, setor privado e academia contribuam para uma aplicação mais precisa, uniforme e juridicamente segura da lei.

Reafirmamos a disposição do CGI.br em cooperar com recomendações técnicas e princípios de governança da Internet que possam auxiliar na implementação do ECA Digital, reconhecendo sua importância para a proteção integral e a prioridade absoluta de crianças e adolescentes no ambiente digital.

Destacamos, ainda, que esta Tomada de Subsídios é instrumento valioso para assegurar que os termos e definições trazidos pelo ECA Digital resultem em práticas regulatórias capazes de proteger crianças e adolescentes sem comprometer privacidade, usabilidade, inclusão digital, segurança ou inovação, preservando ao mesmo tempo os valores fundamentais de abertura, interoperabilidade e universalidade da Internet.

¹ <https://cgi.br/atribuicoes/>

² Cf. <https://cgi.br/publicacao/resposta-do-cgi-br-ao-oficio-n-18-gdja-2025-colaboracao-tecnica-sobre-definicoes-presentes-no-pl-n-2628-2022/>

Assim, as contribuições apresentadas pelo CGI.br concentram-se nos termos e expressões adiante indicados e previstos no ECA Digital que demandam maior precisão para sua adequada interpretação e aplicação

1. Acesso provável aos produtos e serviços (Art. 1º);
2. Produtos e serviços de tecnologia da informação (Art. 2º); e
3. Modulação de obrigações de acordo com o grau de interferência sobre o conteúdo (Art. 39).

1. Definição de “acesso provável” por criança e adolescente

O ECA digital acertadamente adotou uma abordagem que considera a materialidade de uso das crianças e adolescentes, isto é, aplica-se não apenas aos produtos ou serviços formalmente direcionados a este público, mas também àqueles que podem ser utilizados por crianças e adolescentes. Resta, no entanto, para melhor precisão e para sua adequada interpretação e aplicação, definir o que seria este “acesso provável”.

Embora a Lei 15.211/2025 já estabeleça diretrizes gerais para definir situações que são consideradas “acesso provável” por crianças e adolescentes no seu Art. 1º, a saber: (I) suficiente probabilidade de uso e atratividade do produto; (II) facilidade de acesso e de utilização do produto ou serviço; e (III) significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes³, **persistem dúvidas operacionais para aplicação da lei, especialmente se:**

- a) os critérios trazidos pelo artigo 1º do ECA Digital são **cumulativos, alternativos ou graduais**;
- b) há critérios adicionais para a apuração prática de cada um deles;
- c) há fatores, características e funcionalidades que devem ser considerados.

A ausência de parâmetros regulatórios mais claros para a definição de “acesso provável” por crianças e adolescentes pode gerar incerteza jurídica e risco de aplicação inadequada ou ineficaz da lei. Por exemplo, sem critérios objetivos, serviços que não têm materialidade de uso infantil podem ser indevidamente classificados como de acesso provável, criando obrigações desnecessárias e/ou excessivas, gerando, inclusive, custos injustificados. Ao mesmo tempo, plataformas amplamente utilizadas por crianças e adolescentes, inclusive de forma não intencional, podem deixar de ser enquadradas, esvaziando a efetividade protetiva do ECA Digital.

³ “Art. 1º [...] Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações: I – suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes; II – considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes; e III – significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital”.

Além disso, a falta de critérios claros dificulta a atuação uniforme dos órgãos fiscalizadores e do próprio Poder Judiciário, abrindo espaço para decisões divergentes. Essa heterogeneidade compromete a segurança jurídica, a eficiência administrativa e a coerência regulatória.

Por essas razões, mostra-se essencial que a ANPD estabeleça complementação para orientar a interpretação e aplicação do termo “acesso provável”, garantindo proteção efetiva às crianças e adolescentes sem impor obrigações inadequadas ou incompatíveis com o funcionamento da Internet.

Visando contribuir para a construção dessa complementação, mencionamos a seguir, **a título apenas elucidativo**, a regulamentação conduzida sobre “acesso provável” pela legislação internacional, que, em alguma medida, serviu de inspiração para o ECA digital.

A) Acesso provável no Online Safety Act (Reino Unido)

O Online Safety Act do Reino Unido define deveres específicos para serviços *likely to be accessed by children*, definindo três situações em que essa probabilidade ocorre: i) quando a avaliação de acesso de crianças realizada pelo provedor conclui que o serviço é de acesso provável por crianças; ii) quando o provedor do serviço falha em realizar essa avaliação de acesso e; iii) quando o órgão regulatório, após investigação, determina que o serviço seja tratado como de uso provável por crianças⁴.

Dessa forma, a **avaliação de acesso por crianças**⁵ que deve ser realizada pelo provedor do serviço, é peça central para a aplicação da legislação. Segundo a lei britânica, nesta avaliação são analisados dois principais critérios: primeiro, se é possível que crianças acessem o serviço ou parte dele; **e**, segundo, se a condição de usuário da criança é atendida em relação ao serviço ou parte dele⁶. Ambas as condições precisam ser preenchidas para que a avaliação conclua que se trata de um serviço de acesso provável por crianças.

Quanto ao primeiro critério, para concluir que não é possível acessar o serviço, a legislação britânica define como única medida a verificação ou estimativa de idade com o resultado de que crianças não estão, normalmente, aptas a acessá-lo⁷, tendo em vista — complementa o guia da autoridade regulatória — que se utiliza um “método altamente efetivo de aferição de idade”⁸. Se o serviço analisa esta primeira etapa e conclui que não é possível acessá-lo, não é necessário prosseguir a avaliação do segundo critério, conforme o Office of Communication informa no guia de avaliação de acesso. Contudo, caso não seja possível afirmar que o serviço não pode ser acessado por crianças — pois não se utiliza um método efetivo de aferição de idade — o provedor deve partir para a segunda etapa que é avaliar se a criança atende a “condição de usuário”.

Quanto ao segundo critério, o Online Safety Act define que a condição de usuário da criança é encontrada quando há um número significativo de crianças que são usuárias do serviço — sendo “número significativo” considerado em relação ao total de usuários britânicos do serviço e

⁴ Cf. Seção 37 do Online Safety Act. Disponível em: <https://www.legislation.gov.uk/ukpga/2023/50/contents>

⁵ Destaca-se que, a legislação britânica, embora use apenas o termo “criança”, considera criança como todos menores de 18 anos de idade.

⁶ Cf. Seção 36 (1).

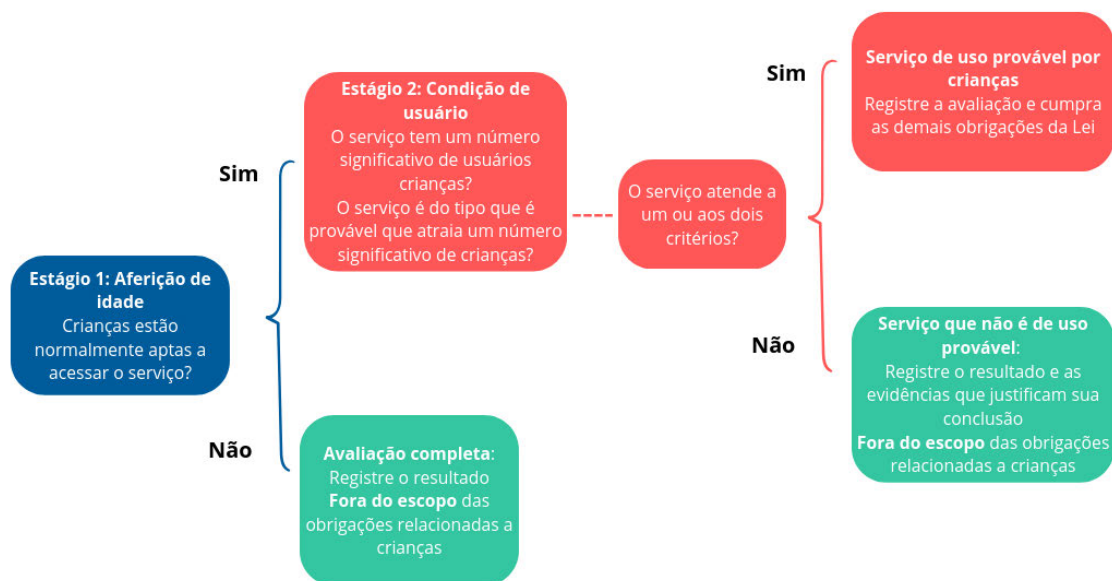
⁷ Cf. Seção 36 (2).

⁸ Ofcom “Children’s access Assessments – Guidance”. 2025. Disponível em:

<https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679>

considerando evidências sobre quem de fato usa o serviço, não os usuários que se pretende ter —, ou se é provável que o serviço ou parte dele atraia um número significativo de crianças⁹.

Em suma, a lei britânica e sua autoridade reguladora — Ofcom — delineiam o seguinte caminho para que os serviços definam se são serviços de acesso provável:



Fonte: Adaptada de figura do guia “Children’s access assessments – Guidance”, produzido pela Ofcom.

A Ofcom traz, em seu guia sobre avaliação de acesso de crianças, uma série de sugestões de fatores, características e outros critérios para auxiliar aos provedores dos serviços a realizar uma boa avaliação de acesso.

Sobre a análise da **primeira etapa**, a autoridade detalha as condições em que não é possível afirmar se o serviço não pode ser acessado por crianças, isto é, o que significa não adotar um método altamente eficiente de aferição de idade, são estas:

- i) quando o serviço não utiliza qualquer meio de aferição de idade;
- ii) quando a forma adotada de aferição de idade não é capaz de ser altamente efetiva (como autodeclaração ou por meio de dados de cartão de crédito);
- iii) quando a aferição de idade não é implementada ou usada de forma altamente efetiva, isto é, não é tecnicamente acurada, robusta, confiável e justa;
- iv) não adota medidas para mitigar métodos de circunvenção à aferição de idade que sejam possivelmente adotáveis por crianças; ou
- v) se o provedor permite que crianças ainda acessem parte, funcionalidades, comunidades ou conteúdos do serviço.

Para a **segunda etapa** (ou critério), a Ofcom exemplifica os fatores e características (não exaustivos) que podem auxiliar na análise se o serviço tem um número significativo de usuários ou se é atrativo para este público. De antemão, a autoridade alerta que pode ser desafiador buscar evidências para identificar se há um número significativo de usuários em serviços que não realizam aferição de idade.

⁹ Cf. Seção 36 (3)(4).

Quanto ao número significativo de usuários, a Ofcom esclarece que significativo é, como define a lei, em relação à quantidade de usuários no Reino Unido do serviço, mas o número exato (absoluto ou proporcional) depende fortemente do contexto e natureza do serviço, devendo-se ter em mente que a lei britânica busca estabelecer altos padrões de proteção para crianças nos serviços regulados. Nesse sentido, destaca que mesmo um número ou percentual relativamente pequeno de usuários crianças pode ser considerado significativo. A autoridade destaca fontes de dados que não são apropriadas para estabelecer o número de usuários crianças — como idade autodeclarada e métodos de pagamento online e — traz três exemplos de fatores que auxiliam a identificar se o serviço tem um número significativo de usuários que são crianças:

- Se as crianças fazem parte da estratégia comercial (por exemplo, informações fornecidas por anunciantes, como o número de cliques em publicidade voltada para crianças).
 - Evidências de fontes internas (como relatórios e reclamações de usuários menores de 18 anos e estatísticas sobre a remoção de contas de usuários deste público).
 - Evidências de fontes externas e independentes (como pesquisas de mercado e evidências quantitativas de terceiros que monitoram o consumo de mídia infantil).
- (Adaptado e traduzido da Tabela 6 “Factors to consider when assessing whether the child user condition is met”)

Quanto à atratividade dos serviços para crianças, a Ofcom estabelece critérios para indicar os tipos de serviços que provavelmente atraem quantidade significativa de crianças — mesmo que se trate de um número relativamente pequeno. Segundo a autoridade uma série de razões podem ser relevantes para definir a atratividade, como os benefícios gerados, o tipo de conteúdo, de funcionalidades, de design e a estratégia comercial. Se a estratégia comercial inclui, por exemplo, obter receitas de crianças e pais via publicidade, então seria razoável supor que o serviço atinge esse critério. Da mesma forma, se uma ampla gama de tipos de conteúdos estão disponíveis, pode-se supor que é provável que haja tipos de conteúdos atrativos para crianças. Em contrapartida, se há no serviço tipos reduzidos de conteúdos, deve-se avaliar se estes são atrativos para crianças – por exemplo, evidências sugerem, segundo a autoridade, que conteúdos relacionados a relacionamento (*dating*) e pornografia são atrativos para crianças e adolescentes. Em síntese, a autoridade elenca os seguintes **fatores exemplificativos para avaliar a atratividade do serviço**:

- Se o serviço traz benefícios para as crianças.
 - Se o conteúdo do serviço é atraente para as crianças.
 - Se o design do serviço é atraente para as crianças (cores, apresentação, recursos e funcionalidades).
 - Se as crianças fazem parte do modelo de negócios, estratégia de marketing e plano de crescimento.
 - Evidências de fontes internas (como denúncias e reclamações de usuários menores de 18 anos e estatísticas sobre a remoção de contas deste público).
 - Evidências de fontes externas e independentes (como pesquisas de mercado e evidências de terceiros que acompanham o consumo de mídia por crianças).
- (Adaptado e traduzido da Tabela 6 “Factors to consider when assessing whether the child user condition is met”)

Assim, nota-se que os critérios bases para configurar acesso provável no Reino Unido — possibilidade de acesso medida por aferição de idade **E** haver um número significativo de crianças que são usuárias **OU** ser provável que o serviço seja atrativo para crianças — são bastante similares

aos critérios estabelecidos no Art. 1º do ECA Digital, com exceção do terceiro critério brasileiro (sobre risco) que não está presente na legislação britânica como critério para definir uso provável:

Online Safety Act (RU)	ECA Digital (Brasil)
Se é normalmente possível para crianças acessarem o serviço ou parte dele (Seção 35 (1a)).	“Considera-se acesso provável por crianças e adolescentes as seguintes situações [...] considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes”
Se a condição de usuário é atendida, se: - há uma quantidade significativa de crianças que são usuários do serviço ou parte dele; - O serviço, ou parte dele, é do tipo que provavelmente atrai quantidade significativa de usuários que são crianças (Seção 35 (1b)(3)).	“Considera-se acesso provável por crianças e adolescentes as seguintes situações [...] I - suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes”
—	“Considera-se acesso provável por crianças e adolescentes as seguintes situações [...] III – significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes [...]”

Dessa forma, de um lado, a exemplificação de fatores, características e funcionalidades que a autoridade britânica indica para auxiliar a definição de acesso provável podem servir de inspiração para a complementação a ser feita pela autoridade brasileira. De outro lado, a interessante relação estabelecida pela legislação britânica de critérios cumulativos (possibilidade de acesso e condição de usuário) e critérios alternativos (quantidade significativa de usuários ou atratividade significativa) trazem luz para como a legislação brasileira não estabeleceu claramente a relação entre os três critérios elencados — podendo esta definição ser elencada pela ANPD.

Ainda, é importante lembrar que tais obrigações são aplicáveis apenas a “Part 3 services”, isto é, “regulated user-to-user services” e “regulated search services” e com serviços explicitamente excepcionados – em outras palavras, tem uma aplicação mais restrita que o ECA digital — o que será tratado no item dois desta contribuição.

B) Age appropriate design: a code of practice for online services (Reino Unido)

O “Design adequado para idade: código de boas práticas para serviços online” do Reino Unido — que aborda salvaguardas de proteção de dados em serviços online — também pode servir de inspiração para o detalhamento da definição de serviço e produtos de uso provável. O código é aplicável a serviços da sociedade da informação que são de uso provável por crianças (*relevant information society services which are likely to be accessed by children*)¹⁰.

A identificação de uso provável por crianças e adolescentes também é, no caso deste código, uma avaliação proveniente do próprio serviço, de acordo com alguns critérios estabelecidos pela autoridade de proteção de dados pessoais no Reino Unido, o Information Commissioner’s Office (ICO). O código é aplicável a serviços direcionados a crianças ou quando acessados por um número significativo de crianças (**significant number of children**), ou seja, se é razoável concluir que pessoas menores de 18 anos formam um grupo material de pessoas que usam o serviço.

¹⁰ Cf. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/>

A ICO indica que a probabilidade de um serviço ser acessado por crianças ou não dependerá (i) da **natureza e conteúdo** do serviço e se isso tem um **apelo** especial para as crianças e (ii) da forma **como o serviço é acessado** e das medidas adotadas para impedir o acesso de crianças. Assim, se a natureza, o conteúdo ou a apresentação do serviço fizer com que as crianças queiram usá-lo e/ou se as crianças formarem um grupo de usuários substancial e identificável, a autoridade britânica entende que a definição “provavelmente acessado por” será aplicada.

Para a definição do que é “significativo”, a ICO destaca, além do possível número de usuários crianças, os **riscos relacionados ao tratamento de dados que o serviço impõe**. Ainda são citados uma série de indicadores possíveis para essa avaliação, como evidências sobre o comportamento de usuários (e.g. picos de uso após o horário escolar ou em feriados), a existência de publicidade direcionada a crianças e reclamações relacionadas; ou ainda os tipos de conteúdos e atividades atrativas para crianças, dentre outros exemplos¹¹.

Nesse sentido, as indicações de critérios (natureza e conteúdo; apelo para crianças e; como o serviço é acessado), assim como os fatores exemplificativos são bastante semelhantes aos determinados no Online Safety Act e em sua regulamentação. Nota-se, no entanto, que dentre os fatores possíveis para determinar o que é significativo estão os riscos relacionados ao tratamento de dados, em semelhança à legislação brasileira.

C) Recomendações do CGI.br para a complementação da definição de acesso provável

A legislação brasileira não definiu com precisão a relação e hierarquia entre os critérios previstos no art. 1º do ECA Digital, isto é, se a ocorrência de apenas uma das situações já seria suficiente para caracterizar “acesso provável”. Por essa razão, **a regulamentação pode esclarecer, de forma inequívoca, como a relação entre os três critérios elencados se articula, se devem ser interpretados de maneira cumulativa ou alternativa**, como ilustrado pela experiência de regulamentação do Online Safety Act. Caso contrário, corre-se o risco de estabelecer um escopo excessivo de aplicação da legislação, abrangendo produtos e serviços que não possuem participação relevante de crianças ou adolescentes ou com probabilidade baixíssima ou nula de que venha haver.

C.1 Sobre o inciso II

O inciso II menciona a “considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes”, entre as situações para configurar acesso provável.

Todas as aplicações de Internet, conforme o Marco Civil da Internet, **são acessadas por meio de um terminal conectado à Internet, condição que, por si, já representa de amplo e fácil acesso** por qualquer indivíduo com um dispositivo e acesso à Internet. Mesmo assim, **não nos parece correto dizer que toda a Internet é de acesso provável por crianças e adolescentes**, dado que, por exemplo, sites específicos sobre assuntos como investimentos, regulamentações do Banco central, aposentadoria, serviços jurídicos, etc. embora facilmente acessíveis não são destinados nem atraentes ao público infantojuvenil.

¹¹ Cf. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/>

Permitir essa interpretação tão ampla seria, assim, desproporcional e indesejada podendo incentivar que todos os provedores de aplicações (e demais fornecedores elencados na lei) adotassem meios para dificultar o acesso e uso de seu produto ou serviço, o que, no geral, implicaria uma obrigação generalizada de métodos de aferição etária.

Destaca-se que, para o **CGI.br**, **impor uma obrigação generalizada de aferição etária para todos os fornecedores de produtos e serviços de tecnologia da informação contrariaria o princípio da proporcionalidade e necessidade** e seria potencialmente prejudicial à inovação e ao funcionamento adequado do ecossistema digital¹².

Dessa forma, **o CGI.br recomenda que o critério do inciso II do art. 1o. do ECA Digital sobre a facilidade de acesso e uso do produto ou serviço não seja interpretado e considerado de forma isolada dos outros critérios, a fim de garantir uma aplicação proporcional, necessária e alinhada à finalidade da Lei.**

Por outro lado, diferente da regulação britânica, **mesmo quem adota meios altamente efetivos de aferição de idade**, isto é, quem dificulta ao máximo o acesso e uso por crianças e adolescentes, mas é atrativo ou apresenta riscos a crianças e adolescentes, **não deve ficar totalmente de fora do escopo da legislação**. Isso porque, permanece importante a aplicação de diversos dispositivos, como as obrigações relacionados à aferição de idade, à prevenção e combate a violações graves contra crianças e adolescentes, além dos mecanismos de responsabilização e aplicação de sanções.

A interpretação do que é facilidade ou dificuldade de acesso, ainda, pode passar por indicar quais são os métodos e procedimentos mais efetivos de aferição de idade — o que não significa sua recomendação para toda e qualquer situação. Envolvendo, além da definição de métodos eficientes, uma implementação robusta, acurada e justa.

C.2 Sobre os incisos I e III

Quanto à situação prevista no inciso I — suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes —, **entende-se que a Agência deve estabelecer critérios adicionais para esclarecer o dispositivo**. Para isso, deve-se considerar como a natureza do produto ou serviço, suas funcionalidades, design, estratégia comercial, os benefícios gerados com seu uso e os tipos de conteúdos disponíveis impactam a probabilidade de uso e atratividade para crianças e adolescentes. Nesse sentido, podem ser indicados conteúdos, ou benefícios e estratégias específicas para ilustrar a interpretação da Agência, a fim de facilitar a compreensão dos diferentes fornecedores quanto a estarem fora ou dentro do escopo da legislação.

Consideramos que atender às condições de fácil acesso (inciso II) e uso provável ou atrativo (inciso I) já deve ser suficiente para indicar a materialidade de uso por crianças e adolescentes e, portanto, para implicar a aplicação da lei, mesmo que sem a avaliação se o serviço oferece risco significativo a este grupo. Isso porque, avaliações de risco são necessariamente mais complexas e envolvem maior grau de subjetividade, como a prospecção de possíveis e futuros impactos às crianças e adolescentes além de potenciais conflitos de interesse. Ao passo que os critérios de atratividade podem se embasar em evidências mais objetivas e até quantitativas, como a

¹² Cf. contribuição do CGI.br à consulta pública do Ministério da Justiça sobre aferição de idade. Disponível em: <https://cgi.br/publicacao/contribuicao-do-cgi-br-a-consulta-publica-afericao-de-idade-na-internet-brasileira-do-ministerio-da-justica-e-seguranca-publica/>.

receita com publicidade infantil, ou a quantidade de denúncias relacionadas a usuários menores de idade. Dada essa assimetria metodológica, parece-nos que exigir a realização de avaliações de risco mesmo para produtos ou serviços que sejam considerados de fácil acesso e atrativos, poderia gerar implicações regulatórias indesejadas, excluindo fornecedores relevantes e impondo complexidade desnecessária para a definição do escopo de aplicação da lei.

Sobre a hipótese prevista no inciso III, qual seja “significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital”, entende-se que a existência de risco significativo no produto ou serviço configura, por si só, uso provável e enseja a aplicação da legislação, ou seja, independente da presença ou ausência das situações previstas nos incisos I e II. .

Assim, delinea-se o seguinte desenho entre os critérios do Art. 1º, conforme as seguintes hipóteses:

- a) quando o produto ou serviço for de **considerável facilidade de acesso e utilização por esse público** (inciso II) e, **adicionalmente**, for de provável uso **ou** apresentar atratividade relevante para crianças e adolescentes (inciso I), ainda que não se tenha caracterizado comprovadamente significativo grau de risco específico nos termos do inciso III, deverá ser reconhecido o acesso provável;
- b) quando o produto ou serviço apresentar **significativo grau de risco** à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e adolescentes (inciso III), ainda que não se verifique provável uso ou apresentar atratividade relevante para crianças e adolescentes (inciso I) e, também, independentemente da comprovação de facilidade de acesso e utilização (inciso II), igualmente deverá ser reconhecido o acesso provável.

Em síntese, configura-se acesso provável o produto ou serviço de tecnologia da informação que:

- é de considerável fácil acesso e utilização (II) + é suficiente atrativo ou de uso provável para crianças e adolescentes (I); **OU**
- tem significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes (III)

Para além da articulação entre os critérios previstos no art. 1º. do ECA Digital, é **importante que a regulamentação estabeleça critérios que permitam aos fornecedores avaliarem com facilidade se seu produto ou serviço oferece risco a crianças e adolescentes**. Nesse sentido, a classificação de riscos online conhecida como os 4Cs pode servir de baliza:

- no conteúdo (na relação com informações prejudiciais);
- no contato (com atores de risco que integram a mesma rede);
- na conduta (potencialmente danosa, que pode ser observada ou experimentada pela criança/adolescente);

- em relações de contrato (quando na adesão a determinados serviços há contrapartidas impostas aos usuários, que costumam ser desconhecidas destes e resultam na sua exploração).

Por fim, embora a legislação brasileira não imponha o dever de realizar uma avaliação de acesso por crianças e adolescentes, **a construção de um modelo de avaliação de acesso, que seja opcional**, é interessante para facilitar e dirimir dúvidas sobre este processo de compreensão do próprio serviço ou produto em relação ao ECA digital. Um modelo de avaliação de acesso, além de incentivar o cumprimento da legislação, também ajuda a promover o registro e monitoramento periódico das evidências sobre os usos do produto ou serviço.

Síntese das sugestões para definição de acesso provável:

1. Recomenda-se esclarecer a relação (cumulativa, alternativa ou gradual) entre os três critérios elencados no Art. 1º do ECA Digital;
2. Recomenda-se que o critério de facilidade de acesso e uso do produto ou serviço (inciso II) nunca seja considerado isoladamente para configurar acesso provável, a fim de evitar abrangência excessiva e garantir uma aplicação proporcional e racional da Lei;
3. Recomenda-se que o critério de probabilidade de uso e atratividade (inciso I) seja considerado cumulativamente com o critério de facilidade de acesso e uso do produto ou serviço (inciso II) e alternativamente em relação ao critério de significativo grau de risco (inciso III), a fim de garantir uma aplicação proporcional e racional da Lei;
4. Recomenda-se que o critério significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes seja, isoladamente, suficiente para configurar acesso provável e ensejar a aplicação da lei, independentemente da comprovação das situações previstas nos demais incisos, a fim de evitar abrangência excessivamente reduzida e garantir uma aplicação proporcional e racional da Lei;
5. Considera-se que a Agência deve detalhar parâmetros para definir o que é facilidade ou dificuldade de acesso e uso de produto ou serviço (inciso II). Para isso, pode-se indicar quais parâmetros definem o que é aferição de idade altamente eficaz para impedir o acesso por crianças e adolescentes, esclarecendo que sua adoção não é obrigatória para evitar a aplicação da Lei — dado que existem outros critérios em análise (inciso I e III);
6. Recomenda-se que a ANPD estabeleça critérios adicionais e exemplos não exaustivos para definir probabilidade de uso e atratividade (inciso I), considerando a natureza do produto ou serviço, suas funcionalidades, design, estratégia comercial, os benefícios gerados com seu uso, os tipos de conteúdos disponíveis e fontes externas, como dados estatísticos.
7. Recomenda-se que a ANPD defina parâmetros adicionais para o critério de risco a crianças e adolescentes, considerando, especialmente, a matriz de 4Cs, isto é, riscos de: conteúdo, contato, conduta e contrato.

2. Esclarecimentos sobre produto e serviço de tecnologia da informação

A Lei 15.211/2025 aplica-se a produtos ou serviços de tecnologia da informação direcionados ou de uso provável por crianças e adolescentes. O Art. 2º, I do ECA Digital traz uma definição para produtos e serviços de tecnologia da informação que é semelhante à contribuição fornecida pelo CGI.br no Ofício “CGI.br 152/2025” feito em resposta ao ofício enviado pelo Deputado Jadyel Alencar sobre definições do PL 2628/2022¹³. No entanto, a definição sugerida pelo CGI.br que foi adotada — “produto ou serviço fornecido a distância, por meio eletrônico e provido em virtude de requisição individual” — depende ainda de definições complementares de cada um destes elementos para esclarecer a interpretação da Lei.

2.1 Definições complementares para produtos e serviços de tecnologia da informação

A sugestão apresentada pelo CGI.br foi, em grande medida, inspirada pela definição adotada pelo “Age appropriate design: a code of practice for online services” do Reino Unido. Se no Online Safety Act as obrigações relacionadas à proteção de crianças são aplicáveis a “Part 3 services”, isto é, a serviços regulados entre usuários (regulated user-to-user service)¹⁴ ou serviços de busca regulados¹⁵, no caso do código de boas práticas, aplica-se a um “serviço da sociedade da informação relevante”. Em ambos os casos, a regulação (seja pela legislação ou pela regulamentação do poder executivo) define, exemplifica e apresenta exceções para definir quais são estes atores.

No Online Safety Act, a lei prevê algumas exceções a estas definições, isto é, estabelece alguns atores ou funcionalidades que são *user-to-user* ou *search engines*, mas aos quais a lei não se aplica, tais como: serviços de email e de SMS, se forem estes o único conteúdo gerado por usuário disponível no serviço; serviços em que a única possibilidade de conteúdo gerado por usuários são comunicações auditivas em tempo real; serviços internos de empresas, ou serviços providos pelo poder público, dentre outros.

Já o código de condutas britânico define “serviço da sociedade da informação” como: “qualquer serviço normalmente prestado mediante remuneração, à distância, por meios eletrônicos e mediante solicitação individual de um destinatário de serviços”. Sendo cada um dos elementos presentes nessa definição também definidos:

- (i) ‘**at a distance**’ means that the service is provided without the parties being simultaneously present;
- (ii) ‘**by electronic means**’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- (iii) ‘**at the individual request of a recipient of services**’ means that the service is provided through the transmission of data on individual request.” (ICO)¹⁶

Nesse sentido, segundo a ICO, um site que apenas provê informações sobre sua empresa, mas não oferece produtos ou serviços de forma online não seria considerado um serviço da sociedade da

¹³ Cf. <https://cgi.br/publicacao/resposta-do-cgi-br-ao-oficio-n-18-gdja-2025-colaboracao-tecnica-sobre-definicoes-presentes-no-pl-n-2628-2022/>

¹⁴ Entendido como um serviço de Internet por meio do qual o conteúdo gerado diretamente no serviço por um usuário deste serviço, ou carregado ou compartilhado, pode ser encontrado por outro usuário(s).

¹⁵ Serviço de busca é aquele que é ou inclui um mecanismo de busca.

¹⁶ Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code4>

informação, pois não seria fornecido a distância. Assim como serviços tradicionais de telefonia estariam fora, pois não são prestados por meio eletrônico. Ou como serviços gerais de radiodifusão, mesmo que fornecidos via Internet, não seriam solicitados individualmente pelo recipiente do serviço (como uma programação fixa de televisão).

Embora os termos “fornecidos a distância” ou “por meio eletrônico” possam ser entendidos sem explicações adicionais, **o termo “provido em virtude de requisição individual” pode gerar dúvidas entre os regulados, podendo ser melhor definido pela Agência, a semelhança das definições da ICO.**

2.2. Definir parâmetros para o que são as funcionalidades essenciais para o funcionamento da Internet

Assim como o Online Safety Act determina funcionalidades que são *user-to-user services* ou serviços de busca, mas que estão excepcionados da Lei, ou como o Código de boas práticas de design excetua serviços que não são relevantes, o ECA digital esclarece funcionalidades e agentes que não se enquadram na definição, conforme sugestão fornecida pelo CGI.br no “OF. CGI.br 152/2025”:

§ 2º Para os fins desta Lei, não são consideradas produtos ou serviços de tecnologia da informação **as funcionalidades essenciais para o funcionamento da internet**, como os protocolos e os padrões técnicos abertos e comuns que permitem a interconexão entre as redes de computadores que compõem a internet.

O esclarecimento foi feito considerando a conturbada experiência de categorização de agentes no Marco Civil da Internet (MCI) e a ampla definição de “produto e serviço da tecnologia da informação” que pode englobar uma diversidade de atores relacionados à Internet ou ao digital, incorrendo no risco de incluir aqueles que essencialmente apenas operam para o funcionamento técnico da Internet, sem gestão sobre os conteúdos que ali trafegam.

A Internet é um ecossistema complexo com a presença de múltiplos atores com variadas funções para seu funcionamento. O MCI estabelece duas categorias de agentes, os provedores de conexão e os provedores de aplicações de Internet (que estão no escopo do ECA Digital), definido na lei como “o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet” (Art. 5º, VII). No entanto, tal categorização possui lacunas e desafios no endereçamento correto de todos os atores na Internet, suas funções e respectivos deveres e responsabilidades, o que poderia repercutir no ECA Digital, não fosse a exceção adicionada no § 2º.

O principal exemplo de repercussão desta categorização dual é a celeuma arredor do regime de responsabilidade aplicável aos provedores de aplicação, previsto no Art. 19 do MCI. Conforme ressaltado na nota técnica do CGI.br “Tipologia de Provedores de Aplicação”, há, não apenas, diversos tipos de provedores de aplicações com funcionalidades diversas na Internet, como um conjunto de agentes do ecossistema da Internet que desempenham funções essenciais para o funcionamento da Internet e não se enquadram como provedores de conexão, nem provedores de aplicação nos termos do MCI.

Há diversos esquemas para explicar o funcionamento da Internet, mas, conforme a Nota Técnica do CGI.br, um modelo de arquitetura de camadas da Internet pode ser sintetizado em três níveis:

i) a camada de infraestrutura de telecomunicações, que faz referência à rede física (linhas telefônicas, fibra ótica, cabos em geral, ondas de satélite e de rádio, dentre outras) sobre a qual a Internet funciona; **ii) a camada intermediária**, estabelecida sobre a camada de telecomunicações e que, com ela, não se confunde. Trata-se da camada que define a Internet em si e onde está sua linguagem comum (protocolos e padrões técnicos) entre as redes de computadores que compõem a Internet. Tais protocolos e padrões descrevem as funções essenciais para o funcionamento da rede, são abertos e documentados em Requests for Comments (RFC), e produzidos por consenso nos fóruns do Internet Engineering Task Force (IETF)⁵ e; **iii) a camada de aplicações**, onde residem as aplicações de rede e seus protocolos específicos. Nessa última camada, os conteúdos gerados por terceiros são criados e utilizados por aplicações, como o Instagram e o YouTube, construídas sobre a estrutura da Internet.

A camada intermediária compreende os protocolos e os padrões da linguagem comum entre as redes de computadores e é basilar para o funcionamento dos demais componentes da rede, permitindo o desenvolvimento de milhões de aplicações na camada superior da Internet, a camada de aplicações. As funções desenvolvidas na camada intermediária, destaca-se, não utilizam o conteúdo das comunicações para serem executadas, isto é, a forma como tais agentes organizam suas atividades e seus modelos de negócio prescinde do acesso aos conteúdos das comunicações, mas apenas transportam de um servidor a outro.

Assim, para evitar que — em virtude da categorização dual do MCI — deveres formulados inicialmente para provedores de aplicações específicos fossem estendidos para demais atores da rede (que apenas viabilizam o transporte e comunicação de conteúdos sobre a infraestrutura de telecomunicações), **a proteção explícita para a camada intermediária é fundamental**. Em outras palavras, deveres (fundamentais) como a obrigação de tomar medidas razoáveis para prevenir e mitigar o acesso e a exposição a conteúdos nocivos e indevidos a crianças e adolescentes (Art. 6º), ou deveres para realizar avaliação do conteúdo disponibilizado de acordo com faixa etária (Art. 8º), ou de adotar mecanismos para verificação de idade dos usuários, **seriam aplicáveis a atores que não operam sobre os conteúdos e que sequer intermedeiam ou têm contato com os usuários finais**. Seria um incentivo para que atores que fornecem a infraestrutura básica da Internet — da qual diversas aplicações dependem — passassem a interferir ativamente sobre os conteúdos, podendo implicar obrigações desproporcionais e de alto impacto sobre o funcionamento geral da Internet.

Nesse sentido, **é importante que a Agência compreenda e reconheça a diferenciação entre estes atores e funcionalidades, eventualmente, apresentando exemplos de funcionalidades essenciais para o funcionamento da Internet, que estão fora do escopo de aplicação do ECA digital** — tais como o sistema de nomes de domínio, ou funcionalidades de roteamento empregadas por provedores de conexão à Internet, operadores de Pontos de Troca de Tráfego ou IX e CDNs, operação dos protocolos smtp por provedores de serviços de email, dentre outros.

Síntese das recomendações do CGI.br sobre produtos e serviços de tecnologia da informação:

1. Definir parâmetros para a compreensão dos termos “fornecidos a distância” ou “por meio eletrônico” e, especialmente, para o termo “provido em virtude de requisição individual”, considerando como exemplo a experiência da ICO com o Age appropriate design code que possui termos similares (Art. 2º, I).
2. Explicar e exemplificar o que são funcionalidades essenciais para o funcionamento da Internet

que estão fora do escopo de aplicação do ECA digital, considerando especialmente as diferenças entre a camada intermediária — que é basilar para o funcionamento dos demais componentes da rede — e a camada de aplicações, conforme as recomendações dadas pelo CGI.br neste documento e na Tipologia de Provedores de Aplicações.

3. Esclarecimentos sobre a aplicação modulada de obrigações de acordo com o grau de interferência sobre o conteúdo de terceiro (Art. 39)

O Art. 39 do ECA Digital define que determinadas obrigações serão aplicadas “conforme as características e as funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o grau de interferência do fornecedor do produto ou serviço sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor”. Tal dispositivo tem como inspiração a contribuição do CGI.br feita no Ofício “CGI.br 152/2025”, que, por sua vez, baseou-se na Nota Técnica do CGI.br “Tipologia dos Provedores de Aplicações”. A tipologia dispõe sobre a necessária diferenciação entre provedores de aplicação por meio das funcionalidades oferecidas por esses agentes e contribui, não apenas para a correta especificação de regimes de responsabilidade, mas também para a especificação de quaisquer obrigações regulatórias de forma a não comprometer a estabilidade e o desenvolvimento da Internet e, ao mesmo tempo, assegurar a devida proteção aos direitos fundamentais de usuários.

Nesse sentido, é importante que a regulamentação esclareça o que é:

- i) interferência sobre o circulação de conteúdo de terceiro; e
- ii) defina parâmetros para a aplicação modulada das aplicações de forma a não restringir direitos e sem diminuir o grau de proteção às crianças e adolescentes.

Em outras palavras, a regulamentação “definirá critérios objetivos para a aferição do grau de intervenção e para a aplicação proporcional das obrigações previstas neste artigo” (Art. 39, § 3º).

3.1. Interferência sobre a circulação de conteúdo de terceiro (“critérios objetivos para a aferição do grau de intervenção”)

No entendimento do CGI.br, a interferência sobre o fluxo do conteúdo de terceiro tornou-se um demarcador fundamental na atribuição de responsabilidade e obrigações para um provedor de acordo com suas funcionalidades. Na tipologia, o CGI.br elenca três tipos de provedores de aplicação que podem auxiliar na especificação de uma regulação assimétrica e proporcional. São estes:

- i) Provedores de aplicação com funcionalidades sem interferência sobre a circulação de conteúdo de terceiros:** atuam na Internet como simples meio de transporte e armazenamento. Esses agentes caracterizam-se por desempenhar funcionalidades que não interferem sobre o fluxo de conteúdo de terceiros, podendo ser classificados pelo entendimento de que são passivos ou agnósticos em relação a eles. Exemplos são provedores de aplicações que oferecem funcionalidade de certificação, hospedagem de sites, envio e recebimento de e-mail, envio e recebimento de mensagens de texto, dentre outras. Tais provedores podem promover ações sobre os conteúdos de terceiros voltadas exclusivamente para a segurança e a estabilidade do serviço que oferecem.
- ii) Provedores de aplicação com funcionalidades de baixa interferência sobre a circulação de conteúdo de terceiros:** oferecem funcionalidades na Internet que exercem

baixa interferência sobre o fluxo de conteúdo de terceiros, sem o emprego de recomendações baseadas em perfilização e com reduzida capacidade de geração de riscos. Exemplos são provedores com funcionalidade de curadoria de conteúdos para registro histórico, funcionalidades de participação social pública, edição de artigos e verbetes, dentre outros.

iii) Provedores de aplicação com funcionalidades de alta interferência sobre a circulação de conteúdo de terceiros: oferecem funcionalidades com alta interferência no fluxo de conteúdos gerados por terceiros, constituindo atividade de risco. Tais agentes organizam e distribuem os conteúdos por meio do emprego de técnicas de coleta e tratamento de dados para perfilização, difusão em massa, recomendação algorítmica, microsegmentação, estratégias de incentivo ao engajamento contínuo, impulsionamento próprio ou pago, publicidade direcionada, dentre outras. Ainda que essa intermediação, por vezes, seja benéfica aos atores envolvidos, as atividades desses provedores oferecem riscos, considerando seus incentivos e a forma como são realizadas. Exemplos de funcionalidades que promovem alta interferência na circulação e na disponibilidade de conteúdos produzidos por terceiros são os sistemas de impulsionamento e recomendação de conteúdo baseados em perfilização, veiculação de anúncios, propaganda programática etc (CGI.br, 2025).

Essas diferenciações, que consideram a operação, os efeitos e riscos de cada provedor, foram utilizadas para guiar a imposição de deveres de acordo com as funcionalidades oferecidas por cada provedor. Embora a proteção da criança e adolescente seja uma responsabilidade compartilhada entre todos, **a sugestão do CGI.br foi feita para que os deveres que envolvem maior intervenção ao conteúdo sejam direcionados, isto é, aplicáveis de forma proporcional àqueles que têm funcionalidades com maior interferência sobre o conteúdo, de forma a evitar transformações e obstáculos indesejados no desenvolvimento da Internet brasileira e sob pena de impor deveres excessivos e tecnicamente inviáveis.**

De forma prática, seria tecnicamente difícil ou inviável que provedores de aplicações que oferecem funcionalidades como simples hospedagem de sites — sem interferência sobre a disposição e visibilidade de quais conteúdos aparecem para quais usuários — passassem a determinar quais conteúdos de seu cliente (sites por ele hospedados) deveriam aparecer mais ou menos (ou não aparecer) para cada faixa etária. Isso porque este provedor de aplicações apenas configura um servidor web para hospedar sites para que terceiros possam dispor seus conteúdos, diferentemente de aplicações como as redes sociais que já interferem sobre conteúdo para determinar o que é mais ou menos visualizado e, portanto, têm capacidade técnica para interferir de acordo com os parâmetros legais. Destaca-se que, caso o mesmo provedor (a exemplo da hospedagem de sites) ofereça funcionalidade de espaço para publicidade direcionada, neste caso, entende-se que os deveres listados em questão podem ser aplicáveis no âmbito desta funcionalidade específica, dado que há interferência sobre a circulação dos conteúdos de terceiros.

Essa recomendação foi feita a um conjunto de obrigações relacionadas a moderação de conteúdos de terceiros, presente nos arts. 6º, 8º e 11 do Projeto de Lei no. 2628/22 (atuais 6º, 8º e 17), que tratam, respectivamente, de: ações para prevenir ou mitigar o acesso a determinados conteúdos; deveres para avaliação de conteúdo por faixa etária e de mecanismos para impedir o seu encontro e; ferramentas para limitar visibilidade de conteúdos, ou controlar sistemas de recomendação. No entanto, **a recomendação foi expandida para uma série de outras obrigações**, inclusive a obrigações que inerentemente envolvem interferência sobre o conteúdo, vez que se tratam de conteúdos do próprio provedor.

No mesmo sentido, a recomendação foi incorporada sem explicitar que a interferência em questão é referente à circulação sobre o **conteúdo de terceiro**. Vale retomar a sugestão do CGI.br para inclusão da seguinte definição:

Interferência sobre a circulação de conteúdos de terceiro: corresponde a qualquer ação tomada pelo provedor de aplicações que altere a disposição, a circulação e a distribuição do conteúdo de terceiros, isto é, quaisquer ações tomadas para ampliar ou reduzir alcance, para exibir ou ocultar conteúdos de terceiro.

A demarcação de que o conteúdo é de terceiro é fundamental, pois eventual flexibilização de obrigação ou responsabilidade apenas se justifica pelo fato de o provedor não possuir interferência sobre este conteúdo disponibilizado no site. Contudo, **quando o conteúdo é do próprio provedor — como no caso de jogos eletrônicos ou de apostas online —, logicamente sempre há interferência sobre o conteúdo, dado que o conteúdo foi produzido e gerenciado por ele, devendo operar a lógica de responsabilidade civil tradicional e não havendo qualquer razão para modulação**. Caso contrário, estabelecer-se-ia uma flexibilização ainda maior que a prevista no Art. 19 do Marco Civil da Internet — que possui justificativas como a proteção da liberdade de expressão dos usuários (terceiros).

Nesse sentido, **o CGI.br recomenda que a regulamentação, na definição de critérios objetivos para a aferição do grau de intervenção sobre o conteúdo, esclareça que a interferência tratada no Art. 39 é relativa apenas aos conteúdos de terceiro**, vez que não há justificativa plausível para estendê-la a conteúdos próprios do fornecedor do produto ou serviço, pois estes possuem total controle (e, portanto, deveres e responsabilidades integrais) sobre o conteúdo veiculado.

Ademais, **recomenda-se que os parâmetros de número de usuários e o porte do fornecedor — não recomendados pelo CGI.br e que foram adicionados para a modulação das obrigações citadas — não sejam utilizados de maneira a diminuir o grau de proteção às crianças e adolescentes proposto pelo ECA digital**. Isso significa que mesmo fornecedores pequenos de produtos e serviços com baixo número de usuários, mas com atividades de alto risco, não devem ter suas obrigações flexibilizadas.

3.2. Critérios para a aplicação proporcional das obrigações previstas

Como mencionado, em ofício, o CGI.br havia recomendado modular os deveres previstos no PL às capacidades técnicas de cada provedor de aplicação para obrigações específicas relacionadas à prevenção ou mitigação do acesso a determinados conteúdos; avaliação de conteúdo por faixa etária e mecanismos para impedir o seu encontro e; ferramentas para limitar visibilidade de conteúdos, ou controle de sistemas de recomendação — em suma, situações que envolvem necessariamente alta interferência sobre o conteúdo de terceiro. A modulação de acordo com o grau de interferência foi aplicada a duas das situações sugeridas (prevenir ou mitigar o acesso a determinados conteúdos e ferramentas de controle parental para controlar sistemas de recomendação personalizados) e ampliada para outros deveres e situações NÃO sugeridas pelo CGI.br:

- Art. 17 e 18: ferramentas de supervisão parental (não apenas à sugestão inicial sobre ferramentas para controle de recomendação algorítmica)
- Art. 19: aos produtos ou serviços de monitoramento infantil (inviolabilidade dos dados e informe sobre a realização do monitoramento)

- Art. 20: aos jogos eletrônicos, com delimitações para caixas de recompensa;
- Art. 27: dever de comunicar os conteúdos de aparente exploração, abuso sexual, sequestro e aliciamento detectados em seus produtos ou serviços às autoridades nacionais e internacionais competentes;
- Art. 28: mecanismos de notificações (denúncia) sobre violações;
- Art. 29: dever de proceder à retirada de conteúdos independente de ordem judicial, após notificação por determinados atores;
- Art. 31: dever de elaborar relatórios semestrais, para provedores com mais de um milhão de usuários;
- Art. 32: adotar mecanismos eficazes para a identificação de uso abusivo dos instrumentos de denúncia;
- Art. 40: obrigação de representação legal no país.

Destaca-se, a seguir, algumas situações que são incompatíveis com a aplicação da modulação de acordo com o grau de interferência sobre o conteúdo, pois se tratam de situações que não envolvem a circulação de conteúdos de terceiro. Em geral, observa-se como um dos critérios objetivos que podem ser estabelecidos pela regulamentação (§ 3º), que a modulação de obrigação de acordo com o grau de interferência apenas pode ocorrer quando há conteúdo de terceiro.

A) Deveres para produtos ou serviços de monitoramento infantil não devem ser modulados

Os deveres previstos no Art. 19 para produtos ou serviços de monitoramento infantil são relativos a garantir a inviolabilidade dos dados das crianças e adolescentes monitorados (imagens, sons e outras informações) e à necessidade de informar crianças e adolescentes sobre a realização do monitoramento. Não há qualquer relação entre a interferência ou não sobre o conteúdo de terceiro e o dever de inviolabilidade dos dados ou a necessidade de transparência, pelo contrário, tratam-se de direitos fundamentais (já positivados) de proteção de dados pessoais que não podem ser flexibilizados. O tratamento destes dados depende de ações de coleta, processamento e transferência, diferindo das situações e objetivos que justificam a modulação pela interferência — não há, por exemplo, a necessidade de evitar impactos injustos sobre a produção de conteúdo de terceiro, pois não há esta produção de conteúdo, mas apenas uma coleta constante de dados em que o titular dos dados age passivamente.

Nesse sentido, considerando a prerrogativa dada pela legislação para o estabelecimento de critérios para a aplicação proporcional das obrigações (Art. 39, § 3º), **o CGI.br recomenda que não seja aplicada a modulação dos deveres de inviolabilidade de dados e de informação direcionados aos fornecedores de produtos ou serviços de monitoramento infantil, sob pena de prejudicar a proteção de dados de crianças e adolescentes.**

A) Deveres para jogos eletrônicos não devem ser modulados

A vedação de caixas de recompensa em jogos eletrônicos direcionados a crianças e a adolescentes ou de acesso provável por eles tampouco envolve conteúdo de terceiro. O fornecedor destes jogos possuem total controle sobre as funcionalidades oferecidas e, portanto, capacidade para oferecer ou deixar de oferecer caixas de recompensa, não havendo qualquer justificativa razoável para modular esta obrigação de acordo com o grau de interferência sobre a circulação de conteúdo de terceiro.

Nesse sentido, **o CGI.br recomenda que não seja aplicada a modulação dos deveres de vedação de caixas de recompensa, sob pena de gerar o descumprimento da Lei, criar mecanismos de vulnerabilidades a crianças e adolescentes** e prejudicar seu desenvolvimento biopsicossial.

C) Deveres de transparência podem ser modulados apenas quando estiverem relacionados à moderação de conteúdo

O Art. 31 já estabelece uma modulação de acordo com a quantidade de usuários (mais de um milhão). Em seus incisos, há diversas obrigações que não são relativas à moderação de conteúdos de terceiro. A obrigação relativa à transparência sobre aprimoramentos técnicos para a proteção de dados pessoais ou para o consentimento parental, por exemplo, não têm relação com o racional da interferência sobre conteúdo de terceiro.

Nesse sentido, entende-se que o racional da modulação de obrigação de acordo com interferência sobre conteúdo de terceiro pode ser aplicado apenas quando envolverem deveres de transparência relacionados à moderação de conteúdo — isto é, aos incisos I e III do Art. 31.

E) Representação legal no país não deve ser modulada de acordo com a interferência sobre o conteúdo de terceiro

O dever de representação legal no país pode ser modulado por critérios como quantidade de usuários e porte, mas não tem conexão com o racional envolvido na modulação por conteúdo de terceiro, não devendo este ser aplicado.

Em síntese, recomenda-se as seguintes recomendações neste tema:

1. O CGI.br recomenda que a regulamentação esclareça que a interferência tratada no Art. 39 é relativa apenas aos conteúdos de terceiro, vez que não há justificativa plausível para estendê-la a conteúdos próprios do fornecedor, pois estes são integralmente responsáveis pelos produtos ou serviços que ofertam.
2. Recomenda-se que os parâmetros de número de usuários e o porte do fornecedor — não recomendados pelo CGI.br e que foram adicionados para a modulação das obrigações citadas — não sejam utilizados de maneira a diminuir a proteção às crianças e adolescentes proposta pelo ECA digital.
3. Recomenda-se que não seja aplicada qualquer modulação aos deveres de inviolabilidade de dados e de informação, direcionados aos fornecedores de produtos ou serviços de monitoramento infantil, e aos deveres de vedação de caixas de recompensa, sob pena de prejudicar a proteção das crianças e adolescentes.
4. Considera-se que os relatórios de transparência podem ser parcialmente modulados de acordo com a interferência sobre o conteúdo de terceiro apenas em relação às questões de moderação de conteúdo (incisos I e III, pois envolvem conteúdos de terceiro)
6. Considera-se que o dever de representação legal no país pode ser modulado por critérios como quantidade de usuários e porte, mas não tem conexão com o racional envolvido na modulação por conteúdo de terceiro, não devendo este ser aplicado.

4. Medidas para a suspensão temporária de atividades e para a proibição de exercício das atividades

Destaca-se que há termos e conceitos acerca das medidas de suspensão e proibição de exercício de atividades a serem melhor definidos e complementados. No entanto, tais esclarecimentos serão feitos em tomada de subsídios ou consulta pública referente à dosimetria e sancionamento.

TOMADA DE SUBSÍDIOS

ECA DIGITAL | DEZ/2025

ANEXO

O presente anexo, elaborado pela área de Privacidade e Inteligência Artificial do escritório **BECKER BRUZZI & LAMEIRÃO ADVOGADOS (“BBL Advogados”)**, tem por objetivo contribuir para a interpretação e a aplicação do Estatuto Digital da Criança e do Adolescente (“ECA Digital”) por meio do esclarecimento de conceitos, termos e expressões que desempenham papel estruturante no regime jurídico instituído pela Lei nº 15.211/2025.

A proposta parte do reconhecimento de que a efetividade da proteção conferida pela norma depende de definições suficientemente precisas para orientar a atuação regulatória, a fiscalização e o desenho responsável de produtos e serviços digitais, sem comprometer a proporcionalidade, a viabilidade tecnológica e a liberdade de expressão.

Os conceitos a seguir são analisados de forma autônoma, com indicação dos dispositivos legais correlatos, identificação das principais ambiguidades interpretativas e proposição de parâmetros técnicos, objetivos e baseados em risco, capazes de conferir maior previsibilidade jurídica e coerência sistêmica à aplicação do Estatuto.

1. ACESSO PROVÁVEL POR CRIANÇAS E ADOLESCENTES (ART. 3º, I E § 1º)

O conceito de “acesso provável” por crianças e adolescentes é o eixo estruturante do ECA Digital, pois define quando produtos e serviços de tecnologia da informação que não são explicitamente destinados ao público infantojuvenil passam, ainda assim, a se submeter ao regime especial de obrigações previsto na Lei nº 15.211/2025. Trata-se, portanto, de um conceito de incidência normativa, cujo grau de precisão impacta diretamente a segurança jurídica, a proporcionalidade regulatória e a capacidade de fiscalização da autoridade competente. Se interpretado de forma excessivamente ampla ou subjetiva, o conceito tende a expandir o alcance do Estatuto para praticamente todo o ecossistema digital, diluindo a proteção efetiva nos cenários de maior risco e gerando custos regulatórios desnecessários. Por outro lado, se interpretado de forma excessivamente restritiva, pode permitir que serviços com riscos relevantes escapem do regime protetivo.

A própria redação legal indica que o “acesso provável” não se confunde com a mera possibilidade abstrata de uso por crianças e adolescentes. O Estatuto não adota uma lógica de acesso potencial universal, mas sim um teste qualificado, baseado em três elementos distintos: a probabilidade e atratividade do uso por esse público, a facilidade de acesso e utilização do serviço, e a existência de risco significativo à privacidade, à segurança ou ao desenvolvimento biopsicossocial. Esses elementos não são redundantes e não cumprem a mesma função normativa. Por essa razão, a interpretação mais coerente com a sistemática da lei é a de que esses critérios devem ser aplicados de forma cumulativa, e não alternativa. Cada um deles atua como um filtro sucessivo, evitando que o enquadramento decorra de impressões genéricas ou de juízos morais sobre o ambiente digital.

Do ponto de vista operacional, a aferição da probabilidade de uso deve se apoiar prioritariamente em evidências observáveis e verificáveis, e não em presunções abstratas. Parâmetros adequados incluem dados sobre usuários ativos mensais no Brasil, estimativas da proporção de crianças e adolescentes na base de usuários, informações provenientes de relatórios de transparência, métricas internas auditáveis, dados de mercado ou sinais etários fornecidos por sistemas operacionais e lojas de aplicativos quando disponíveis. A atratividade, por sua vez, deve ser analisada a partir de características objetivas do produto ou serviço, como linguagem, design visual, mecânicas de engajamento, temas abordados, estratégias de marketing, canais de divulgação e elementos funcionais que indiquem direcionamento ou apelo específico ao público infantojuvenil. Não se trata de avaliar se crianças eventualmente gostam do serviço, mas se ele é concebido, promovido ou estruturado de modo a capturar esse público.

A facilidade de acesso e utilização constitui um terceiro eixo autônomo e fundamental. Mesmo que haja interesse ou presença residual de crianças, a existência de fricções relevantes pode afastar o enquadramento como acesso provável. Nesse ponto, devem ser considerados fatores como exigência de verificação etária, necessidade de mediação adulta, dependência de instrumentos financeiros, controles de supervisão parental, restrições de funcionalidades por idade, barreiras técnicas de cadastro e limites à interação com outros usuários. Serviços que implementam mecanismos eficazes de controle e mediação reduzem de forma concreta a facilidade de acesso autônomo por crianças e adolescentes, o que deve ser reconhecido como elemento mitigador na análise regulatória.

Por fim, o conceito de “acesso provável” exige a presença de risco significativo, entendido não como risco hipotético ou genérico, mas como a possibilidade concreta de dano relevante. Esse risco deve ser avaliado a partir das funcionalidades do serviço e da natureza dos dados tratados, considerando fatores como interação social em larga escala, sistemas de recomendação personalizados, práticas de monetização e publicidade, coleta de dados sensíveis ou de geolocalização, e dinâmicas que possam intensificar exposição a conteúdos inadequados, exploração comercial ou impactos negativos ao bem-estar psicológico. A análise deve conjugar severidade e probabilidade do dano, evitando presunções automáticas baseadas apenas no fato de o serviço ser digital, social ou amplamente utilizado.

A conceituação que se propõe, portanto, é a de que o “acesso provável” por crianças e adolescentes se caracteriza quando, no contexto brasileiro, coexistem evidências verificáveis de uso relevante por esse público, ausência ou insuficiência de fricções e mecanismos de controle que dificultem o acesso autônomo, e riscos concretos decorrentes das funcionalidades, da arquitetura ou das práticas do serviço. Essa leitura permite uma aplicação responsiva e baseada em risco, compatível com a lógica de proporcionalidade adotada pelo próprio Estatuto, reconhece a relevância das medidas de adequação já implementadas pelos fornecedores e evita incentivos perversos à sobrecoleta de dados apenas para fins defensivos. Ao mesmo tempo, preserva o núcleo protetivo da lei e direciona a atuação regulatória para os cenários em que a intervenção é efetivamente necessária.

2. ANÁLISE EMOCIONAL (ART. 19, III)

A “análise emocional” é um dos conceitos mais sensíveis e, ao mesmo tempo, mais tecnicamente indeterminados do ECA Digital, justamente porque se localiza na fronteira entre tratamentos de dados tradicionalmente aceitos no ecossistema digital e práticas emergentes de inferência altamente invasivas. O Estatuto veda expressamente o uso de análise emocional para fins de direcionamento de publicidade comercial a crianças e adolescentes, mas não delimita de forma suficiente o que deve ser compreendido como “análise emocional”, nem quais técnicas, níveis de inferência ou efeitos práticos caracterizam essa prática para fins regulatórios. Essa ausência de precisão cria o risco de interpretações expansivas que acabem por abranger operações legítimas de detecção de sinais, classificação de conteúdo ou moderação de riscos, que não se confundem com exploração emocional.

A necessidade de esclarecimento decorre do fato de que o termo “análise emocional” não possui definição técnica unívoca. Ele pode abarcar desde sistemas sofisticados de inferência de estados emocionais internos, baseados em múltiplas fontes de dados e modelos preditivos complexos, até mecanismos rudimentares de categorização contextual, como a identificação de palavras associadas a tristeza, violência ou sofrimento em textos ou imagens, com finalidade exclusivamente protetiva. Tratar essas realidades como equivalentes do ponto de vista jurídico compromete a coerência do regime regulatório e pode gerar incentivos negativos, como a retração de ferramentas voltadas à segurança, ao bem-estar ou à prevenção de danos psicossociais.

Para tornar o conceito operacional e compatível com a finalidade protetiva da lei, é essencial adotar parâmetros que diferenciem a análise emocional relevante para fins de vedação daquelas práticas que, embora envolvam sinais afetivos, não produzem inferências individualizadas ou exploratórias. Um primeiro parâmetro central é a finalidade do tratamento. A “análise emocional” deve ser compreendida como juridicamente relevante quando utilizada para influenciar decisões de consumo, direcionar publicidade, modular estímulos comerciais ou explorar vulnerabilidades emocionais de crianças e adolescentes. Em contrapartida, análises destinadas à moderação de conteúdo, à detecção de risco de automutilação ou suicídio, à identificação de interações abusivas ou à adequação etária da experiência digital não se enquadram no mesmo patamar de risco e devem ser tratadas de forma distinta.

Outro parâmetro indispensável diz respeito ao grau de inferência e à natureza dos dados utilizados. A análise emocional de alto risco caracteriza-se pela construção de inferências internas sobre estados psicológicos, humor, impulsividade, fragilidade emocional ou propensão comportamental, especialmente quando essas inferências são persistentes, cumulativas ou associadas a identificadores individuais. Técnicas que combinam múltiplos sinais biométricos, comportamentais ou contextuais para produzir escores emocionais individualizados apresentam risco substancialmente maior do que classificações pontuais, transitórias ou agregadas, baseadas em padrões genéricos de conteúdo. A presença de modelos preditivos que extrapolam sinais observáveis para inferir estados mentais não diretamente verificáveis

deve ser considerada um elemento qualificante da análise emocional para fins regulatórios.

A mensuração do impacto da análise emocional sobre a criança ou o adolescente constitui outro eixo relevante. A prática torna-se especialmente sensível quando as inferências emocionais produzem efeitos concretos sobre a experiência do usuário, como alteração de fluxos de conteúdo, intensificação de estímulos, priorização de mensagens comerciais ou modulação de recompensas e notificações. Quanto maior o grau de influência exercido sobre o comportamento, maior deve ser o rigor na avaliação da licitude e da compatibilidade da prática com o melhor interesse da criança e do adolescente. A ausência de transparência, a impossibilidade de desativação e a falta de mediação parental reforçam esse risco e devem ser consideradas agravantes na análise regulatória.

A conceituação que se propõe, portanto, é a de que o termo “análise emocional”, para fins do Estatuto, deve ser entendido como o tratamento de dados pessoais ou comportamentais destinado a inferir, de forma automatizada ou sistemática, estados emocionais ou psicológicos individualizados de crianças e adolescentes, especialmente quando essas inferências são utilizadas para direcionamento publicitário, monetização, impulsionamento de conteúdo ou exploração comercial da atenção. Essa leitura preserva a coerência com a lógica de proteção reforçada adotada pela lei, evita a proibição indiscriminada de ferramentas voltadas à segurança e ao bem-estar e permite que a atuação regulatória se concentre nas práticas que efetivamente instrumentalizam a vulnerabilidade emocional como ativo econômico. Ao mesmo tempo, fornece parâmetros claros para a fiscalização e para o desenho de soluções técnicas responsáveis, alinhadas à LGPD e ao princípio da proporcionalidade.

3. PRODUTO OU SERVIÇO DIRECIONADO A CRIANÇAS E ADOLESCENTES (ART. 3º, I, CAPUT)

O conceito de “produto ou serviço direcionado a crianças e adolescentes” é central para a arquitetura do Estatuto Digital da Criança e do Adolescente, pois delimita o campo de incidência mais intenso das obrigações previstas na Lei nº 15.211/2025. Diferentemente do conceito de “acesso provável”, que opera como um critério de incidência por risco, o direcionamento pressupõe uma escolha deliberada do fornecedor quanto ao público-alvo do produto ou serviço. A ausência de maior precisão sobre o que caracteriza esse direcionamento cria, contudo, um risco relevante de sobreposição com o termo “acesso provável”, bem como de interpretações excessivamente subjetivas que podem desconsiderar a intencionalidade do agente econômico e as características objetivas da oferta.

A necessidade de esclarecimento decorre do fato de que, no ambiente digital, crianças e adolescentes podem acessar praticamente qualquer serviço disponível na internet, o que torna inadequada qualquer leitura que equipare uso eventual ou presença residual de usuários infantojuvenis ao direcionamento propriamente dito. O Estatuto não adota uma lógica de responsabilização universal baseada na mera acessibilidade técnica, mas distingue, de forma consciente, produtos e serviços concebidos para

crianças e adolescentes daqueles que apenas apresentam risco de acesso por esse público. Confundir esses planos normativos compromete a proporcionalidade do regime regulatório e desestimula o desenvolvimento de soluções responsáveis que, embora não voltadas ao público infantojuvenil, implementam medidas robustas de proteção.

Para que o conceito de direcionamento seja aplicado de forma consistente, é necessário adotar parâmetros objetivos que permitam identificar a intenção comunicacional, funcional e comercial do produto ou serviço. Entre esses parâmetros, destacam-se elementos de design e experiência do usuário, como uso predominante de linguagem infantil ou juvenil, personagens, cores, animações e narrativas típicas do universo infantojuvenil, bem como mecânicas de engajamento associadas a jogos, recompensas visuais ou estímulos simplificados. Também são relevantes as escolhas editoriais e funcionais, como conteúdos educativos voltados a faixas etárias específicas, ausência de temas adultos, limitação deliberada de interações abertas e estruturação da experiência com base em mediação parental como elemento central.

Outro parâmetro fundamental reside nas estratégias de comunicação, marketing e distribuição do produto ou serviço. A veiculação de publicidade em canais majoritariamente frequentados por crianças e adolescentes, o uso de influenciadores infantis ou juvenis, a adoção de mensagens promocionais voltadas diretamente a esse público e a presença em ambientes educacionais ou recreativos infantis constituem indícios relevantes de direcionamento. Da mesma forma, classificações etárias atribuídas pelo próprio fornecedor ou por autoridades competentes, bem como descrições em lojas de aplicativos que indiquem público-alvo infantojuvenil, devem ser consideradas elementos objetivos na análise regulatória.

O modelo de negócio e as funcionalidades oferecidas também contribuem para a caracterização do direcionamento. Produtos e serviços que pressupõem, por sua própria arquitetura, a participação ativa de crianças ou adolescentes, como plataformas educacionais infantis, jogos voltados a determinadas faixas etárias ou aplicações concebidas para uso escolar ou recreativo juvenil, apresentam um grau de direcionamento significativamente distinto daquele de serviços generalistas com público amplo e heterogêneo. Nesse ponto, a análise deve considerar se a experiência principal foi desenhada para atender às necessidades, capacidades cognitivas e expectativas típicas do público infantojuvenil, e não apenas se o serviço é compatível com esse público.

A conceituação que se propõe, portanto, é a de que um “produto ou serviço direcionado a crianças e adolescentes” é aquele cuja concepção, comunicação, design funcional e estratégia de distribuição revelam de forma objetiva e consistente a intenção de atender prioritariamente esse público, independentemente da presença eventual de usuários adultos. Essa definição permite distinguir o direcionamento deliberado da mera acessibilidade técnica, preserva a lógica de proporcionalidade do Estatuto e evita que obrigações mais gravosas sejam automaticamente impostas a serviços generalistas que adotam medidas adequadas de proteção. Ao mesmo tempo, assegura que produtos efetivamente concebidos para crianças e adolescentes estejam sujeitos a um regime reforçado de

salvaguardas, compatível com o grau de vulnerabilidade envolvido e com o melhor interesse da criança e do adolescente.

4. RISCO SIGNIFICATIVO AO DESENVOLVIMENTO BIOPSIKOSSOCIAL (ART. 3º, I; ART. 4º; ART. 6º, CAPUT)

O conceito de “risco significativo ao desenvolvimento biopsicossocial” opera como critério transversal para a incidência, a intensidade e a modulação de diversas obrigações previstas na Lei nº 15.211/2025. Trata-se de um conceito normativo aberto, que conecta a lógica de proteção integral da criança e do adolescente a avaliações de risco próprias do ambiente digital, mas que, sem parâmetros suficientemente claros, pode resultar em interpretações excessivamente amplas, subjetivas ou moralizantes, com impacto direto sobre a previsibilidade regulatória e a proporcionalidade das medidas exigidas dos fornecedores.

A necessidade de esclarecimento decorre do fato de que o desenvolvimento biopsicossocial é um processo complexo, multifatorial e fortemente influenciado por contextos sociais, culturais e individuais. No ambiente digital, praticamente toda interação pode, em tese, produzir algum efeito sobre o desenvolvimento cognitivo, emocional ou social de crianças e adolescentes. Se qualquer impacto potencial for tratado como risco significativo, o conceito perde capacidade discriminatória e deixa de cumprir sua função regulatória de priorização dos cenários de maior gravidade. O Estatuto, contudo, não se orienta por uma lógica de risco abstrato ou meramente especulativo, mas pela identificação de riscos relevantes, concretos e proporcionais às funcionalidades e práticas adotadas.

Para que o conceito seja aplicado de forma consistente, é fundamental distinguir risco significativo de risco residual ou ordinário. O risco significativo deve ser compreendido como aquele que, dadas as características do produto ou serviço, apresenta probabilidade não desprezível de causar danos relevantes ao desenvolvimento físico, psicológico ou social da criança ou do adolescente, considerados tanto a severidade do potencial dano quanto a frequência e a intensidade da exposição. Essa análise exige uma abordagem baseada em evidências, e não em percepções genéricas sobre a tecnologia ou em juízos morais sobre determinados conteúdos ou comportamentos.

Entre os parâmetros mais adequados para a avaliação do risco significativo estão, em primeiro lugar, as funcionalidades do serviço. Produtos ou serviços que envolvem interação social em larga escala, comunicação direta com desconhecidos, sistemas de recomendação personalizados, monetização de atenção, publicidade direcionada ou coleta extensiva de dados comportamentais apresentam, em regra, maior potencial de risco do que aplicações de uso passivo, com conteúdo editorial controlado ou com forte mediação adulta. A arquitetura do serviço, portanto, deve ser considerada elemento central na análise, inclusive para diferenciar riscos inerentes ao modelo de negócio daqueles mitigáveis por design.

Outro parâmetro relevante diz respeito ao tipo de conteúdo ou prática potencialmente associada ao risco. A exposição reiterada a conteúdos que promovam automutilação, transtornos alimentares, violência extrema,

sexualização precoce, exploração comercial abusiva ou comportamentos de alto risco constitui cenário qualitativamente distinto de conteúdos sensíveis, controversos ou simplesmente inadequados a determinadas faixas etárias. A distinção entre conteúdos ilícitos, conteúdos nocivos e conteúdos meramente sensíveis é essencial para evitar que o conceito de risco significativo seja utilizado como fundamento genérico para remoções excessivas ou para restrições desproporcionais à liberdade de expressão.

A análise do risco também deve considerar a idade, o estágio de desenvolvimento e o contexto de uso da criança ou do adolescente. O mesmo produto ou funcionalidade pode representar níveis distintos de risco a depender da faixa etária, do grau de autonomia, da presença de mecanismos de supervisão parental e das medidas de proteção já implementadas. Nesse sentido, a existência de controles parentais eficazes, configurações padrão protetivas, limites de tempo de uso, restrições de interação e mecanismos de denúncia acessíveis deve ser reconhecida como fator de mitigação relevante, reduzindo o grau de risco residual associado ao serviço.

A conceituação que se propõe, portanto, é a de que o “risco significativo ao desenvolvimento biopsicossocial” deve ser entendido como a probabilidade concreta de ocorrência de danos relevantes à saúde física, mental ou social de crianças e adolescentes, decorrentes das funcionalidades, práticas ou modelos de negócio de produtos e serviços digitais, considerada a combinação entre severidade do dano, frequência da exposição e existência de medidas de mitigação eficazes. Essa leitura permite uma aplicação calibrada e baseada em risco do Estatuto, evita generalizações que esvaziam o conceito e direciona a atuação regulatória para os cenários em que a intervenção estatal é efetivamente necessária. Ao mesmo tempo, assegura que a proteção integral seja implementada de forma racional, técnica e compatível com a diversidade de contextos do ecossistema digital.

5. INTERAÇÃO SOCIAL EM LARGA ESCALA (ART. 3º, I; ART. 6º, § 1º)

A interação social é um elemento estrutural de muitos produtos e serviços digitais contemporâneos, mas, quando combinada com escala, automação e baixa mediação, passa a assumir relevância jurídica própria no contexto da proteção de crianças e adolescentes. O ECA Digital faz referência explícita à interação social em larga escala como fator de risco, especialmente para fins de caracterização do acesso provável e da avaliação do risco ao desenvolvimento biopsicossocial, sem, contudo, delimitar de forma clara quando a interação deixa de ser episódica ou controlada e passa a configurar um ambiente estruturalmente mais arriscado. Essa indeterminação pode levar tanto à banalização do conceito quanto à sua aplicação indiscriminada a qualquer funcionalidade comunicacional.

O ponto central que demanda esclarecimento é que a interação social em larga escala não se confunde com a simples possibilidade de comunicação entre usuários. O risco regulatório não decorre da interação em si, mas da combinação entre volume, alcance, anonimato relativo, baixa fricção de contato e ausência de mediação eficaz. Serviços que permitem a exposição contínua a um número indeterminado de usuários, especialmente

desconhecidos, ampliam significativamente os riscos de assédio, aliciamento, exploração, manipulação social e exposição a conteúdos inadequados. Esses riscos são potencializados quando a arquitetura do serviço favorece a descoberta algorítmica de perfis, a amplificação de interações ou a comunicação direta sem filtros proporcionais à idade.

Para que o conceito seja aplicado de forma objetiva, é necessário adotar parâmetros que permitam diferenciar interações sociais estruturais de interações limitadas ou controladas. Entre os parâmetros mais relevantes estão o número potencial de interlocutores acessíveis a uma criança ou adolescente, a existência de mecanismos de descoberta ativa ou passiva de usuários, a possibilidade de envio de mensagens não solicitadas, a presença de chats públicos ou semiabertos e o grau de persistência das interações. Funcionalidades que permitem comunicação apenas entre contatos previamente aprovados, em ambientes fechados ou mediados por responsáveis, apresentam um perfil de risco substancialmente distinto de plataformas que incentivam interações abertas, randômicas ou baseadas em recomendações algorítmicas.

Outro parâmetro importante diz respeito ao papel da automação na amplificação da interação social. Sistemas de recomendação que promovem conexões entre usuários, sugerem novos contatos ou priorizam conteúdos gerados por terceiros aumentam exponencialmente a escala da interação, mesmo quando o número absoluto de usuários não é elevado. A escala, nesse contexto, não deve ser medida apenas quantitativamente, mas também qualitativamente, considerando a velocidade, a recorrência e a intensidade com que novas interações são geradas e expostas ao usuário infantojuvenil. Ambientes em que a criança é constantemente colocada em contato com novos estímulos sociais apresentam riscos distintos daqueles em que a interação é previsível e delimitada.

A análise regulatória também deve levar em conta as medidas de mitigação implementadas pelo fornecedor. Mecanismos de restrição de contato, filtros de mensagens, moderação ativa, bloqueio de usuários, limitação de comentários, controles parentais e configuração padrão de contas privadas são elementos que reduzem significativamente os riscos associados à interação social em larga escala. A presença dessas salvaguardas deve ser reconhecida como fator relevante na modulação das obrigações e na avaliação do grau de risco residual do serviço.

A conceituação que se propõe, portanto, é a de que a “interação social em larga escala” deve ser compreendida como a estruturação de ambientes digitais que possibilitam ou incentivam a comunicação recorrente, automatizada ou amplificada entre crianças e adolescentes e um número indeterminado ou amplo de usuários, especialmente na ausência de mediação proporcional à idade e ao risco. Essa leitura permite diferenciar serviços cujo modelo de interação constitui fator central de risco daqueles em que a interação é acessória, controlada ou mitigada por design. Ao mesmo tempo, orienta a aplicação proporcional das obrigações do Estatuto, concentrando a intervenção regulatória nos cenários em que a arquitetura social do serviço efetivamente potencializa danos relevantes.

6. DADOS INFERIDOS E DADOS DERIVADOS (ART. 2º, V; ART. 14; ART. 19)

Como grande parte dos riscos associados ao uso de tecnologias digitais não decorre apenas dos dados fornecidos diretamente por crianças e adolescentes, mas das inferências produzidas a partir desses dados ao longo do tempo, a “distinção entre dados inferidos e dados derivados” revela-se fundamental para a adequada aplicação do ECA Digital. O Estatuto, embora trate de perfilamento, análise emocional e publicidade direcionada, não explicita de forma direta como devem ser compreendidos e regulados os dados que não são declarados pelo titular, mas construídos por meio de correlações, modelos preditivos e análises comportamentais. Essa lacuna conceitual é particularmente sensível no contexto infantojuvenil, em que inferências podem cristalizar percepções sobre comportamento, preferências e vulnerabilidades em uma fase ainda em formação.

A necessidade de esclarecimento decorre do fato de que dados inferidos e derivados possuem natureza jurídica e impacto prático distintos dos dados fornecidos conscientemente pelo usuário. Enquanto os dados fornecidos tendem a ser episódicos, explícitos e, em alguma medida, compreensíveis para o titular ou seus responsáveis, as inferências operam de forma opaca, cumulativa e muitas vezes irreversível do ponto de vista decisório. No caso de crianças e adolescentes, essas inferências podem gerar efeitos desproporcionais, como a rotulação precoce de comportamentos, a amplificação de estímulos direcionados ou a exclusão silenciosa de determinadas experiências digitais, sem que haja consciência ou possibilidade real de contestação.

Para fins regulatórios, é fundamental diferenciar dados derivados de baixa complexidade de dados inferidos de alto impacto. Dados derivados podem incluir informações técnicas ou contextuais geradas automaticamente para viabilizar o funcionamento do serviço, como registros de acesso, logs operacionais, métricas agregadas de uso ou estatísticas anonimizadas. Já os dados inferidos de maior risco envolvem a construção de categorias, escores ou classificações comportamentais, emocionais ou cognitivas, especialmente quando persistentes e associadas a identificadores individuais ou pseudonimizados. A ausência dessa distinção pode levar à aplicação indistinta de restrições severas a operações técnicas legítimas, sem ganho efetivo de proteção.

Os parâmetros mais adequados para analisar a relevância regulatória dos dados inferidos incluem, em primeiro lugar, a finalidade da inferência. Inferências utilizadas para fins de segurança, moderação de conteúdo, prevenção de riscos ou adequação etária apresentam perfil distinto daquelas voltadas à monetização, publicidade, impulsionamento de conteúdo ou exploração comercial da atenção. Em segundo lugar, deve-se considerar o grau de individualização e persistência da inferência. Inferências transitórias, não armazenadas ou não reutilizadas para decisões futuras representam risco significativamente menor do que perfis duradouros que acompanham a criança ou o adolescente ao longo do tempo e influenciam de forma contínua sua experiência digital.

Outro parâmetro relevante é o impacto concreto da inferência sobre a experiência do usuário. Dados inferidos que produzem efeitos comportamentais relevantes, como alteração sistemática do conteúdo

exibido, intensificação de estímulos, priorização de interações específicas ou restrição de acesso a determinados recursos, demandam maior escrutínio do que inferências que permanecem em nível agregado ou meramente estatístico. Esse impacto deve ser avaliado em conjunto com a possibilidade de controle ou mitigação, considerando a existência de configurações que permitam limitar, revisar ou desativar o uso dessas inferências, bem como a transparência oferecida aos responsáveis legais.

A conceituação que se propõe é a de que “dados inferidos”, para fins do Estatuto, devem ser compreendidos como informações construídas a partir do tratamento automatizado ou sistemático de dados pessoais de crianças e adolescentes, capazes de gerar classificações, previsões ou avaliações individualizadas com impacto relevante sobre sua experiência digital ou comportamento. Dados derivados de caráter meramente técnico, operacional ou agregado não devem ser automaticamente equiparados a dados inferidos de alto risco, desde que não sejam reutilizados para fins de perfilamento, publicidade direcionada ou exploração comercial. Essa leitura permite alinhar o Estatuto à lógica de proteção baseada em risco, evita a ampliação indevida do escopo regulatório e direciona a atuação da autoridade para as práticas inferenciais que efetivamente comprometem o melhor interesse da criança e do adolescente.

7. AUTONOMIA PROGRESSIVA DA CRIANÇA E DO ADOLESCENTE (ART. 2º, VII; ART. 4º)

A “autonomia progressiva da criança e do adolescente” é um dos conceito já conhecido no direito da criança e do adolescente, mas que, no contexto tecnológico, adquire contornos próprios e exige um esforço adicional de concretização normativa, por funcionar como elemento de modulação entre proteção reforçada e reconhecimento gradual da capacidade de autodeterminação no ambiente digital. Sem parâmetros claros, a autonomia progressiva corre o risco de ser utilizada de forma contraditória, ora como justificativa para afastar salvaguardas essenciais, ora como fundamento para uma tutela excessivamente paternalista, incompatível com a realidade do uso digital por adolescentes.

A necessidade de esclarecimento decorre do fato de que a autonomia progressiva não pode ser compreendida como um marco etário fixo nem como uma presunção genérica de capacidade. No ambiente digital, as capacidades cognitivas, sociais e emocionais se desenvolvem de forma não linear e interagem diretamente com a arquitetura dos sistemas, com o grau de complexidade das decisões exigidas e com os riscos associados a determinadas funcionalidades. A simples distinção legal entre criança e adolescente, embora relevante, não é suficiente para orientar escolhas regulatórias que envolvem consentimento, configuração de privacidade, participação em interações sociais ou exposição a práticas comerciais.

Para fins de aplicação do Estatuto, a autonomia progressiva deve ser analisada de forma contextual e funcional, levando em conta o tipo de decisão envolvida e o potencial de impacto sobre os direitos da criança ou do adolescente. Decisões de baixo risco, reversíveis e compreensíveis, como escolhas básicas de personalização estética ou preferências de conteúdo não comercial, admitem maior espaço para exercício autônomo,

especialmente por adolescentes. Em contraste, decisões que envolvem tratamento intensivo de dados pessoais, exposição a interações sociais abertas, monetização, publicidade direcionada ou uso de inferências comportamentais exigem maior grau de mediação adulta e salvaguardas reforçadas, independentemente da idade exata do usuário.

Parâmetros objetivos para operacionalizar a autonomia progressiva incluem a complexidade cognitiva da funcionalidade, o grau de irreversibilidade dos efeitos da decisão, a sensibilidade dos dados tratados e a existência de impactos econômicos ou comportamentais relevantes. Também deve ser considerada a presença de mecanismos de explicação adequados à idade, a possibilidade de revisão ou reversão das escolhas realizadas e a coexistência de ferramentas de supervisão parental que não sejam meramente formais. A autonomia progressiva não elimina o papel dos responsáveis legais, mas redefine esse papel como acompanhamento ativo e proporcional ao risco, em consonância com a própria lógica do Estatuto.

Outro aspecto essencial é evitar que a autonomia progressiva seja instrumentalizada para transferir responsabilidades regulatórias ao próprio usuário infantojuvenil. A lei não autoriza que fornecedores se eximam de obrigações técnicas ou organizacionais sob o argumento de que a criança ou o adolescente exerceu uma escolha autônoma, especialmente quando essa escolha ocorre em ambientes assimétricos, opacos ou projetados para maximizar engajamento. A autonomia progressiva deve ser exercida dentro de um espaço previamente estruturado de proteção, e não como substituto das medidas de segurança e governança exigidas dos agentes econômicos.

A conceituação que se propõe, portanto, é a de que a “autonomia progressiva da criança e do adolescente” deve ser compreendida como a ampliação gradual e contextual da capacidade de tomar decisões no ambiente digital, modulada pelo risco, pela complexidade da funcionalidade e pelo potencial impacto sobre seus direitos fundamentais. Essa autonomia deve operar sempre dentro de um arcabouço de proteção por design, com transparência adequada à idade, possibilidade de mediação parental e limites claros para práticas de maior risco. Essa leitura preserva o equilíbrio entre proteção integral e desenvolvimento da cidadania digital, evita tanto a infantilização excessiva dos adolescentes quanto a exposição prematura a riscos desproporcionais e fornece bases mais sólidas para a atuação regulatória e para o desenho de produtos compatíveis com o Estatuto.

8. MECANISMOS DE VERIFICAÇÃO DE IDADE CONFIÁVEIS (ART. 9º)

A exigência de mecanismos de verificação de idade confiáveis representa uma das mudanças mais estruturais introduzidas pelo ECA Digital, pois desloca o foco da autorresponsabilização do usuário para a adoção de soluções técnicas ativas pelos fornecedores de produtos e serviços digitais. Ao vedar expressamente a autodeclaração como meio suficiente de aferição etária, a Lei nº 15.211/2025 reconhece que a proteção efetiva de crianças e adolescentes depende de instrumentos mais robustos, mas, ao mesmo tempo, deixa em aberto o que deve ser compreendido como um “mecanismo confiável”, criando um espaço interpretativo que pode gerar

tanto soluções excessivamente invasivas quanto abordagens meramente formais, incapazes de atingir o objetivo protetivo da norma.

A necessidade de esclarecimento decorre do fato de que confiabilidade, no contexto da verificação etária, não pode ser confundida com certeza absoluta nem com coleta indiscriminada de dados pessoais. A própria estrutura do Estatuto, em diálogo com a LGPD, afasta qualquer leitura que autorize práticas de vigilância massiva, retenção excessiva de dados ou uso de informações sensíveis além do estritamente necessário. Assim, a confiabilidade deve ser entendida como um atributo relacional, que combina grau razoável de acurácia, proporcionalidade ao risco envolvido, minimização de dados e adequação ao contexto de uso do produto ou serviço.

Para tornar o conceito operacional, é fundamental adotar parâmetros técnicos objetivos que permitam avaliar a adequação das soluções empregadas. Entre esses parâmetros, destaca-se, em primeiro lugar, a finalidade da verificação. Ambientes que dão acesso a conteúdos manifestamente impróprios ou proibidos para menores de idade, como conteúdos pornográficos ou práticas comerciais vedadas, justificam mecanismos mais robustos do que aqueles exigidos para simples adequação etária de experiências ou funcionalidades de baixo risco. A intensidade da verificação deve, portanto, ser calibrada em função do potencial de dano associado ao acesso indevido.

Outro parâmetro essencial é o grau de intrusividade da solução adotada. Mecanismos baseados em sinais etários fornecidos por sistemas operacionais, lojas de aplicativos ou terceiros confiáveis, por meio de APIs seguras e pautadas pela minimização de dados, tendem a apresentar melhor equilíbrio entre proteção e privacidade do que soluções que exigem o compartilhamento direto de documentos ou a retenção de dados biométricos pelo fornecedor do serviço final. A verificação deve, sempre que possível, operar de forma descentralizada, efêmera e sem a criação de bases permanentes de dados etários, reduzindo riscos secundários de vazamento, uso indevido ou discriminação.

A acurácia técnica também deve ser considerada de forma realista e contextualizada. Nenhum mecanismo de verificação de idade é infalível, e a confiabilidade não deve ser medida pela eliminação absoluta de falsos positivos ou negativos, mas pela adoção de soluções que apresentem desempenho adequado em relação ao estado da técnica e ao risco específico da aplicação. A exigência de perfeição técnica tende a incentivar práticas excessivamente invasivas, enquanto a aceitação de soluções manifestamente frágeis esvazia a finalidade da norma. A análise regulatória deve, portanto, considerar benchmarks técnicos, auditorias independentes e métricas de desempenho compatíveis com o uso pretendido.

Outro elemento relevante é a governança do mecanismo de verificação. Soluções confiáveis pressupõem transparência quanto ao funcionamento geral do sistema, definição clara de responsabilidades entre os agentes da cadeia digital e possibilidade de supervisão por autoridades competentes. A ausência de clareza sobre quem valida, armazena ou descarta os dados utilizados na verificação compromete tanto a proteção de dados quanto a responsabilização em caso de falhas. Nesse sentido, modelos que se

baseiam em sinais binários ou faixas etárias, em vez de dados brutos, tendem a oferecer maior segurança jurídica e técnica.

A conceituação que se propõe, portanto, é a de que “mecanismos de verificação de idade confiáveis” devem ser entendidos como soluções técnicas que, de forma proporcional ao risco do serviço, permitem aferir ou confirmar a idade ou faixa etária do usuário com grau razoável de acurácia, observando os princípios da minimização, finalidade e segurança, sem recorrer à autodeclaração e sem implicar coleta ou retenção excessiva de dados pessoais. Essa leitura permite compatibilizar a proteção reforçada de crianças e adolescentes com a preservação da privacidade, evita incentivos à vigilância generalizada e orienta a adoção de soluções interoperáveis, auditáveis e alinhadas ao estado da técnica, em consonância com os objetivos centrais do Estatuto.

9. CONFIGURAÇÕES-PADRÃO MAIS PROTETIVAS (ART. 8º)

A exigência de configurações-padrão mais protetivas desloca o foco da proteção de escolhas individuais posteriores para o desenho inicial dos produtos e serviços digitais. Ao estabelecer que a experiência padrão deve operar no nível mais elevado de proteção disponível, o Estatuto reconhece que a arquitetura das plataformas exerce influência direta e significativa sobre o comportamento de crianças e adolescentes, especialmente em contextos marcados por assimetria informacional, estímulos de engajamento contínuo e baixa previsibilidade dos impactos de longo prazo das interações digitais.

A necessidade de esclarecimento desse conceito decorre do fato de que a expressão “mais protetivo” não possui conteúdo técnico auto evidente e pode ser interpretada de forma excessivamente abstrata ou maximalista. Sem parâmetros claros, fornecedores podem tanto adotar soluções meramente simbólicas, que preservam riscos relevantes sob a aparência de conformidade, quanto serem pressionados a implementar restrições desproporcionais que inviabilizam funcionalidades legítimas ou reduzem significativamente o acesso à informação e à participação social. A precisão conceitual é, portanto, essencial para garantir coerência regulatória e previsibilidade jurídica.

Para fins de aplicação do Estatuto, a proteção por padrão deve ser compreendida como a adoção inicial de configurações que reduzam a exposição da criança ou do adolescente a riscos previsíveis, especialmente aqueles relacionados à privacidade, à segurança e ao uso excessivo, sem impedir o funcionamento básico do serviço. Entre os parâmetros objetivos relevantes estão a desativação inicial de funcionalidades que ampliem a exposição pública, como perfis abertos e compartilhamento automático de conteúdo, a limitação de mecanismos de engajamento contínuo, como reprodução automática, notificações persistentes e recompensas vinculadas ao tempo de uso, e a restrição de sistemas de recomendação personalizados baseados em histórico comportamental sensível.

Outro parâmetro essencial diz respeito à reversibilidade e à transparência das escolhas. Configurações-padrão mais protetivas não significam imutabilidade. O Estatuto admite a possibilidade de adoção de

configurações menos restritivas, desde que essa transição seja fruto de escolha informada, ativa e compreensível, compatível com a idade e o estágio de desenvolvimento do usuário, e, quando aplicável, mediada pelos responsáveis legais. A ausência de fricção adequada, a utilização de padrões manipulativos ou a apresentação assimétrica de opções compromete a legitimidade dessa escolha e esvazia o sentido da proteção por padrão.

A análise também deve considerar o grau de risco associado à funcionalidade específica. Quanto maior o potencial de impacto negativo sobre direitos fundamentais, maior deve ser o nível de proteção incorporado ao padrão inicial. Funcionalidades envolvendo interação social ampla, coleta de dados sensíveis, geolocalização, monetização ou publicidade exigem salvaguardas mais robustas do que recursos de uso passivo ou informacional. Essa abordagem baseada em risco permite modular a aplicação do conceito de forma proporcional, em consonância com o próprio desenho do Estatuto.

A conceituação que se propõe, portanto, é a de que “configurações-padrão mais protetivas” correspondem ao conjunto de escolhas técnicas iniciais que minimizam riscos previsíveis à criança e ao adolescente, assegurando privacidade elevada, limitação de estímulos compulsivos e controle sobre interações e dados, sem eliminar o acesso significativo às tecnologias digitais. Essas configurações devem ser transparentes, reversíveis de forma informada e calibradas conforme o risco da funcionalidade, preservando o equilíbrio entre proteção integral, desenvolvimento progressivo e viabilidade tecnológica. Essa leitura reforça o caráter preventivo do Estatuto e orienta a adoção de práticas de design compatíveis com seus objetivos, sem transformar a proteção por padrão em obstáculo desproporcional à inovação ou à liberdade de expressão.

10. USO COMPULSIVO E MECANISMOS DE ENGAJAMENTO ARTIFICIAL (ART. 6º, II E III)

A referência à prevenção do “uso compulsivo de produtos e serviços digitais” pelo ECA Digital representa um reconhecimento explícito de que determinadas escolhas de design e de arquitetura de sistemas podem afetar de forma significativa o desenvolvimento biopsicossocial de crianças e adolescentes. O Estatuto não trata o uso compulsivo como resultado exclusivo de comportamento individual, mas como fenômeno estruturalmente influenciado por mecanismos técnicos concebidos para maximizar tempo de permanência, recorrência e intensidade de interação. Essa abordagem é relevante, mas exige esclarecimentos conceituais para evitar interpretações excessivamente amplas ou imprecisas que possam gerar insegurança jurídica e dificuldades práticas de implementação.

A necessidade de esclarecimento decorre do fato de que o conceito de uso compulsivo não se confunde com uso frequente, prolongado ou intenso. Crianças e adolescentes podem utilizar produtos digitais por longos períodos para fins educacionais, criativos ou de socialização legítima, sem que isso configure compulsividade. O elemento distintivo reside na presença de mecanismos artificiais que reduzem a autonomia do usuário, dificultam a interrupção voluntária do uso ou exploram vulnerabilidades cognitivas e emocionais próprias das fases de desenvolvimento. Sem essa distinção, o conceito corre o risco de se tornar excessivamente subjetivo, abrindo

espaço para interpretações que penalizam funcionalidades neutras ou socialmente relevantes.

Para fins de aplicação do Estatuto, o uso compulsivo deve ser analisado a partir de parâmetros técnicos e funcionais relacionados ao desenho do sistema. Entre esses parâmetros, destacam-se a existência de reprodução automática contínua sem fricção adequada, a utilização de notificações persistentes ou escalonadas com finalidade de reengajamento, a concessão de recompensas variáveis ou progressivas vinculadas exclusivamente ao tempo de uso e a ausência de pontos naturais de interrupção da experiência. Esses elementos, quando combinados, tendem a criar ciclos de uso prolongado que não dependem de escolha consciente do usuário, especialmente em públicos em desenvolvimento.

Outro parâmetro relevante é a possibilidade efetiva de controle e limitação do uso. A presença de ferramentas claras para visualização do tempo de uso, definição de limites temporais, pausas programadas e desativação de estímulos de engajamento constitui indicativo de mitigação do risco de compulsividade. A ausência dessas ferramentas, ou sua implementação de forma obscura, fragmentada ou difícil de acessar, reforça a caracterização de mecanismos de engajamento artificial incompatíveis com o espírito protetivo do Estatuto. A análise deve considerar não apenas a existência formal desses recursos, mas sua eficácia prática e adequação à idade do usuário.

Também é relevante distinguir mecanismos de engajamento voltados à funcionalidade do serviço daqueles orientados predominantemente à maximização de métricas comerciais. Recursos necessários para a navegação, progressão lógica de atividades ou conclusão de tarefas não se confundem, por si só, com práticas abusivas. O problema surge quando o engajamento é artificialmente ampliado por técnicas que exploram reforços psicológicos, escassez simulada ou pressão temporal, sem relação direta com a utilidade do serviço para a criança ou o adolescente.

A conceituação que se propõe, portanto, é a de que “uso compulsivo” deve ser entendido como o resultado da combinação de mecanismos técnicos de engajamento artificial que reduzem a capacidade de autodeterminação do usuário infantojuvenil, dificultam a interrupção voluntária do uso e ampliam a exposição prolongada sem finalidade proporcional ao benefício oferecido. A prevenção do uso compulsivo exige a identificação desses mecanismos, a adoção de configurações-padrão que limitem sua intensidade e a disponibilização de controles claros e eficazes, calibrados conforme o risco e a faixa etária. Essa leitura permite proteger a saúde e o bem-estar de crianças e adolescentes sem equiparar, de forma indevida, engajamento legítimo a práticas abusivas, preservando a inovação responsável e o acesso significativo às tecnologias digitais.

11. SUPERVISÃO PARENTAL E CUIDADO ATIVO (ART. 5º; ART. 8º, § 2º)

A “supervisão parental e o cuidado ativo”, conforme previstos no Estatuto, devem ser compreendidos como um modelo de acompanhamento informado, contínuo e proporcional do uso de produtos e serviços digitais por crianças e adolescentes, estruturado a partir de uma

corresponsabilidade entre fornecedores e responsáveis legais. Esse modelo reconhece que a proteção efetiva no ambiente digital não pode ser alcançada nem pela imposição exclusiva de obrigações técnicas às plataformas nem pela simples transferência de deveres às famílias, exigindo a combinação de arquitetura de proteção por design, transparência informacional e ferramentas que viabilizem o exercício real do cuidado.

Para que a supervisão parental seja efetiva, não basta a disponibilização formal de mecanismos de controle. É necessário que esses instrumentos sejam acessíveis, intuitivos e adequados às diferentes faixas etárias e estágios de desenvolvimento, permitindo configurações granulares compatíveis com o risco das funcionalidades envolvidas. O cuidado ativo pressupõe que pais e responsáveis compreendam claramente quais interações são permitidas, quais dados são tratados, quais sistemas de recomendação ou de engajamento estão ativos e quais salvaguardas estão em vigor, sob pena de a supervisão se tornar meramente simbólica e incapaz de mitigar riscos concretos.

Nesse contexto, a adoção de linguagem clara, descomplicada e adequada a distintos níveis de letramento digital e jurídico constitui elemento essencial para a efetividade do instituto. Informações excessivamente técnicas, fragmentadas ou redigidas em linguagem hermética dificultam o exercício do cuidado ativo, especialmente por responsáveis com menor familiaridade tecnológica. A utilização de práticas de visual law, como fluxos explicativos, painéis visuais de controle, ícones intuitivos e sinalizações claras sobre riscos, configurações ativas e impactos das escolhas realizadas, deve ser considerada parâmetro relevante para aferir a conformidade das soluções oferecidas com o Estatuto.

Esses recursos não substituem o conteúdo jurídico ou técnico subjacente, mas funcionam como instrumentos de tradução normativa, ampliando a transparência, a compreensão e a capacidade de decisão informada dos responsáveis legais. A supervisão parental, assim concebida, não autoriza monitoramento indiscriminado nem afasta a responsabilidade dos fornecedores, mas opera como camada adicional de proteção, alinhada à autonomia progressiva da criança e do adolescente e ao princípio do melhor interesse, fortalecendo a proteção integral sem comprometer o desenvolvimento da cidadania digital.

12. PRODUTOS E SERVIÇOS DE MONITORAMENTO INFANTIL (ART. 12)

Os “produtos e serviços de monitoramento infantil” envolvem, por definição, o tratamento intensivo de dados pessoais altamente sensíveis, como imagens, sons, localização e registros contínuos de atividade. Embora sejam frequentemente apresentados como instrumentos de proteção, esses produtos carregam riscos relevantes de violação à privacidade, normalização da vigilância e comprometimento do desenvolvimento da autonomia e da confiança de crianças e adolescentes. Por essa razão, o Estatuto corretamente impõe limites e condicionantes ao seu uso, mas o conceito demanda esclarecimentos adicionais para evitar interpretações excessivamente permissivas ou, em sentido oposto, proibições implícitas não pretendidas pelo legislador.

A necessidade de esclarecimento decorre do fato de que nem toda forma de acompanhamento parental configura monitoramento infantil nos termos da Lei nº 15.211/2025. O conceito deve ser reservado a produtos ou serviços cuja finalidade principal seja a coleta, o registro ou a transmissão sistemática de informações sobre a criança ou o adolescente, especialmente quando realizada de forma contínua, automatizada ou em tempo real. Soluções pontuais, episódicas ou limitadas a funcionalidades específicas de segurança não devem ser automaticamente enquadradas como monitoramento infantil, sob pena de diluição conceitual e insegurança jurídica.

Para fins de aplicação do Estatuto, a análise desses produtos deve se basear em parâmetros técnicos e funcionais claros. Entre eles, destaca-se a natureza dos dados coletados, com especial atenção a imagens, sons e dados de localização em tempo real, o grau de continuidade do monitoramento e a possibilidade de correlação desses dados para formação de padrões comportamentais. Quanto maior a persistência, granularidade e sensibilidade dos dados tratados, maior deve ser o nível de escrutínio regulatório e de exigência de salvaguardas técnicas e organizacionais.

Outro parâmetro essencial é a finalidade do monitoramento e sua proporcionalidade em relação ao risco que se busca mitigar. O Estatuto não autoriza o uso de soluções de monitoramento como mecanismo genérico de controle da vida digital ou cotidiana da criança ou do adolescente. O monitoramento deve estar vinculado a objetivos legítimos de proteção e segurança, ser limitado no tempo e no escopo e compatível com a idade e o estágio de desenvolvimento do usuário. A utilização de monitoramento permanente, indiscriminado ou desproporcional compromete o melhor interesse e pode gerar efeitos adversos sobre o desenvolvimento psicossocial.

A transparência também é elemento indispensável. Crianças e adolescentes devem ser informados, em linguagem apropriada, sobre a existência do monitoramento, suas finalidades e seus limites. O monitoramento oculto ou dissimulado, ainda que com consentimento dos responsáveis legais, contraria o espírito do Estatuto e enfraquece a construção de autonomia e confiança. Da mesma forma, os responsáveis devem ser informados de forma clara sobre os riscos associados ao uso desses produtos, inclusive riscos de segurança da informação, vazamento de dados e uso indevido por terceiros.

A conceituação que se propõe, portanto, é a de que “produtos e serviços de monitoramento infantil” correspondem a soluções tecnológicas cuja finalidade principal seja o acompanhamento sistemático das atividades, localização ou comunicações de crianças e adolescentes, mediante coleta contínua ou recorrente de dados sensíveis. Esses produtos devem ser utilizados de forma excepcional, proporcional e transparente, orientados pelo melhor interesse, pela minimização de dados e pelo respeito à autonomia progressiva, não podendo servir como instrumentos de vigilância permanente ou de substituição do diálogo, da orientação e do cuidado ativo. Essa leitura preserva a função protetiva legítima do monitoramento sem normalizar práticas incompatíveis com os direitos fundamentais assegurados pelo Estatuto.

13. CONTEÚDOS IMPRÓPRIOS, INADEQUADOS OU PROIBIDOS POR LEI (ART. 25, CAPUT E § 3º)

A “classificação de conteúdos como impróprios, inadequados ou proibidos por lei” orienta deveres de prevenção, verificação de idade, bloqueio, moderação e retirada de conteúdos no ambiente digital. Embora a Lei nº 15.211/2025 apresente referências normativas relevantes, a amplitude e a heterogeneidade dessas categorias exigem esclarecimentos adicionais para assegurar aplicação consistente, proporcional e compatível com a liberdade de expressão e com o acesso à informação por crianças e adolescentes.

A necessidade de esclarecimento decorre, em primeiro lugar, da distinção conceitual entre conteúdo proibido por lei e conteúdo impróprio ou inadequado. Conteúdos proibidos correspondem àqueles cuja ilicitude decorre diretamente do ordenamento jurídico, como material pornográfico envolvendo crianças e adolescentes ou outras hipóteses expressamente vedadas pela legislação penal e infraconstitucional. Nesses casos, não há margem para ponderação quanto à adequação etária, sendo legítima a imposição de deveres rigorosos de bloqueio, remoção e comunicação às autoridades competentes. Já os conteúdos impróprios ou inadequados situam-se em zona distinta, relacionada ao potencial de dano ao desenvolvimento biopsicossocial, e não à ilicitude em sentido estrito.

Para fins de aplicação do Estatuto, é fundamental que o conceito de conteúdo impróprio ou inadequado seja delimitado por parâmetros objetivos e verificáveis, de modo a evitar subjetivismos ou ampliações indevidas. Esses parâmetros devem considerar a natureza do conteúdo, o contexto de apresentação, a faixa etária a que se destina e a probabilidade de causar danos concretos à saúde física, mental ou emocional de crianças e adolescentes. A simples presença de temas sensíveis ou controversos não pode, por si só, justificar a classificação como inadequado, sob pena de confusão com censura ou restrição desproporcional à liberdade de expressão.

Outro parâmetro relevante é a articulação com os sistemas de classificação indicativa já existentes no ordenamento jurídico brasileiro. O Estatuto não cria um regime autônomo de valoração moral de conteúdos, mas se insere em um ecossistema normativo que reconhece a importância de critérios etários, sinalização adequada e contextualização. A aplicação do conceito de inadequação deve, portanto, dialogar com essas referências, evitando soluções fragmentadas ou contraditórias entre diferentes regimes regulatórios.

A análise também deve considerar o papel das funcionalidades e da arquitetura de distribuição. Um mesmo conteúdo pode assumir graus distintos de risco conforme o modo como é apresentado, recomendado ou amplificado. Sistemas de recomendação ativa, impulsionamento ou direcionamento algorítmico para públicos infantojuvenis elevam significativamente o potencial de dano e justificam salvaguardas mais rigorosas do que a mera disponibilização passiva de conteúdo acessível mediante busca deliberada. Esse elemento funcional é essencial para calibrar as obrigações impostas aos fornecedores.

A conceituação que se propõe, portanto, é a de que “conteúdos proibidos por lei” correspondem àqueles cuja vedação decorre diretamente do ordenamento jurídico e demandam medidas imediatas de bloqueio e remoção, enquanto conteúdos impróprios ou inadequados devem ser definidos a partir de critérios objetivos de risco ao desenvolvimento da criança e do adolescente, considerados a faixa etária, o contexto, a forma de distribuição e o potencial de dano concreto. Essa leitura permite proteger de forma eficaz os direitos infantojuvenis, sem transformar o Estatuto em instrumento de restrição genérica de conteúdos legítimos, preservando o equilíbrio entre proteção integral, liberdade de expressão e segurança jurídica.

14. CLASSIFICAÇÃO INDICATIVA E ADEQUAÇÃO ETÁRIA DO CONTEÚDO (ART. 26)

A noção de “classificação indicativa e de adequação etária do conteúdo” serve de base para a definição de deveres de avaliação prévia, sinalização informativa, modulação de acesso e restrição de funcionalidades em produtos e serviços digitais. Embora o Estatuto dialogue com o sistema brasileiro de classificação indicativa já existente, especialmente aquele desenvolvido no âmbito do Ministério da Justiça, a aplicação desses conceitos ao ambiente digital apresenta desafios específicos que demandam esclarecimentos adicionais para evitar interpretações excessivamente amplas ou tecnicamente inexecutáveis.

No contexto digital, a classificação indicativa não pode ser compreendida apenas como um rótulo estático atribuído a um conteúdo isolado, mas deve considerar a dinâmica própria das plataformas, nas quais conteúdos são constantemente combinados, recomendados, priorizados ou amplificados por sistemas automatizados. A ausência de critérios claros pode gerar insegurança jurídica quanto ao alcance das obrigações impostas aos fornecedores, especialmente no que diz respeito à distinção entre disponibilização passiva de conteúdo, curadoria editorial e recomendação algorítmica ativa. Essa distinção é fundamental para calibrar responsabilidades e evitar que obrigações pensadas para ambientes editoriais fechados sejam transpostas de forma inadequada para ecossistemas digitais abertos.

Para tornar o conceito mais preciso, a análise da adequação etária deve se apoiar em parâmetros técnicos e objetivos, que considerem tanto as características intrínsecas do conteúdo quanto a forma como ele é apresentado, distribuído e priorizado. Entre esses parâmetros, destacam-se a presença de temas sensíveis associados a violência, sexualidade, autolesão, uso de substâncias ou linguagem imprópria, bem como o grau de contextualização e finalidade do conteúdo, distinguindo-se, por exemplo, material informativo ou educativo de conteúdos cujo objetivo principal seja entretenimento ou estímulo comportamental. A forma de acesso também é relevante, devendo ser diferenciado o conteúdo acessível apenas mediante busca ativa daquele que é impulsionado ou recomendado de maneira automática ao usuário.

Do ponto de vista operacional, a classificação indicativa em ambientes digitais deve ser concebida como um processo contínuo e proporcional ao

risco, e não como uma exigência absoluta de avaliação manual de todo e qualquer conteúdo. Parâmetros como o número de usuários ativos mensais, a escala de circulação do conteúdo, o grau de automação na recomendação e o público efetivamente alcançado devem orientar o nível de diligência exigido do fornecedor. Serviços que operam com recomendação personalizada para crianças e adolescentes, por exemplo, justificam um grau mais elevado de controle e revisão, enquanto plataformas que apenas hospedam conteúdo de forma neutra demandam abordagem distinta.

A conceituação que se propõe, portanto, é a de que a “classificação indicativa e a adequação etária”, no âmbito do ECA Digital, consistem em um conjunto de critérios técnicos, informativos e operacionais destinados a assegurar que conteúdos digitais sejam apresentados, sinalizados e, quando necessário, restritos de forma compatível com o estágio de desenvolvimento da criança e do adolescente, levando em conta não apenas o conteúdo em si, mas também os mecanismos de acesso, recomendação e amplificação utilizados pelo serviço. Essa leitura permite harmonizar a proteção integral prevista na lei com a viabilidade tecnológica das plataformas e com a preservação da liberdade de expressão e de acesso à informação, evitando soluções genéricas ou desproporcionais que poderiam comprometer o equilíbrio do ecossistema digital.

15. SERVIÇO COM CONTROLE EDITORIAL (ART. 39)

O conceito de “serviço com controle editorial” funciona como critério de modulação das obrigações impostas aos fornecedores, especialmente no que diz respeito à responsabilização por conteúdos, à intensidade dos deveres de prevenção e à aplicabilidade de regimes diferenciados previstos no art. 39 da Lei nº 15.211/2025. Trata-se de um conceito estrutural, cujo alcance inadequadamente definido pode gerar efeitos regulatórios desproporcionais, ao equiparar realidades técnicas e econômicas profundamente distintas no ecossistema digital.

A necessidade de esclarecimento decorre, em primeiro lugar, da ambiguidade inerente à expressão “controle editorial” no contexto de serviços digitais contemporâneos. Diferentemente dos meios de comunicação tradicionais, nos quais o controle editorial pressupõe seleção prévia, curadoria humana direta e responsabilidade integral sobre o conteúdo veiculado, os ambientes digitais operam, em larga medida, por meio de sistemas automatizados de organização, ranqueamento e recomendação de conteúdos produzidos por terceiros. A simples existência de ordenação algorítmica ou de mecanismos de moderação não equivale, por si só, ao exercício de controle editorial no sentido clássico ou jurídico do termo.

Para fins de aplicação do Estatuto, é essencial distinguir entre controle editorial ativo e curadoria funcional ou técnica. O controle editorial relevante para fins regulatórios deve ser compreendido como a atuação deliberada do fornecedor na seleção, aprovação, edição ou produção de conteúdos, com base em critérios próprios e com capacidade efetiva de determinar o que será disponibilizado ao público. Esse tipo de controle pressupõe intervenção substantiva sobre o conteúdo, e não apenas a aplicação de regras gerais de

uso, termos de serviço ou sistemas automatizados voltados à organização ou à segurança da plataforma.

Parâmetros objetivos para identificar a existência de controle editorial incluem a produção direta de conteúdo pelo fornecedor, a aprovação prévia sistemática de materiais antes da publicação, a edição ou adaptação substancial de conteúdos de terceiros, a definição temática ou narrativa do conteúdo ofertado e a existência de linhas editoriais claras que orientem a disponibilização de informações ao público. A presença cumulativa desses elementos indica um grau elevado de ingerência sobre o conteúdo, compatível com a noção de controle editorial adotada pelo Estatuto.

Em contraste, práticas como moderação reativa, aplicação de diretrizes de comunidade, remoção de conteúdos ilícitos ou inadequados, ordenação cronológica, ranqueamento por popularidade agregada ou recomendação baseada em critérios genéricos não devem ser automaticamente enquadradas como controle editorial. Esses mecanismos cumprem funções técnicas essenciais para a segurança, a usabilidade e a escalabilidade dos serviços digitais, e sua equiparação ao controle editorial pleno ampliaria de forma indevida o escopo das obrigações legais, com impactos negativos sobre a liberdade de expressão, a inovação e a diversidade de modelos de negócio.

Outro elemento relevante é a finalidade da intervenção sobre o conteúdo. O Estatuto busca reforçar a proteção de crianças e adolescentes sem desestruturar o funcionamento do ambiente digital. Intervenções voltadas à prevenção de danos, à adequação etária, à segurança e ao cumprimento de obrigações legais não devem ser interpretadas como indícios automáticos de controle editorial, sob pena de criar incentivos perversos para a inação regulatória ou para a redução de salvaguardas protetivas por parte dos fornecedores.

A conceituação que se propõe, portanto, é a de que “serviço com controle editorial” deve ser entendido como aquele em que o fornecedor exerce influência direta, substantiva e deliberada sobre o conteúdo disponibilizado, por meio de seleção, edição, produção ou aprovação prévia sistemática, assumindo papel ativo na definição do conteúdo acessível ao público. Serviços que se limitam a hospedar, organizar, ranquear ou moderar conteúdos de terceiros com base em critérios gerais, automatizados ou de segurança não devem ser automaticamente enquadrados nessa categoria. Essa leitura preserva a coerência do Estatuto, assegura a proporcionalidade regulatória e permite diferenciar, de forma técnica e juridicamente consistente, modelos editoriais de plataformas intermediárias, direcionando as obrigações mais intensas aos cenários em que o grau de ingerência efetivamente justifica maior responsabilidade.

16. IMPULSIONAMENTO (ART. 2º, XI; ART. 19)

O conceito de “impulsionamento” assume relevância central no ECA Digital porque se situar no ponto de interseção entre arquitetura de distribuição de conteúdo, práticas comerciais e amplificação de riscos no ambiente digital. A Lei nº 15.211/2025 faz referência expressa ao impulsionamento em diferentes dispositivos, associando-o à publicidade, à monetização e à

intensificação da exposição de crianças e adolescentes a conteúdos e práticas potencialmente nocivas. Contudo, a ausência de uma delimitação conceitual precisa sobre o que constitui impulsionamento cria incertezas relevantes quanto ao alcance das obrigações e vedações previstas, especialmente em ecossistemas digitais altamente automatizados.

A necessidade de esclarecimento decorre do fato de que o impulsionamento não se confunde com a mera circulação ou disponibilidade de conteúdo. Em plataformas digitais, praticamente todo conteúdo é submetido a algum grau de ordenação ou priorização, seja por critérios cronológicos, seja por relevância, popularidade ou personalização. Equiparar qualquer forma de ordenação algorítmica ao impulsionamento levaria a uma interpretação excessivamente abrangente, capaz de esvaziar a distinção entre distribuição neutra e amplificação intencional, além de gerar obrigações desproporcionais e tecnicamente inexecutáveis.

Para fins de aplicação do Estatuto, é fundamental diferenciar impulsionamento de recomendação funcional ou organização básica do conteúdo. O impulsionamento juridicamente relevante deve ser compreendido como a adoção de medidas técnicas ou comerciais destinadas a ampliar artificialmente o alcance, a visibilidade ou a recorrência de um conteúdo para além do que ocorreria por fluxo orgânico ordinário, especialmente quando direcionado ou exposto de forma ativa a crianças e adolescentes. Esse elemento de amplificação intencional constitui o núcleo do risco regulatório associado ao impulsionamento.

Parâmetros objetivos para caracterizar o impulsionamento incluem a existência de pagamento direto ou indireto para ampliação de alcance, o uso de ferramentas específicas de promoção ou destaque, a priorização deliberada de conteúdos em sistemas de recomendação com base em objetivos comerciais ou de engajamento intensificado e a segmentação ativa de públicos, inclusive por faixa etária ou por perfis comportamentais. O impulsionamento pode ocorrer tanto de forma paga quanto não paga, desde que haja intervenção consciente do fornecedor ou de terceiros para maximizar a exposição do conteúdo.

Outro parâmetro relevante é a direção do impulsionamento. A amplificação genérica de conteúdos para públicos amplos não apresenta o mesmo perfil de risco que o impulsionamento direcionado ou previsivelmente acessível a crianças e adolescentes. Quando a arquitetura do sistema favorece a exposição reiterada de usuários infantojuvenis a conteúdos impulsionados, especialmente em contextos de monetização, publicidade ou engajamento artificial, o potencial de dano se eleva significativamente, justificando salvaguardas reforçadas e restrições específicas.

A análise também deve considerar a natureza do conteúdo impulsionado. O Estatuto não veda o impulsionamento em abstrato, mas busca limitar práticas que intensificam a exposição a conteúdos inadequados, práticas comerciais abusivas ou estímulos incompatíveis com o desenvolvimento saudável. Impulsionamento de conteúdos educativos, informativos ou culturais, devidamente classificados e adequados à faixa etária, apresenta perfil de risco distinto daquele associado à amplificação de conteúdos sensíveis, comerciais ou exploratórios. Essa diferenciação é essencial para preservar a proporcionalidade da intervenção regulatória.

A conceituação que se propõe, portanto, é a de que “impulsionamento” deve ser entendido como a amplificação deliberada e artificial do alcance ou da visibilidade de conteúdos, por meios técnicos ou comerciais, que excede a distribuição orgânica ordinária do serviço, especialmente quando direcionada ou previsivelmente acessível a crianças e adolescentes. Essa leitura permite distinguir práticas legítimas de organização e recomendação funcional de estratégias de amplificação com impacto relevante sobre o comportamento e a exposição do público infantojuvenil, assegurando aplicação proporcional do Estatuto e evitando a equiparação indevida entre arquitetura básica de plataformas e práticas de promoção intensificada.

17. REVISÃO REGULAR DE FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL (ART. 20)

A exigência de “revisão regular de ferramentas de inteligência artificial” no ECA Digital reflete o reconhecimento de que sistemas baseados em IA, especialmente aqueles utilizados em produtos e serviços acessíveis a crianças e adolescentes, não são estáticos e podem produzir efeitos distintos ao longo do tempo. O Estatuto impõe esse dever como instrumento de governança contínua, voltado à identificação, mitigação e correção de riscos associados ao funcionamento desses sistemas. No entanto, a ausência de parâmetros claros sobre o alcance, a periodicidade e o conteúdo dessa revisão demandam esclarecimentos adicionais para assegurar aplicação uniforme, tecnicamente viável e juridicamente previsível.

A necessidade de esclarecimento decorre do fato de que a expressão “revisão regular” pode ser interpretada de forma excessivamente ampla ou indeterminada, gerando expectativas de monitoramento constante ou auditoria permanente, incompatíveis com a complexidade e a escala dos sistemas digitais contemporâneos. A revisão não deve ser confundida com reengenharia contínua ou com obrigação de validação *ex ante* de cada alteração incremental do sistema, sob pena de inviabilizar o uso legítimo de IA em ambientes dinâmicos. Trata-se, antes, de um mecanismo de avaliação periódica e proporcional ao risco, orientado por critérios objetivos.

Para fins de aplicação do Estatuto, a revisão regular deve ser calibrada a partir de parâmetros técnicos que considerem a finalidade da ferramenta de IA, o grau de automação decisória, a sensibilidade dos dados tratados e o impacto potencial sobre a experiência e os direitos de crianças e adolescentes. Sistemas utilizados para moderação de conteúdo, recomendação personalizada, inferência comportamental ou análise emocional justificam um nível de revisão distinto daquele aplicável a ferramentas de uso meramente auxiliar ou operacional. A intensidade da revisão deve, portanto, acompanhar o risco associado à funcionalidade, e não a simples presença de IA no serviço.

Outro parâmetro essencial é a periodicidade da revisão, que não pode ser fixada de forma abstrata ou uniforme para todos os sistemas. A revisão deve ocorrer em intervalos razoáveis, compatíveis com a velocidade de evolução do sistema e com a ocorrência de eventos relevantes, como mudanças substanciais no modelo, ampliação de escopo funcional, introdução de novas fontes de dados ou identificação de incidentes, vieses ou falhas

recorrentes. A lógica que se impõe é a de revisão orientada a eventos e a risco, e não a cronogramas arbitrários.

O conteúdo da revisão também demanda delimitação. A revisão regular não se restringe à avaliação técnica de desempenho do sistema, mas deve abranger aspectos relacionados à proteção de dados, à adequação etária, à segurança, à explicabilidade e aos efeitos comportamentais observáveis sobre crianças e adolescentes. A análise deve verificar se o sistema continua operando de acordo com suas finalidades declaradas, se as salvaguardas originalmente implementadas permanecem eficazes e se novos riscos emergiram em decorrência de mudanças no contexto de uso ou no perfil dos usuários. Esse processo pode se apoiar em métricas internas, testes controlados, análises de impacto e mecanismos de monitoramento de incidentes.

Do ponto de vista da governança, é relevante que a revisão regular esteja documentada e integrada aos processos internos do fornecedor, permitindo rastreabilidade e demonstração de diligência em eventual fiscalização. Isso não implica a divulgação irrestrita de informações sensíveis ou segredos industriais, mas a manutenção de registros proporcionais que evidenciem a adoção de práticas responsáveis de gestão de riscos. A ausência de qualquer estrutura formal de revisão, por outro lado, compromete a efetividade do dever imposto pelo Estatuto.

A conceituação que se propõe, portanto, é a de que a “revisão regular de ferramentas de inteligência artificial” deve ser entendida como um processo periódico e orientado por risco de avaliação do funcionamento, dos impactos e das salvaguardas associadas a sistemas de IA utilizados em produtos e serviços acessíveis a crianças e adolescentes. Essa revisão deve considerar a finalidade do sistema, seu grau de automação e seu potencial de impacto, ocorrer de forma proporcional e ser acionada especialmente diante de mudanças relevantes ou indícios de risco. Essa leitura assegura a efetividade da proteção prevista no Estatuto sem impor obrigações tecnicamente inviáveis ou desproporcionais, incentivando práticas sólidas de governança de IA alinhadas ao melhor interesse da criança e do adolescente.

18. FUNÇÕES NÃO ESSENCIAIS AO FUNCIONAMENTO BÁSICO DOS SISTEMAS (ART. 8º; ART. 6º)

A distinção entre “funções essenciais e não essenciais ao funcionamento básico dos sistemas” opera como critério de modulação das obrigações aplicáveis a produtos e serviços digitais acessíveis a crianças e adolescentes. Ao referir-se a funcionalidades que podem ou devem ser limitadas, desativadas ou condicionadas em determinados contextos, o Estatuto introduz um mecanismo de calibragem normativa que visa reduzir riscos sem comprometer a utilidade fundamental dos serviços. Contudo, a ausência de parâmetros claros para definir o que constitui o funcionamento básico de um sistema e quais funções se situam fora desse núcleo exige esclarecimentos adicionais para assegurar aplicação consistente e proporcional.

A necessidade de esclarecimento decorre do fato de que o funcionamento básico de um sistema não é um conceito absoluto, mas relacional e dependente do tipo de produto ou serviço oferecido. O que é essencial para uma plataforma educacional pode não ser essencial para uma rede social, um jogo digital ou um serviço de *streaming*. Interpretar o funcionamento básico de forma genérica ou uniforme pode levar à imposição de restrições inadequadas, que comprometem a finalidade legítima do serviço ou, inversamente, à manutenção de funcionalidades de alto risco sob o argumento de essencialidade mal delimitada.

Para fins de aplicação do Estatuto, o funcionamento básico deve ser compreendido como o conjunto mínimo de funcionalidades necessárias para que o produto ou serviço cumpra sua finalidade principal declarada ao usuário, independentemente de estratégias de engajamento, monetização ou amplificação de interação. Esse núcleo funcional deve ser identificado a partir da proposta central do serviço, de sua comunicação institucional, de sua classificação em lojas de aplicativos e do uso esperado pelo público-alvo. Funcionalidades acessórias, ainda que amplamente utilizadas, não se confundem automaticamente com funções essenciais se não forem indispensáveis à realização dessa finalidade principal.

Parâmetros objetivos para diferenciar funções essenciais de não essenciais incluem a necessidade funcional da ferramenta para a prestação do serviço, a possibilidade de desativação sem perda substancial da utilidade central, o grau de dependência do usuário em relação à funcionalidade para acessar o conteúdo ou serviço principal e a existência de alternativas menos arriscadas para atingir o mesmo resultado. Funcionalidades como reprodução automática contínua, notificações persistentes, recomendações personalizadas baseadas em histórico comportamental, *rankings* públicos, métricas de popularidade ou elementos de gamificação intensiva tendem a se situar fora do núcleo essencial, sobretudo quando associados a riscos de uso compulsivo, exposição excessiva ou exploração comercial.

Outro parâmetro relevante é o impacto da funcionalidade sobre os direitos da criança e do adolescente. Funções que ampliam significativamente a coleta de dados pessoais, intensificam a exposição a interações sociais abertas, estimulam comportamento aditivo ou viabilizam práticas comerciais direcionadas apresentam perfil de risco distinto e justificam tratamento regulatório mais restritivo. Nesses casos, a caracterização como não essencial permite que o Estatuto atue de forma preventiva, exigindo desativação por padrão, limitação etária ou mediação parental, sem inviabilizar o acesso ao serviço em si.

A análise também deve considerar a reversibilidade e a transparência. Funções não essenciais, quando mantidas disponíveis, devem ser facilmente identificáveis, compreensíveis e passíveis de ativação consciente, especialmente em ambientes acessíveis a crianças e adolescentes. A imposição de fricções adequadas para a ativação dessas funcionalidades constitui elemento relevante de conformidade, ao passo que sua integração opaca ou automática ao fluxo principal do serviço enfraquece a lógica de proteção por design adotada pelo Estatuto.

A conceituação que se propõe, portanto, é a de que “funções não essenciais ao funcionamento básico dos sistemas” correspondem a funcionalidades

acessórias que não são indispensáveis para o cumprimento da finalidade principal do produto ou serviço, especialmente aquelas associadas a engajamento intensificado, monetização, personalização comportamental ou ampliação de exposição. Essas funções devem ser objeto de modulação específica, podendo ser desativadas por padrão ou condicionadas conforme o risco e a faixa etária, preservando o núcleo funcional do serviço e assegurando aplicação proporcional e tecnicamente viável das obrigações previstas no Estatuto.

19. FUNDADOS INDÍCIOS DE QUE UMA CONTA É OPERADA POR CRIANÇA OU ADOLESCENTE (ART. 10)

A expressão “fundados indícios de que uma conta é operada por criança ou adolescente” desempenha papel relevante no Estatuto Digital da Criança e do Adolescente ao funcionar como gatilho para a adoção de medidas específicas de proteção, verificação, limitação de funcionalidades ou intervenção procedimental por parte dos fornecedores de produtos e serviços digitais. Trata-se de um conceito operacional sensível, pois se situa no ponto de contato entre deveres de diligência ativa e os limites técnicos e jurídicos da inferência automatizada, especialmente em contextos de incerteza etária e proteção de dados pessoais.

A necessidade de esclarecimento decorre do fato de que a noção de indício fundado não pode ser confundida com suspeita genérica, intuição subjetiva ou inferência isolada baseada em um único sinal. No ambiente digital, diversos elementos podem, de forma fragmentada, sugerir que um usuário é menor de idade, mas a utilização acrítica ou automática desses sinais como fundamento para medidas restritivas pode gerar erros relevantes, discriminação indevida, violações à privacidade e restrições injustificadas de acesso. O Estatuto não autoriza a adoção de medidas invasivas ou punitivas com base em presunções frágeis, mas exige um juízo qualificado, proporcional e tecnicamente justificável.

Para fins de aplicação da lei, os indícios devem ser compreendidos como sinais objetivos, verificáveis e consistentes, avaliados de forma contextual e cumulativa. Parâmetros adequados incluem a combinação de informações fornecidas voluntariamente pelo usuário, sinais comportamentais recorrentes e coerentes ao longo do tempo, padrões de uso compatíveis com determinadas faixas etárias e, quando disponíveis, sinais etários provenientes de sistemas confiáveis ou integrações técnicas legítimas. Nenhum desses elementos, isoladamente, deve ser considerado suficiente para caracterizar a operação da conta por criança ou adolescente.

Outro parâmetro essencial é a natureza e a intensidade da medida adotada em resposta aos indícios identificados. A existência de fundados indícios não autoriza automaticamente a suspensão da conta, o bloqueio permanente ou a coleta invasiva de dados adicionais. A resposta deve ser graduada e orientada por risco, privilegiando medidas proporcionais, como solicitação de confirmação etária, limitação temporária de funcionalidades sensíveis, reforço de configurações protetivas ou acionamento de mecanismos de supervisão parental. A adoção de medidas mais gravosas deve estar

condicionada à persistência dos indícios ou à confirmação por meios adicionais adequados.

A análise também deve considerar o risco de erro inerente a inferências automatizadas, especialmente quando baseadas em linguagem, preferências de conteúdo ou padrões de interação. Crianças e adolescentes não constituem um grupo homogêneo, e muitos comportamentos atribuídos a esse público podem ser igualmente observados em adultos. Por essa razão, o Estatuto deve ser interpretado de modo a evitar a normalização de práticas de vigilância ou categorização excessiva, reconhecendo explicitamente a possibilidade de falsos positivos e a necessidade de mecanismos de correção, contestação e revisão humana quando apropriado.

A transparência e a governança do processo também são elementos centrais. Sempre que medidas forem adotadas com base em indícios fundados, os usuários ou seus responsáveis devem ser informados de forma clara, compreensível e adequada à idade, sobre os motivos gerais da intervenção e sobre as opções disponíveis para esclarecimento ou regularização da situação. A ausência de transparência ou de canais acessíveis de contestação enfraquece a legitimidade das medidas e compromete a confiança no ecossistema digital.

A conceituação que se propõe, portanto, é a de que “fundados indícios de que uma conta é operada por criança ou adolescente” correspondem à identificação consistente e contextual de sinais objetivos que, avaliados de forma cumulativa, indiquem probabilidade relevante de uso por esse público, sem se basear em inferências isoladas ou presunções genéricas. Esses indícios devem ensejar respostas proporcionais, graduadas e orientadas à proteção, e não à punição, respeitando os princípios da minimização de dados, da transparência e da correção de erros. Essa leitura assegura a efetividade das salvaguardas do Estatuto, evita incentivos à vigilância excessiva e oferece parâmetros técnicos claros para a atuação responsável dos fornecedores e da autoridade reguladora.

*

*

*

A/C

Rodrigo Santana dos Santos

Coordenação-Geral de Normatização

Autoridade Nacional de Proteção de Dados - ANPD

São Paulo/SP, 12 de dezembro de 2025

Ref.: Considerações da Zetta sobre Tomada de Subsídios da ANPD sobre conceitos previstos no ECA Digital

A Zetta, associação que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, vem, por esta manifestação, apresentar contribuições à Tomada de Subsídios referente aos conceitos previstos no ECA Digital, publicada por essa Autoridade Nacional de Proteção de Dados (“ANPD”), e submetida à sociedade em 28 de novembro de 2025.

1. Quais os principais conceitos, termos e expressões previstos no Estatuto Digital da Criança e do Adolescente – Lei nº 15.211, de 17 de setembro de 2025 – que demandam esclarecimentos adicionais para a devida compreensão e aplicação da lei? Quais parâmetros poderiam ser considerados para tornar cada um desses conceitos, termos e expressões mais precisos?

É amplamente reconhecido que as diretrizes gerais do ECA Digital são relevantes e necessárias em um cenário marcado por rápidas evoluções tecnológicas, pela ampliação do acesso digital por públicos vulneráveis e pelos riscos associados à fase peculiar de desenvolvimento de crianças e adolescentes. O objetivo de proteção integral e prevenção de danos é, nesse contexto, legítimo.

Contudo, apesar de seu propósito geral protetivo, a legislação apresenta diversos pontos que carecem de esclarecimentos técnicos e normativos. Há termos não definidos, obrigações de difícil interpretação e situações que demandam regulamentação específica para assegurar a efetiva aplicação da lei, a segurança jurídica e a proporcionalidade regulatória.

Este é o foco central desta Tomada de Subsídios. A seguir, destacamos alguns dos temas que consideramos essenciais para detalhamento e harmonização normativa.

- No que se refere ao **relatório de transparência**, a lei determina de forma taxativa a obrigatoriedade de elaboração e divulgação pública para provedores que possuam mais de 1 milhão de usuários cadastrados (de crianças e adolescentes). Entretanto, o

texto legal não contém referência expressa ao resguardo de sigilo comercial, tampouco esclarece dois elementos fundamentais:

(i) se o número de 1 milhão deve ser aferido considerando o grupo econômico como um todo ou individualmente por produto/serviço, especialmente quando cada solução é operada por empresas distintas dentro do mesmo grupo; e

(ii) se provedores com menos de 1 milhão de usuários estariam dispensados tanto da elaboração quanto da divulgação do relatório, ou se continuam sujeitos a alguma obrigação residual.

- Outro ponto relevante refere-se à **vedação absoluta ao uso de técnicas de perfilamento**. O texto não diferencia as múltiplas modalidades técnicas envolvidas, como segmentação, clusterização, tagueamento e analytics, que, em muitos casos, são empregadas justamente para reforçar mecanismos de proteção, segurança e moderação, inclusive para o público infantil. Ademais, a simples distinção entre usuários maiores e menores de idade, necessária para fins de conformidade regulatória, pode ser caracterizada como uma forma de perfilamento. Assim, é imprescindível esclarecer o escopo e o limite da vedação, evitando interpretações que inviabilizem práticas essenciais para mitigação de riscos.
- Ao exigir que plataformas digitais ofereçam experiências adequadas à idade ou restrinjam o acesso a determinados serviços, a legislação determina a adoção de **mecanismos confiáveis de verificação etária**, vedando expressamente a autodeclaração. Neste sentido, é importante que a norma traga balizas mínimas que fundamentem a escolha da plataforma pelo mecanismo que entender mais confiável. Além disso, é importante que a realização de verificações não gere degradação da experiência do usuário nem imponha a necessidade de coleta de dados pessoais desnecessários.
- Adicionalmente, o ECA Digital dispõe que os **dados coletados para verificação de idade devem ser utilizados exclusivamente para essa finalidade**, vedado seu uso para qualquer outro propósito. Isso implica que informações sobre a verificação da idade não podem ser compartilhadas, reutilizadas ou integradas a outros fluxos de tratamento. Em contraste, a LGPD, combinada com o Enunciado nº 1 da ANPD, admite que dados pessoais desse público alvo sejam tratados com base nas hipóteses legais dos artigos 7º e 11, desde que prevaleça o melhor interesse do menor e haja autorização parental, conforme o artigo 14. Essa divergência entre os dois regimes reforça a necessidade de harmonização regulatória.

É essencial, portanto, que a regulamentação subsequente estabeleça critérios técnicos e objetivos para as definições em aberto, além de observar as particularidades de cada setor e os riscos atrelados àquele modelo, requisito fundamental para garantir que a aplicação do ECA Digital seja eficaz, proporcional e aderente aos princípios de proteção integral, sem impor obrigações idênticas a serviços com realidades e riscos substancialmente distintos.

A seguir, apresentamos os artigos previstos na Lei nº 15.211, de 17 de setembro de 2025 cujos conceitos, termos e expressões demandam esclarecimentos em nosso entendimento:

Dispositivo	Texto legal	Comentário
Art. 1º	Art. 1º. Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.	Necessário esclarecimento sobre o que se entende por "todo produto ou serviço de tecnologia da informação", inclusive, se a legislação é direcionada apenas para o setor privado ou se também é aplicável ao setor público.
	Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações: I. suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes;	Necessário esclarecimento, com critérios técnicos e objetivos, do significado de "suficiente probabilidade de uso e atratividade". Um exemplo de redação com maior objetividade é a referência a produtos, serviços e/ou funcionalidades intencionalmente direcionadas a crianças e adolescentes.
	II. considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e adolescentes; e	Necessário esclarecimento, com critérios técnicos e objetivos, do significado de "facilidade de acesso", particularmente à luz dos constantes avanços tecnológicos e ampliação de acesso ao seu uso.

	III. significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital.	Necessário esclarecimento, com critérios técnicos e objetivos, do significado de "significativo grau de risco à privacidade", especialmente levando em conta a Resolução 15 da ANPD que apresentou equivalência entre risco e dano, do significado de "permitir interação social" e "compartilhamento de informações em larga escala".
Art. 2º	Art. 2º Para os fins desta Lei, considera-se: [...] V. perfilamento: qualquer forma de tratamento de dados pessoais, automatizada ou não, para avaliar certos aspectos de uma pessoa natural, com o objetivo de classificá-la em grupo ou perfil de modo a fazer inferências sobre seu comportamento, situação econômica, saúde, preferências pessoais, interesses, desejos de consumo, localização geográfica, deslocamentos, posições políticas ou outras características assemelhadas;	Necessário esclarecimento acerca do conceito de perfilamento, com o estabelecimento de critérios técnicos e objetivos, inclusive do que não é considerado perfilamento (ex. classificação indicativa).
Art. 4º	Art. 4º A utilização de produtos ou serviços de tecnologia da informação por crianças e adolescentes tem como fundamentos: [...] VI. a proteção contra a exploração comercial;	Necessário esclarecimento, com critérios técnicos e objetivos, do significado de "exploração comercial", garantindo o diálogo com o princípio da liberdade econômica (Constituição Federal, art. 170).

	Art. 5º Os produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão observar os deveres de prevenção, de proteção, de informação e de segurança previstos neste Capítulo e nas Leis nºs 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), em conformidade com o princípio do melhor interesse da criança e do adolescente e da sua proteção integral, especial e prioritária. § 1º Os fornecedores dos produtos ou serviços de tecnologia da informação de que trata o caput deste artigo deverão adotar as medidas técnicas adequadas, inclusive mecanismos de segurança amplamente reconhecidos, que possibilitem à família e aos responsáveis legais prevenir o acesso e o uso inadequado por crianças e adolescentes.	Necessário esclarecimento, com critérios técnicos e objetivos, do significado, ou trazer parâmetros do que é “amplamente reconhecido”. Também recomendamos que seja considerada a diferenciação por porte e segmento de empresas para adoção de medidas técnicas mínimas exigidas. Necessário ainda esclarecimento, com critérios técnicos e objetivos, para o nível de controle parental exigido. Necessário esclarecimento, com critérios técnicos e objetivos, do significado de “uso inadequado”.
Art. 6º	Art. 6º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão tomar medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo	Necessário estabelecer diferenciação por porte e segmento de empresas para aplicação de medidas razoáveis.

	de prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com os seguintes conteúdos, produtos ou práticas: [...] III. indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e automedicação, automutilação e suicídio;	
	§ 2º Entre as medidas de prevenção previstas no caput deste artigo, incluem-se políticas claras, eficazes e adequadas à legislação brasileira de prevenção à intimidação sistemática virtual e a outras formas de assédio na internet, com mecanismos de apoio adequado às vítimas, bem como o desenvolvimento e a disponibilização de programas educativos de conscientização direcionados a crianças, adolescentes, pais, educadores, funcionários e equipes de suporte	Necessário estabelecer diferenciação por porte e segmento de empresas para aplicação de medidas previstas no artigo, objetivando entender se a aplicação de todos os requisitos é obrigatória a todo e qualquer modelo de negócio.

Zetta

	sobre os riscos e as formas de prevenção e de enfrentamento dessas práticas, nos termos de regulamento.	
Art. 7º	Art. 7º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo mais protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerados a autonomia e o desenvolvimento progressivo do indivíduo e justificado o melhor interesse da criança e do adolescente.	Necessário definir, com critérios técnicos e objetivos, do significado de "modelo mais protetivo disponível", considerando que pode ser rapidamente mutável em razão das inovações tecnológicas. Necessário estabelecer critérios de proporcionalidade por risco e tipo de serviço.
	§ 1º O produto ou serviço referido no caput deste artigo deverá, por padrão, operar com o grau mais elevado de proteção da privacidade e dos dados pessoais, observado que será obrigatória a disponibilização de informações claras, acessíveis e adequadas para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à eventual adoção de configurações menos protetivas.	Necessário definir, com critérios técnicos e objetivos, do significado de "grau mais elevado" e "configuração mais protetiva da aplicação".
Art. 9º	Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou	Necessário esclarecer de forma precisa em que consiste “conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade”, a fim de possibilitar

	acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos.	a operacionalização do artigo em pauta e evitar insegurança jurídica. Sugerimos também harmonizar a redação existente ao longo do texto legal, que implicaria na substituição da expressão “menores de 18 (dezoito) anos de idade” por “crianças e de adolescentes”.
	§ 1º Para dar efetividade ao disposto no caput, deverão ser adotados mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração.	Necessário definir ou exemplificar quais são os mecanismos de verificação de idade considerados confiáveis, considerando critérios relacionados às funcionalidades e aos riscos concretos dos serviços. Considerando que a autodeclaração é vedada pela lei, deve haver parâmetros para verificação de idade a cada acesso sem que isso implique em degradação da experiência do usuário, perdas econômicas significativas para as plataformas, coleta massiva de dados pessoais e considerando a inexistência de base de dados oficial do governo para checagem de informações. Além disso, sugerimos que a verificação de idade “a cada acesso do usuário” seja reavaliada a fim de evitar prejuízos à experiência do usuário. Uma sugestão seria excepcionalizá-la para casos como retomada de acesso após período de inatividade, ou alteração dos produtos e serviços oferecidos.
Art. 13.	Art. 13. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito.	Deve ser avaliada a possibilidade de realização do tratamento de dados coletados para a verificação de idade de crianças e de adolescentes para finalidades diretamente relacionadas ao seu melhor interesse, inclusive para combate e prevenção à fraude e para fins de prestação de contas.

Art. 16.	Art. 16. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar a pais, responsáveis legais, crianças e adolescentes, com acesso de forma independente da aquisição do produto, informações sobre os riscos e as medidas de segurança adotadas para esse público, incluídas a privacidade e a proteção de dados, em conformidade com o disposto no art. 14 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).	O texto conflita com as disposições da LGPD. Necessário esclarecer a redação do parágrafo único "sobretudo quando não realizados para fins que não os estritamente necessários para a operação", pois pode existir o tratamento de dados para outras finalidades, como prevenção à fraude. Necessário esclarecer também se o Relatório de Impacto aqui solicitado será o mesmo exigido pela LGPD e, de preferência, permitir a sua aplicabilidade também ao caso do presente texto legal. Necessário esclarecer se o tratamento realizado para fins não estritamente necessários para a operação configura tratamento sem finalidade ou adequação, podendo gerar fiscalização relacionada à LGPD.
	Parágrafo único. Na hipótese de tratamento de dados de crianças e de adolescentes, sobretudo quando realizado para fins que não os estritamente necessários para a operação do produto ou serviço, o controlador a que se refere o inciso VI do art. 5º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverá:	
	I. mapear os riscos e envidar esforços para mitigá-los; e	
	II. elaborar relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais, a ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e de	

Zetta

	adolescentes no ambiente digital, na forma de regulamento.	
Art. 17		
	Art. 17. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão: [...]	Esclarecer em quais situações deve haver o monitoramento de tempo de uso, considerando as funcionalidades e riscos concretos do serviços. A título de exemplo, citamos as aplicações do setor financeiro, que não são desenhadas para que a criança e/ou adolescente passem horas navegando. O objetivo é a transação financeira, e que o Eca já exige a gestão.
	IV. oferecer funcionalidades que permitam limitar e monitorar o tempo de uso do produto ou serviço.	
	§ 2º. O desenvolvimento e o uso de mecanismos de supervisão parental deverão ser orientados pelo melhor interesse da criança e do adolescente, considerado o desenvolvimento progressivo de suas capacidades.	Necessário considerar as funcionalidades e riscos concretos do serviço para o desenvolvimento do mecanismo de supervisão, além de estabelecer critérios técnico e objetivos para "desenvolvimento progressivo de suas capacidades", considerando que cada indivíduo se desenvolve de uma maneira e o mecanismo desenvolvido será único.
	V. controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação;	Necessário definir com critérios técnicos e objetivos em relação ao que seriam "sistemas de recomendação personalizados".
	VI. restrição ao compartilhamento da geolocalização e fornecimento de aviso prévio e claro sobre seu rastreamento;	Necessário esclarecer em quais hipóteses deve ocorrer a restrição ao compartilhamento de geolocalização, considerando funcionalidades e riscos concretos do serviço. Ex., aplicações do setor financeira utilizam geolocalização para fins de combate e prevenção à fraude.
	VIII. revisão regular das ferramentas de inteligência artificial, com participação de	Necessário definição com critérios técnicos e objetivos de "funcionalidades não essenciais ao funcionamento básico do sistema",

	especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes, garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas;	considerando que ferramentas de IA podem estar presentes nos sistemas por diversas outras razões, como para viabilizar a experiência adequada ao usuário, de acordo com sua faixa etária, para detecção de fraudes ou anomalias, dentre outras finalidades legítimas.
	IX. disponibilização, sempre que tecnicamente viável, de recursos ou de conexões a serviços de suporte emocional e de bem-estar, com conteúdo adequado à faixa etária e orientações baseadas em evidências, especialmente nos casos de interações com riscos psicossociais identificados.	Necessário definir com critérios técnicos e objetivos o termo "tecnicamente viável".
Art. 22.	Art. 22. Para além das demais disposições desta Lei, é vedada a utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e a adolescentes, bem como o emprego de análise emocional, de realidade aumentada, de realidade estendida e de realidade virtual para esse fim.	O artigo define perfilamento de maneira ampla, como qualquer tratamento de dados, automatizado ou não, que gere inferências para classificar a pessoa, abrangendo, portanto, todo e qualquer tipo de atividade. Necessário definir com critérios técnicos e objetivos se o agrupamento por faixa etária ou classificação indicativa é considerado perfilamento. Ou seja, esclarecer se o simples fato de segmentar o público entre maiores e menores de idade, justamente para identificar e proteger o segundo público, uma vez que algumas técnicas de programação são consideradas técnicas de perfilamento e são necessárias para garantir a aferição e segregação por idade. Ao vedar que haja publicidade com base em perfilamento, não fica claro se a lei está permitindo a publicidade sem que haja o

		perfilamento. Esclarecer, portanto, se é possível veicular conteúdo classificado como livre. Recomendamos esclarecer também se o ECA Digital estaria ignorando todas as outras disposições sobre publicidade infantil, como a Resolução 163/2014 do CONANDA, Código de Defesa do Consumidor e Conar, ou como ocorrerá a harmonização de tal proibição geral com a redação das outras normativas. Além disso, é importante manter a legitimidade de atividades de tratamento de dados pessoais de crianças e adolescentes - inclusive por meio de perfilamento - com a finalidade de proteção ao crédito. Isso inclui direcionamento adequado de produtos financeiros de forma responsável em linha com as normas setoriais de gestão integrada de riscos prudenciais e prevenção ao superendividamento.

Art. 26.	Art. 26. É vedada a criação de perfis comportamentais de usuários crianças e adolescentes a partir da coleta e do tratamento de seus dados pessoais, inclusive daqueles obtidos nos processos de verificação de idade, bem como de dados grupais e coletivos, para fins de direcionamento de publicidade comercial.	Avaliar a possibilidade de criação de perfis comportamentais para finalidades benéficas aos interesses de crianças e adolescentes e que não se confundem com publicidade comportamental, a exemplo de ofertas de recomendação de conteúdo educativo com base na faixa etária do menor.
Art. 27.	Art. 27. Os fornecedores de produtos ou serviços de tecnologia da informação disponíveis no território nacional deverão remover e comunicar os conteúdos de aparente exploração, de abuso sexual, de sequestro e de aliciamento detectados em seus produtos ou serviços, direta ou indiretamente, às autoridades nacionais e internacionais competentes, na forma de regulamento.	O STF incluiu na tese (ainda não transitada em julgado), uma obrigação de controle prévio para diversos crimes para "zelar para que tais conteúdos não sejam sequer publicados." O rol taxativo menciona os seguintes crimes: (i) terrorismo; (ii) indução ao suicídio ou à automutilação; (iii) pornografia infantil e crimes graves contra crianças e adolescentes e pessoas vulneráveis; (iv) tráfico de pessoas; (v) discriminação e discurso de ódio; (v) crimes contra mulheres em razão de gênero; e (vi) atos antidemocráticos. A responsabilidade, porém, estará configurada quando houver "falha sistêmica", ou seja, quando o provedor deixar de adotar medidas adequadas para prevenir ou remover esses conteúdos. Apenas 1 ou outro anúncio não caracterizaria uma falha sistêmica, por exemplo. Ela, ainda, é considerada "subjativa" pela tese. Por outro lado, o ECA Digital vai além ao

		estabelecer deveres concretos aos fornecedores de produtos ou serviços de tecnologia da informação, enquanto o STF define apenas o regime geral de responsabilidade civil. Necessário, portanto, que a redação do artigo seja esclarecida, no sentido que não se trata de imposição de monitoramento prévio ou vigilância generalizada, mas sim um dever ser atuação diligente e proporcional. Isso porque a imposição de “detecção” pode ser interpretada como obrigação de monitoramento prévio, podendo impactar na remoção automática de falsos positivos, com impacto sobre conteúdos lícitos (overblocking) e eventual censura estrutural.
Art. 31	Art. 31. Os provedores de aplicações de internet direcionadas a crianças e a adolescentes ou de acesso provável por eles que possuem mais de 1.000.000 (um milhão) de usuários nessa faixa etária registrados, com conexão de internet no território nacional, deverão elaborar relatórios semestrais, em língua portuguesa, a serem publicados no sítio eletrônico do provedor, que contenha: I. os canais disponíveis para recebimento de denúncias e os sistemas e processos de apuração; II. a quantidade de denúncias recebidas;	Considerando que a disponibilização do relatório deve ocorrer no site institucional, a obrigação de disponibilizar os sistemas e processos de apuração referentes aos aprimoramentos técnicos para a proteção de dados pessoais e privacidade, aos aprimoramentos técnicos para aferição do consentimento parental, bem como o detalhamento dos métodos utilizados, pode tornar pública diversas informações internas e estratégia dos provedores de aplicação. Diante disso, recomendamos que sejam apresentados os seguintes esclarecimentos: i) se os provedores que tenham até 1 milhão de cadastros nessa faixa etária estão desobrigados do relatório ou se há modulação da obrigação, e de quais; ii) esclarecer se deve ser considerado 1

	III. a quantidade de moderação de conteúdo ou de contas, por tipo; IV. as medidas adotadas para identificação de contas infantis em redes sociais, conforme o disposto no § 3º do art. 24, e de atos ilícitos, conforme o disposto o art. 27 desta Lei; V. os aprimoramentos técnicos para a proteção de dados pessoais e da privacidade das crianças e dos adolescentes; VI. os aprimoramentos técnicos para aferir consentimento parental conforme o disposto no § 1º do art. 14 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); e VII. o detalhamento dos métodos utilizados e a apresentação dos resultados das avaliações de impacto, identificação e gerenciamento de riscos à segurança e à saúde de crianças e de adolescentes.	milhão de cadastros por produto, e não por grupo econômico, considerando que um grupo econômico pode ter mais de uma empresa com produtos diferentes, cada qual com seu CNPJ e individual.
	Parágrafo único. Os provedores de aplicações de internet deverão viabilizar, de forma gratuita, o acesso a dados necessários à realização de pesquisas sobre os impactos de seus produtos e serviços nos direitos de crianças e de adolescentes e no melhor interesse deles, por parte de instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas, conforme critérios e requisitos	Necessário esclarecer o termo "dados necessários", incluir a necessidade de adoção de métodos que não identifiquem os titulares dos dados divulgados, e estabelecer as proteções necessárias em relação à proteção ao segredo comercial.

	definidos em regulamento, vedada a utilização desses dados para quaisquer finalidades comerciais e assegurado o cumprimento dos princípios da finalidade, da necessidade, da segurança e da confidencialidade das informações.	
Art. 33	Art. 33. Os provedores de aplicações de internet direcionadas a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar aos usuários informações claras e acessíveis sobre as hipóteses de uso indevido dos instrumentos de denúncia, bem como sobre as sanções cabíveis, observado o devido processo interno.	Necessário esclarecer que o termo "usuários" aqui, refere-se a usuários logados na plataforma.
Art. 35	Art. 35. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, em caso de descumprimento das obrigações previstas nesta Lei, assegurados o devido processo legal, a ampla defesa e o contraditório, os infratores estarão sujeitos às seguintes penalidades: I. advertência, com prazo para adoção de medidas corretivas de até 30 (trinta) dias; II. multa simples, de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício ou, ausente o faturamento, multa de R\$ 10,00 (dez reais) até R\$ 1.000,00 (mil	Necessário esclarecer se as sanções poderão ser aplicadas de forma cumulativa ou isoladas.

	reais) por usuário cadastrado do provedor sancionado, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;	
	III. suspensão temporária das atividades;	
	IV. proibição de exercício das atividades.	
	§ 1º. Para fixação e gradação da sanção, deverão ser observadas, além da proporcionalidade e da razoabilidade, as seguintes circunstâncias:	
	I. a gravidade da infração, considerados os seus motivos e a extensão do dano nas esferas individual e coletiva;	Avaliar a possibilidade de considerar como critérios para fixação e gradação da sanção as medidas de proteção adotadas pelo agente para proteção dos dados e da privacidade das crianças e adolescentes (boa-fé), o grau do dano, cooperação; políticas e governança, e adoção de medidas corretivas.
	II. a reincidência na prática de infrações previstas nesta Lei;	
	III. a capacidade econômica do infrator, no caso de aplicação da sanção de multa;	
	IV. a finalidade social do fornecedor e o impacto sobre a coletividade no que se refere ao fluxo de informações no território nacional.	
	§ 3º O processo de apuração das infrações ao disposto nesta Lei e de aplicação das sanções cabíveis reger-se-á pelas disposições relativas à apuração de infrações administrativas às normas de proteção da criança e do adolescente e à imposição das respectivas penalidades previstas na Lei nº 8.069, de 13 de julho de	A ANPD recebeu a atribuição de competência fiscalizatória e sancionatória do ECA Digital. Todavia, o ECADigital remete expressamente ao processo de apuração e aplicação das sanções às disposições da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Enquanto a fiscalização será conduzida pela ANPD, uma autoridade especializada com normativo próprios e atualizados, o ECA Digital, por sua

	1990 (Estatuto da Criança e do Adolescente).	vez, obriga a seguir um rito processual de 1990. É necessário que haja esclarecimento ou correção para que o processo de aplicação de sanções seja efetivo, mediante instrumento atualizado e que promova a justiça da fiscalização, além de esclarecer como será considerada a Lei nº 9.784/1999.
Art. 39	Art. 39. As obrigações previstas nos arts. 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 desta Lei aplicar-se-ão conforme as características e as funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o grau de interferência do fornecedor do produto ou serviço sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor.	Necessário definir com critérios técnicos e objetivos: os seguintes termos: • Grau de interferência • Número de usuários – que pode ser classificado como baixo, médio e alto, especificando parâmetro para que se configure como um ou outro • Porte do fornecedor – que pode ser classificado como pequeno/micro fornecedor, médio, e de grande porte, considerando, inclusive, os parâmetros já utilizados pela ANPD na definição de agende de pequeno porte. • Características e funcionalidades – é um dos requisitos mais importantes pendentes de definição, uma vez que o próprio ECA Digital trouxe, no artigo 1º, III: “significativo grau de risco à privacidade, à segurança ou ao desenvolvimento biopsicossocial de crianças e de adolescentes, especialmente no caso de produtos ou serviços que tenham por finalidade permitir a interação social e o compartilhamento de informações em larga escala entre usuários em ambiente digital”.

	§ 1º. Os provedores dos serviços com controle editorial e os provedores de conteúdos protegidos por direitos autorais previamente licenciados de agente econômico responsável que não se confunda com usuário final estarão dispensados do cumprimento das obrigações previstas nos artigos referidos no caput deste artigo, desde que: [...] III. disponibilizem mecanismos técnicos de mediação parental de acesso facilitado que permitam aos pais ou responsáveis legais exercer o controle sobre a forma com que crianças e adolescentes usam o serviço, a fim de possibilitar a restrição de:	Necessário esclarecer se por "mediação parental" entende-se o mesmo que supervisão parental, uma vez que o termo "mediação parental" não está definido na Lei, tampouco é referenciado em outros momentos.

Tomada de Subsídios - ANPD

Conceitos previstos no ECA Digital

1. Fundamentos hermenêuticos e metodológicos para a regulamentação do ECA Digital

A Câmara Brasileira da Economia Digital, entidade multissetorial que representa diversos provedores de serviços digitais em atuação no Brasil, reconhece a relevância de que sejam esclarecidos os principais conceitos e termos previstos na Lei nº 15.211/2025 e coloca-se à disposição para colaborar com um diálogo produtivo, transparente e embasado em evidências.

Trata-se de um marco regulatório recente, que inaugura um conjunto significativo de obrigações e que exigirá, de todos os atores - reguladores, empresas e sociedade civil - um processo de construção interpretativa incremental, cuidadoso e coerente com a complexidade do ecossistema digital.

A regulamentação do Estatuto Digital da Criança e do Adolescente exige uma hermenêutica que reconheça que o direito, especialmente em matérias tecnológicas, opera com conceitos cuja concretização não é automática, mas depende da articulação entre **estabilidade semântica**, **coerência sistêmica** e **sensibilidade ao contexto**. A tradição interpretativa indica que normas jurídicas não são instruções mecânicas: elas integram um sistema de princípios que precisam ser compreendidos à luz de seu propósito normativo, evitando tanto arbitrariedades quanto rigidez excessiva.

Assim, ao densificar termos como “acesso provável”, “medidas eficazes”, “funcionalidades não essenciais” ou “modelo mais protetivo”, o regulador deve buscar sentidos que sejam publicamente justificáveis, operacionais e compatíveis com a integridade do sistema jurídico, sem reduzir conceitos complexos a propriedades contingentes de tecnologias específicas ou a suposições generalistas sobre modelos de negócio. Uma abordagem baseada em princípios, que não seja excessivamente restritiva, oferece a maior flexibilidade para acomodar tecnologias em desenvolvimento e conceitos relacionados.

Nesse mesmo espírito, torna-se fundamental distinguir entre **propriedades definitórias** e **propriedades acidentais** dos conceitos. Muitas expressões da lei designam categorias normativas cujo núcleo essencial deve ser preservado (proteção integral, proporcionalidade, minimização de

dados, melhor interesse de crianças e adolescentes), mas cujos contornos variam conforme a arquitetura dos serviços digitais. Fixar interpretações baseadas em características tecnológicas transitórias, ou associadas a funcionalidades que não são inerentemente arriscadas, produziria assimetrias regulatórias e imporá obrigações que não capturam o risco real. A interpretação deve identificar **propriedades necessárias** (como a exposição concreta a danos graves) e afastar **propriedades contingentes** (como a simples existência de um canal de interação), sob pena de comprometer a coerência regulatória e a efetividade do Estatuto.

Em ambientes marcados por pluralidade tecnológica e diversidade de interesses legítimos, a decisão normativa precisa atender ao critério da **justificabilidade pública**: apenas interpretações que possam ser defendidas perante todos os afetados - cidadãos, empresas, famílias e o próprio Estado - em termos de razões acessíveis e não arbitrárias podem ser consideradas legítimas. Isso significa reconhecer que: (i) tecnologias diferentes não compartilham, necessariamente, o mesmo perfil de risco; (ii) serviços digitais desempenham funções heterogêneas; e (iii) expressões legais abertas precisam de critérios verificáveis para evitar oscilações interpretativas. Construir sentidos compartilhados das palavras implica oferecer parâmetros claros que permitam a qualquer agente saber, com razoável antecedência, o que a lei exige e por quê.

O enquadramento hermenêutico também ajuda a lidar com **lacunas axiológicas**: situações em que a letra da lei não contém, por si só, a orientação valorativa necessária para resolver casos não simulados pelo legislador. Em um ambiente de transformação acelerada, é inevitável que a legislação deixe espaços que devem ser preenchidos com prudência e razoabilidade. Nessas situações, a resposta interpretativa não deve se apoiar em presunções genéricas de risco, mas sim na proporcionalidade, experiência internacional e compreensão granular do ecossistema digital. A prudência interpretativa, isto é, a fidelidade às razões substantivas que justificam a norma, deve prevalecer sobre leituras maximalistas que convertam cláusulas abertas em obrigações universais e inflexíveis.

Ao mesmo tempo, a regulamentação precisa acolher que conceitos jurídicos aplicados ao ambiente digital exigem **análises incrementais e contextuais**, capazes de acomodar a heterogeneidade dos modelos de negócio e dos perfis de uso. Isso está em linha com o requisito obrigatório da Lei para um tratamento diferenciado e proporcional a serviços de diferentes naturezas, riscos e modelos de negócio. Não é possível partir do pressuposto de que toda funcionalidade é inerentemente arriscada ou de que todos os serviços devam ser disciplinados com a mesma intensidade regulatória. Em linha com a concepção dworkiniana de integridade, o regulador deve buscar soluções que mantenham coerência entre princípios constitucionais

(proteção integral, privacidade, liberdade de expressão, inovação, inclusão digital) sem anular nenhum deles.

Tais elementos hermenêuticos orientam a aplicação da lei para interpretações que sejam: (i) estáveis, para assegurar previsibilidade; (ii) baseada em princípios e flexível, para acomodar tecnologias em desenvolvimento; (iii) contextuais, para capturar riscos reais; (iii) axiologicamente justificadas, para refletir o propósito protetivo da norma; e (iv) compatíveis com a diversidade do ecossistema digital, permitindo calibragem fina entre proteção infantojuvenil, inovação tecnológica, inclusão digital e segurança jurídica.

2. Metodologia das contribuições

A partir desse conjunto de premissas interpretativas, adotamos uma metodologia estruturada para apoiar a regulamentação dos dispositivos que dependem de densificação conceitual. Cada dispositivo foi analisado sob três eixos:

- a. Identificação do conceito impreciso ou abertura semântica da lei;
- b. Diagnóstico do problema interpretativo e potenciais riscos de leituras excessivamente amplas ou restritivas;
- c. Proposição de um parâmetro interpretativo sugerido, com base em princípios jurídicos, práticas internacionais, proporcionalidade e riscos concretos.

3. Aplicação prática e diretrizes sancionatórias

É essencial que o enquadramento hermenêutico seja não apenas um guia para a produção normativa, mas também para a interpretação sancionatória. Como o ECA Digital inaugurará um novo regime regulatório ainda em consolidação, é indispensável que o processo de fiscalização e eventual responsabilização considere a novidade do marco legal, a complexidade técnica das adaptações e a diversidade de modelos de negócio envolvidos.

Assim como ocorre na trajetória da ANPD - a marcada por priorização do diálogo, proporcionalidade, consensualidade e educação regulatória - a aplicação do Estatuto deve estimular a adoção progressiva de melhores práticas, privilegiar a orientação prévia e assegurar que eventuais remédios sancionatórios sejam proporcionais, razoáveis e efetivamente direcionados a riscos reais. A política pública ainda está se consolidando, e a eficácia dependerá, em larga medida, de práticas sancionatórias que incentivem cooperação, aprendizado institucional e maturidade gradativa, e não meramente punição.

4. Contribuições específicas

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação.	“todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles”	Propõe-se que a regulamentação apresente esclarecimento acerca do que considera “todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles”, tendo em vista a amplitude das possibilidades de acesso previstas no parágrafo único, e a insegurança jurídica em relação aos destinatários da norma (a exemplo de questionamentos sobre a sua aplicabilidade ao setor público).
Art. 1º, Parágrafo único. Para os fins desta Lei, considera-se acesso provável por crianças e adolescentes as seguintes situações: I – suficiente probabilidade de uso e atratividade do produto ou serviço de tecnologia da informação por crianças e adolescentes; II - considerável facilidade ao acesso e utilização do produto ou serviço de tecnologia da informação por crianças e	“suficiente probabilidade de uso e atratividade” e “considerável facilidade ao acesso e utilização do produto”	Propõe-se que a regulamentação complemente esses conceitos com base em quatro eixos metodológicos: (i) Critérios verificáveis: os conceitos devem ser interpretados por meio de indicadores empíricos e verificáveis. Parâmetros possíveis incluem: canais e estratégias de marketing; natureza da jornada típica de uso; efetividade comprovada de controles de acesso implementados. (ii) Sentidos compartilhados e estabilidade semântica: o regulamento deve privilegiar significados linguísticos estáveis e replicáveis, evitando resultados divergentes para situações idênticas. “Probabilidade suficiente” não pode equivaler a “possibilidade remota”, e “considerável facilidade” não pode abranger serviços que implementam fricções reais e eficazes para mitigar acesso de menores. (iii) Adaptação incremental à inovação: a interpretação deve refletir a natureza gradual da evolução tecnológica. O

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
adolescentes;		conceito de “acesso provável” deve adaptar-se por meio de revisões periódicas baseadas em evidências, sem gerar deslocamentos abruptos ou obrigações retroativas. (iv) Avaliação contextual e baseada em risco: o foco deve estar no potencial concreto de dano, e não na mera possibilidade de acesso. Interpretação específica dos dois conceitos (i) “Suficiente probabilidade de uso e atratividade”: recomenda-se entendê-lo como: O conceito de «probabilidade suficiente de utilização e atratividade» combinado com «facilidade considerável de acesso e utilização», conforme referido no Art. 1.º, par. único, I e II, destaca a importância de avaliar tanto o apelo como a acessibilidade dos produtos ou serviços digitais, especialmente quando se considera o seu potencial impacto nos menores. Na prática, isso significa que plataformas, aplicações ou recursos que possam atrair e ser usados por crianças ou adolescentes (devido ao seu design, conteúdo ou popularidade) devem ser analisados não apenas quanto ao seu apelo inerente, mas também quanto à facilidade com que os menores podem acessá-los e interagir com eles. Ao avaliar esses critérios, é essencial considerar as ferramentas padrão e os mecanismos de controle parental disponíveis para restringir o acesso por menores. Muitos serviços oferecem controles parentais integrados, processos de verificação de idade e configurações de privacidade personalizáveis que permitem aos responsáveis limitar ou monitorizar as atividades online dos seus filhos. Essas ferramentas são projetadas para reduzir o risco de menores acessarem conteúdos ou recursos que podem não ser apropriados para a sua faixa etária, abordando assim as dimensões de atratividade e facilidade de acesso. (ii) A aferição deve considerar indicadores como: canais de distribuição; existência de funcionalidades claramente orientadas a públicos jovens; histórico de uso por menores em serviços análogos (nem todos são obrigatórios).

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		(iii) “Considerável facilidade ao acesso e utilização”: este conceito deve ser interpretado considerando: a simplicidade intrínseca do serviço; e a existência de fricções projetadas para mitigar o acesso de menores quando pertinente. Recomenda-se defini-lo como: <i>grau de simplicidade operacional que, na ausência de medidas eficazes de limitação, permitiria acesso desautorizado por menores, considerando o design do serviço, a jornada de uso e os mecanismos de controle implementados.</i> Um serviço que implementa fricções efetivas (como verificações contextuais, avisos ou zonas restritas) não deve ser enquadrado como de “considerável facilidade”, ainda que a navegação geral seja simples. Necessidade de integração entre os conceitos Os incisos I e II não devem operar isoladamente. Recomenda-se interpretação articulada na qual: (i) os conceitos de probabilidade e facilidade indiquem potencial de acesso; e (ii) o inciso III (“grau significativo de risco”) funcione como elemento de qualificação, diferenciando serviços neutros de serviços com potencial de dano concreto. A leitura preserva os princípios de proporcionalidade e modulação por porte, risco e natureza do serviço (art. 39 do ECA Digital). Reconhecimento da diversidade de modelos de negócio e necessidade de calibração setorial A regulamentação deve considerar que: (i) diferentes serviços possuem finalidades e perfis de risco distintos; e (ii) empresas devem ter flexibilidade para adotar medidas proporcionais ao seu risco. A regulamentação deve reconhecer que o tamanho da empresa, por si só, pode não ser condizente com o potencial de dano, e que mesmo empresas menores devem ser responsabilizadas por ações que possam causar dano agravado. Resultado esperado: uma interpretação orientada por esses

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		parâmetros proporcionará: (i) previsibilidade para decisões de design e investimentos; (ii) mitigação de riscos reais; (iii) alinhamento com boas práticas internacionais; (iv) adaptação proporcional a diferentes setores; (v) mensuração objetiva de cumprimento; (vi) capacidade de revisão incremental conforme evolui a tecnologia.
Art. 5º § 1º Os fornecedores dos produtos ou serviços de tecnologia da informação de que trata o caput deste artigo deverão adotar as medidas técnicas adequadas, inclusive mecanismos de segurança amplamente reconhecidos, que possibilitem à família e aos responsáveis legais prevenir o acesso e o uso inadequado por crianças e adolescentes.	“uso inadequado por crianças e adolescentes”	Propõe-se que a regulamentação apresente esclarecimento acerca do que considera um “uso inadequado por crianças e adolescentes”, tendo em vista a subjetividade contida no conceito e a multiplicidade de possíveis usos dos produtos ou serviços de tecnologia da informação por parte desse público.
Art. 6º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão tomar medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo	“Conteúdo impróprio para menores”, “mecanismos de apoio adequados” e “medidas razoáveis”	Os termos “conteúdo impróprio”, “mecanismos de apoio adequados” e “medidas razoáveis”, tal como formulados, carecem de maior densidade normativa e parâmetros interpretativos, sob pena de comprometer a previsibilidade da regulamentação e dificultar a aplicação consistente da lei. Problemas hermenêuticos gerais Os desafios decorrem de três características:

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
de prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com os seguintes conteúdos, produtos ou práticas: I – exploração e abuso sexual; II – violência física, intimidação sistemática virtual e assédio; III – indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e automedicação, automutilação e suicídio; IV – promoção e comercialização de jogos de azar, apostas de quota fixa, loterias, produtos de tabaco, bebidas alcoólicas, narcóticos ou produtos de comercialização proibida a crianças e a adolescentes;		(i) Amplitude semântica dos verbos normativos (“prevenir”, “mitigar”, “facilitar contato”, “exposição”), que podem abranger desde recomendações algorítmicas até simples indexação em mecanismos de busca internos; (ii) Categorias descritivas muito amplas, como “violência física”, “uso de substâncias”, “automutilação”, “práticas publicitárias predatórias” ou “conteúdo pornográfico”, que não apresentam distinção entre menção contextual e promoção ou incitação. É relevante haver uma diferenciação clara dessas categorias de conteúdo, quais são elas e como categorias se sobrepõem com conteúdo educacional, jornalístico e artístico; (iii) Ausência de parâmetros operacionais para aferir o que constitui “mecanismos de apoio adequados”, o que pode induzir diferentes órgãos reguladores a exigir abordagens incompatíveis, gerando insegurança jurídica e custos de conformidade desproporcionais. Esclarecer que estes conceitos devem ser lidos em conjunto com o padrão de proporcionalidade do Art. 39 e, portanto, que sua aplicação deve depender da natureza e do risco do serviço, é fundamental para mitigar um cenário de insegurança jurídica na interpretação da lei. Incorporar na orientação proteções explícitas para a expressão artística, o jornalismo, materiais educativos e informativos, e conteúdos similares que possuam valor intrínseco educativo, informativo, artístico e cultural. Sem qualificação adequada, o dispositivo pode levar a uma interpretação de que os provedores teriam responsabilidade objetiva pela mera presença ou possibilidade de descoberta de conteúdos sensíveis, ainda que o serviço não tenha qualquer curadoria editorial, não opere mecanismos de recomendação personalizados ou adote sistemas robustos de moderação. A orientação deve buscar equilibrar a necessidade de proteger as crianças com seu direito inerente de acesso à informação e contra a censura. Isso é explicitamente

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
V – práticas publicitárias predatórias, injustas ou enganosas ou outras práticas conhecidas por acarretarem danos financeiros a crianças e a adolescentes; e VI – conteúdo pornográfico.		reconhecido no Art. 37, Parágrafo Único. Sem a devida qualificação, esta disposição poderia limitar o acesso das crianças a informações valiosas online e limitar sua capacidade de desenvolver hábitos online responsáveis, resultados que são proibidos pelo Art. 4. Para que o artigo se torne operacional, harmônico e aplicável a diferentes modelos de negócio, é necessário especificar o alcance desses conceitos e estabelecer critérios objetivos que permitam aferir, de forma transparente, quando as medidas adotadas por um provedor são suficientes, proporcionais e eficazes. Parâmetros para interpretar “conteúdo impróprio para menores” A regulamentação deve refletir dois princípios fundamentais: (i) contextualidade, ou seja, a distinção clara entre conteúdo que promove, glorifica ou instrui práticas prejudiciais e conteúdo que menciona, discute ou descreve tais práticas em contextos educativos, jornalísticos, artísticos ou informativos; (ii) orientação a risco, para que a regulação se concentre nos cenários em que há probabilidade real de dano e não em menções neutras ou descritivas. Assim, recomenda-se que o regulamento esclareça que: (i) Conteúdos jornalísticos, educativos, literários, artísticos, informativos ou científicos não são considerados impróprios per se, desde que contextualizados e com finalidade legítima; (ii) Menções a violência, automutilação, uso de substâncias ou práticas de risco só se enquadram no art. 6º quando promovam, instruam, incentivem, incitem ou facilitem comportamentos prejudiciais, e não quando os descrevam ou alertem sobre seus riscos; (iii) A expressão “outras práticas conhecidas por acarretar danos financeiros” deve ser interpretada de forma a

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		contemplar o mesmo padrão axiológico, evitando ampliar indevidamente a noção de impropriedade e focando em danos efetivamente comprovados (como jogos de azar ou golpes financeiros específicos dirigidos a menores); (iv) “Conteúdo pornográfico” deve ser definido com base em critérios jurídicos já consolidados, evitando interpretações que incluam conteúdos afetivos ou educativos sobre saúde sexual ou reprodutiva, que possuem natureza diversa. Os parâmetros preservam a finalidade da lei (proteger menores de riscos reais) sem comprometer direitos fundamentais. Também evitam a necessidade de sistemas de moderação excessivamente intrusivos, garantindo proporcionalidade técnica e operacional. Parâmetros para interpretar “mecanismos de apoio adequados” A expressão “mecanismos de apoio adequados”, prevista no §2º, carece de precisão, pois não indica: (i) elementos programáticos mínimos; (ii) objetivos de proteção esperados; (iii) critérios de eficácia; (iv) diferenças proporcionais para serviços de risco baixo, médio ou alto. Sem clarificação, corre-se o risco de exigir dos provedores soluções idênticas, independentemente de suas capacidades técnicas, do perfil do serviço ou do nível de risco das interações que promovem. Para tornar o conceito aplicável, sugerimos que “mecanismos de apoio adequados” sejam entendidos como: (i) medidas compatíveis com o estado da técnica e viáveis na escala do provedor, levando em conta seu modelo de negócio, porte, perfil de risco e nível de interferência sobre

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		conteúdos; (ii) políticas claras sobre prevenção a comportamentos nocivos e orientações para situações envolvendo bullying, assédio ou exposição a risco, comunicadas de forma acessível e adaptadas ao público; (iii) mecanismos de apoio informacional, como links para serviços de apoio público e páginas de ajuda reconhecidas (ex.: canais oficiais de saúde mental, órgãos especializados, linhas de auxílio); (iv) mecanismos de denúncia acessíveis e responsivos, com prazos razoáveis de triagem e encaminhamento; (v) para serviços que não oferecem interação contínua ou contato social entre menores, mecanismos proporcionais e não intrusivos, evitando medidas mais típicas de redes sociais ou serviços de conteúdo audiovisual. Esses elementos oferecem clareza sem engessamento, permitindo que os provedores adaptem suas respostas aos riscos concretos das suas operações. Parâmetros para interpretar “medidas razoáveis” A expressão “tomar medidas razoáveis” deve ser entendida como a imposição de uma obrigação progressiva e proporcional aos provedores, com obrigações mais onerosas limitadas àqueles provedores que criam conteúdo, e obrigações menos onerosas para aqueles que podem geralmente distribuí-lo ou meramente direciona para conteúdos de terceiros, mas não têm controle editorial. Adotar essa abordagem alinha o Artigo 6 com o Artigo 39 e equilibra os direitos mais amplos dos menores com sua proteção. Necessidade de calibragem setorial e governança regulatória A proteção prevista no art. 6º só será eficaz se for aplicada de forma proporcional ao risco e compatível com a

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		diversidade de modelos de negócio, em vez de impor soluções uniformes a setores que apresentam exposições muito distintas. Assim, recomenda-se que: (i) seja enfatizada a necessidade de métricas objetivas, evidências empíricas e metodologias claras para aferição de cumprimento e descumprimento; (ii) sejam previstas revisões incrementais do regulamento, permitindo ajustes proporcionais à evolução tecnológica e a novas evidências sobre riscos e padrões de uso.
Art. 9º Os fornecedores de produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade deverão adotar medidas eficazes para impedir o seu acesso por crianças e adolescentes no âmbito de seus serviços e produtos. § 1º Para dar efetividade ao disposto no caput, deverão ser adotados mecanismos confiáveis de verificação de idade a cada acesso do usuário ao conteúdo, produto ou serviço de que trata o caput deste artigo, vedada a autodeclaração.	“produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos”; “medidas eficazes”; “mecanismos confiáveis de verificação de idade a cada acesso do usuário”	“Produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 anos” A expressão é ampla e, na forma em que está, pode abarcar uma variedade muito extensa de conteúdos e serviços, inclusive materiais de natureza literária, artística, científica, informativa ou educativa destinados ao público adulto em geral, mas não necessariamente proibidos por lei a menores. Para conferir segurança jurídica e estabilidade interpretativa, é importante vincular esse conceito a critérios normativos e classificatórios já existentes, evitando que percepções subjetivas sobre “impropriedade” levem à expansão descontrolada do escopo da lei. Propõe-se que, para fins do art. 9º, sejam considerados “produtos ou serviços de TI cuja oferta ou acesso seja impróprio, inadequado ou proibido para crianças e adolescentes” aqueles que: tenham oferta ou acesso expressamente vedados a menores pela legislação brasileira, como serviços de natureza pornográfica, jogos de azar, apostas, determinados conteúdos de natureza sexual explícita, produtos regulados (como bebidas alcoólicas, tabaco, armas, determinados tipos de narcóticos e congêneres); Nesse sentido, a regulamentação deve esclarecer que:

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		(i) referências a temas adultos em contextos legítimos (como obras literárias, artísticas, jornalísticas, educativas ou científicas) não são, por si, suficientes para enquadrar o serviço como “impróprio, inadequado ou proibido”; (ii) o foco do art. 9º recai sobre conteúdos ou serviços cuja fruição por menores é legalmente vedada, e não sobre toda e qualquer manifestação de temas “maduros” no espaço digital; (iii) a definição de “conteúdo pornográfico” deve se apoiar em parâmetros jurídicos consolidados, distinguindo material explicitamente voltado à excitação sexual de obras que tratem de sexualidade em contexto narrativo, informativo, histórico ou educacional. (iv) a classificação de um produto ou serviço nos termos do art. 9º deve ser baseada em uma parte substancial de suas ofertas; (v) um produto ou serviço deve criar ou exercer um grau significativo de controle editorial. A delimitação é essencial para preservar a coerência entre o ECA Digital e o restante do ordenamento, para evitar interpretações extensivas que tornem praticamente qualquer serviço potencialmente sujeito às obrigações mais rigorosas do art. 9º e para permitir que diferentes modelos de negócio ajustem suas práticas a partir de referenciais objetivos e estáveis. Essas limitações também são cruciais para garantir que os riscos potenciais adicionais, apresentados pela verificação de idade, sejam devidamente equilibrados com o objetivo de proteger os usuários. “Medidas eficazes” para impedir o acesso de menores O comando de adotar “medidas eficazes” pode, se interpretado de forma absoluta, ser lido como imposição de um padrão de resultado perfeito (“acesso zero”), aproximando-se de uma lógica de responsabilidade objetiva

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		pela presença de menores em qualquer contexto. Tal leitura seria incompatível com: (i) as limitações técnicas inerentes aos sistemas de verificação de idade; (ii) a natureza distribuída da responsabilidade pela proteção de crianças e adolescentes (Estado, famílias, escola, provedores); (iii) os princípios de proporcionalidade, razoabilidade e minimização de dados. É crucial que a regulamentação deixe claro que “medidas eficazes” correspondem a um dever de cuidado baseado em risco, avaliado à luz do estado da técnica, da viabilidade de implementação e dos resultados obtidos, e não a uma obrigação de eliminação absoluta de qualquer possibilidade de acesso indevido. Propõe-se que “medidas eficazes” sejam entendidas como: (i) conjunto de medidas técnicas e organizacionais, compatíveis com o estado da técnica e com a escala do serviço, razoavelmente capazes de reduzir de forma material e verificável a probabilidade de acesso indevido de menores a conteúdos, produtos ou serviços estritamente adultos; (ii) salvaguardas que equilibrem proteção e privacidade, evitando a coleta excessiva de dados ou a adoção de métodos desproporcionais ao risco (por exemplo, exigência de documentos oficiais em contextos de baixo risco ou em serviços de grande escala com pouca exposição a menores). A eficácia, assim, deve ser aferida por evidências e contextos e não por um ideal abstrato de segurança absoluta. Essa abordagem é consistente com modelos internacionais de regulação baseada em risco e com o art. 39 do ECA Digital, que prevê modulação de obrigações conforme o tipo de serviço, porte e grau de interferência do provedor.

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		“Mecanismos confiáveis de verificação de idade a cada acesso do usuário” O § 1º exige “mecanismos confiáveis de verificação de idade a cada acesso do usuário”, vedando a autodeclaração. A redação, tal como está, gera dúvidas importantes: (i) “a cada acesso” pode ser lido literalmente como exigência de verificação reiterada a cada visualização de página ou conteúdo, o que seria desproporcional, tecnicamente oneroso, potencialmente lesivo à privacidade e pouco compatível com a experiência de uso em serviços de grande escala; (ii) “mecanismos confiáveis” não são definidos, o que deixa em aberto o tipo de solução admitida em substituição à autodeclaração e o nível de garantia esperado; (iii) a vedação genérica à autodeclaração, sem clareza sobre alternativas, pode gerar incentivos a soluções excessivamente invasivas (como armazenamento de documentos ou biometria em larga escala), em tensão com os princípios da LGPD e parece abranger inadvertidamente a idade declarada pelos pais para menores, a qual pode ser altamente eficaz e confiável (ou seja, quando um dos pais fornece a idade de seu filho). Para tornar o dispositivo operacional e proporcional, recomenda-se que a regulamentação esclareça que: (i) “a cada acesso” deve ser interpretado de forma funcional e contextual, e deve abranger, dependendo da situação: o primeiro acesso a conteúdos expressamente vedados a menores pela legislação brasileira, considerando o risco efetivo que os conteúdos, serviços ou produtos representem a crianças e adolescentes; novos acessos após longo período de inatividade ou alteração relevante de contexto (dispositivo, perfil, sessão); mudanças substanciais no escopo de conteúdo acessado (por exemplo, migração de área geral para uma seção 18+); (ii) “mecanismos confiáveis” devem ser entendidos como

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		métodos de verificação cujo nível de garantia seja adequado ao risco, com parâmetros mínimos de precisão e proteção de dados; (iii) a vedação à autodeclaração simples (por exemplo, clicar em “sou maior de 18 anos” sem qualquer mecanismo adicional) não impede o uso de modelos de aferição que incorporem autodeclaração qualificada, dentro de arquiteturas mais robustas de confirmação de idade, desde que: exista algum elemento adicional de verificação ou controle; e/ou o sistema apresente nível de garantia compatível com o risco da atividade.
Art. 12. Os provedores de lojas de aplicações de internet e de sistemas operacionais de terminais deverão: I – tomar medidas proporcionais, auditáveis e tecnicamente seguras para aferir a idade ou a faixa etária dos usuários, observados os princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); II – permitir que os pais ou responsáveis legais configurem mecanismos de supervisão parental voluntários e supervisionem, de forma ativa, o acesso de crianças e de adolescentes a aplicativos e conteúdos; e	“Sinal de idade”, “aplicações de internet”, “lojas de aplicações” e “sistemas operacionais de terminais”	Termos como “aplicações de internet”, “lojas de aplicações” e “sistemas operacionais de terminais” apresentam grande variedade de significados na prática industrial, abrangendo desde sistemas móveis pessoais até softwares embarcados em aparelhos de uso doméstico compartilhado. A ausência de delimitação pode resultar em obrigações desalinhadas com o risco real que cada categoria de dispositivo apresenta para crianças e adolescentes. Necessidade de interpretação conforme risco e finalidade Para assegurar proporcionalidade e coerência com o art. 39 do ECA Digital - que exige modulação de obrigações segundo modelo de negócio, porte e grau de interferência - recomenda-se que tais conceitos sejam interpretados à luz dos seguintes parâmetros: (i) finalidade e arquitetura do dispositivo: distinguir dispositivos desenhados para navegação plena na internet (por exemplo, celulares pessoais) daqueles cuja funcionalidade é restrita (carros, relógios inteligentes ou e-readers); (ii) cenário típico de uso: dispositivos de uso pessoal e individual apresentam perfil de risco mais elevado; dispositivos domésticos compartilhados apresentam barreiras naturais de supervisão, o que reduz a pertinência

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
III – possibilitar, por meio de Interface de Programação de Aplicações (Application Programming Interface – API) segura e pautada pela proteção da privacidade desde o padrão, o fornecimento de sinal de idade aos provedores de aplicações de internet, exclusivamente para o cumprimento das finalidades desta Lei e com salvaguardas técnicas adequadas. § 1º O fornecimento de sinal de idade por meio de APIs deverá observar o princípio da minimização de dados, vedado qualquer compartilhamento contínuo, automatizado e irrestrito de dados pessoais de crianças e de adolescentes. [...] § 3º Ato do Poder Executivo regulamentará os requisitos mínimos de transparência, de segurança e de interoperabilidade para os mecanismos de aferição de idade e de supervisão parental adotados pelos sistemas operacionais e pelas lojas de aplicativo		de mecanismos de verificação no nível do sistema operacional; (iii) viabilidade de implementação em escala: alguns dispositivos não dispõem de interfaces adequadas para execução de mecanismos complexos de aferição ou transmissão de sinais de idade.

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
Art. 13. Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, <u>vedado seu tratamento para qualquer outro propósito</u> .	“vedado seu tratamento para qualquer outro propósito”	O art. 13 estabelece que “os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito”. A formulação, se lida de forma estritamente literal, cria um problema que pode ser descrito, em termos de teoria do direito, como uma lacuna axiológica: o sistema normativo oferece uma solução que, à luz de padrões valorativos centrais do próprio ECA Digital – em especial o princípio do melhor interesse da criança e do adolescente e os deveres de segurança, prevenção e responsabilização –, torna-se disfuncional. Ao proibir “qualquer outro propósito” sem distinções, o dispositivo acabaria vedando também usos dos dados que não ampliam a esfera de riscos, mas são justamente aqueles que tornam a verificação mais segura, auditável e protetiva, como (i) prevenção e combate a fraude, (ii) calibração e teste da acurácia do mecanismo, (iii) registro de logs para auditoria, revisão e gestão de incidentes, (iv) atendimento a requisições legais válidas e (v) oferta de experiências de uso adequadas à idade aferida. Nessa chave, o problema não é a finalidade de proteção em si, mas o desenho excessivamente estreito da finalidade textual, que ignora uma propriedade relevante do caso: o fato de que, para que a verificação de idade seja lícita, efetiva e segura à luz da LGPD, ela precisa ser acompanhada de um conjunto mínimo de tratamentos acessórios – todos ainda subordinados à mesma finalidade protetiva, e não a finalidades novas ou independentes, como perfilhamento comercial, publicidade comportamental ou exploração econômica dos dados. Se o intérprete toma ao pé da letra a expressão “qualquer outro propósito” e a aplica inclusive a esses usos instrumentais, produz-se a seguinte situação: o direito prevê uma solução que se mostra axiologicamente inadequada, porque desconsidera uma propriedade que deveria ser relevante (a necessidade de segurança, prevenção à fraude e accountability) e, por isso, precisa ser corrigida por via interpretativa. A regulamentação deveria, portanto, clarificar o alcance da

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		expressão “unicamente para essa finalidade”, distinguindo entre: (i) finalidades propriamente autônomas e ilegítimas, que devem ser vedadas; e (ii) finalidades instrumentais ou acessórias, intrinsecamente ligadas à própria verificação de idade e à proteção de crianças e adolescentes. Nessa segunda categoria, deveriam ser incluídos, de forma expressa, tratamentos como: prevenção, detecção e resposta a fraude ou tentativas de burlar o mecanismo; garantia de precisão, segurança e equidade do processo (calibração, testes, melhoria contínua); manutenção de registros e logs necessários à auditoria e à prestação de contas; atendimento a solicitações de autoridades competentes; e utilização dos dados estritamente na medida necessária para configurar experiências e salvaguardas adequadas à faixa etária aferida. Todos esses usos continuam subordinados à mesma finalidade matriz - cumprimento da lei e proteção do público infantojuvenil -, não constituindo uma “segunda finalidade”, mas desdobramentos operacionais da primeira. Além disso, deve se considerar que, a depender do método de verificação de idade utilizado, os mesmos dados podem ser coletados de forma independente e para finalidades distintas que, se fundamentadas em propósitos legítimos, não devem ser vedadas. Em termos de redação orientativa, “exclusivamente para essa finalidade” poderia ser entendido como o tratamento estritamente necessário e realizado com o exclusivo propósito de: (i) verificar a idade ou faixa etária do usuário para fins de conformidade com o ECA Digital e demais normas aplicáveis; e (ii) assegurar a precisão, segurança, responsabilização e efetividade desse processo, inclusive por meio de prevenção à fraude, registros de auditoria, resposta a incidentes, recursos e reverificações, e configuração de experiências compatíveis com a idade. Por outro lado, deveria ficar claro que são proibidos determinados tratamentos que desvinculem esses dados do contexto, em especial para compartilhamento com terceiros sem base legal específica e compatível. A interpretação preserva o núcleo da proteção buscada pelo

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		art. 13 - impedir que dados altamente sensíveis sejam reutilizados de maneira oportunista ou descolada do melhor interesse da criança e do adolescente - e, ao mesmo tempo, corrige a lacuna axiológica que resultaria de uma leitura puramente literal. Em vez de fragilizar a finalidade de proteção, a clarificação regulatória reforça a coerência interna do sistema: os mesmos princípios que limitam o uso (finalidade, necessidade, minimização, adequação) também exigem que a verificação de idade seja segura, auditável e eficaz, o que pressupõe um mínimo de tratamentos instrumentais alinhados a esse objetivo.
Art. 14. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar medidas técnicas e organizacionais para garantir o recebimento das informações de idade de que trata o art. 12 desta Lei.	“Medidas técnicas e organizacionais para garantir o recebimento das informações de idade de que trata o art. 12 desta Lei.”	O artigo apresenta um problema interpretativo típico de normas abertas: ela utiliza um conceito jurídico indeterminado sem fornecer parâmetros para aferir o que é esperado de cada provedor, tampouco como essa obrigação se articula com a realidade tecnológica, e as diferenças entre modelos de negócio. Por isso, a regulamentação deveria densificar o conceito de “medidas técnicas e organizacionais” em três frentes complementares: (i) Medidas proporcionais ao risco e ao modelo de negócio: o regulamento deve reconhecer que não existe uma solução única e uniforme. Marketplaces, serviços de conteúdo audiovisual, aplicativos de mensagens, sistemas de streaming e jogos têm perfis de risco e arquiteturas distintas. A exigência deve, portanto, referir-se ao estado da técnica razoavelmente disponível para o tipo específico de serviço, evitando impor mecanismos que são viáveis para plataformas de alto risco, mas absolutamente desproporcionais para serviços de intermediação ou classificados. (ii) Compatibilidade com a realidade técnica atual e com a ausência de padronização: como não há hoje infraestrutura estabelecida para transmissão de sinais de idade entre lojas, sistemas operacionais e aplicações, “medidas técnicas” não pode significar “resultados garantidos”, mas sim esforços diligentes e proporcionais, como: manter capacidade técnica para receber sinais quando forem disponibilizados;

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		implementar processos de registro, logs e validação que permitam interpretar corretamente sinais recebidos e evitar falsos positivos; A leitura evita transformar a obrigação em responsabilidade objetiva por falhas estruturais fora do controle do provedor. (iii) Medidas organizacionais compatíveis com o melhor interesse e a proteção de dados: no plano organizacional, o regulamento determina que os fornecedores adotem seus próprios mecanismos para prevenir o acesso indevido de crianças e adolescentes. O recebimento de sinal de idade e políticas, proteções e processos relacionados devem ser ferramentas para atingir essa obrigação. Isso pode exigir: políticas internas claras sobre como sinais de idade serão recebidos, armazenados e utilizados; processos de governança para avaliar coerência entre sinais distintos (sem exigir reconciliação automática ou transmissão de volta ao sistema operacional); e definição de procedimentos para lidar com casos em que o sinal não está disponível, é inconsistente ou se mostra tecnicamente inválido. Em suma, “medidas técnicas e organizacionais” deveria ser interpretado como o dever de criar condições para receber sinais de idade quando esses sinais existirem e forem interoperáveis, e não como a obrigação de garantir o recebimento universal, contínuo e padronizado, algo que não é factualmente possível diante da diversidade de dispositivos e da ausência de padrões abertos. Uma redação orientativa possível seria: <i>Para os fins do art. 14, consideram-se “medidas técnicas e organizacionais” aquelas que assegurem, de forma proporcional ao risco do serviço e compatível com o estado da técnica, a capacidade de receber e processar sinais de idade emitidos por sistemas operacionais ou lojas de aplicativos, quando tais sinais forem disponibilizados por meio de APIs interoperáveis e com especificações públicas. Tais medidas incluem procedimentos técnicos, processos de governança e controles de privacidade necessários para garantir a</i>

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		<i>recepção, interpretação segura e uso estritamente vinculado às finalidades desta Lei, sem implicar responsabilidade pela indisponibilidade de sinais fora do âmbito de controle do provedor.</i>
Art. 16. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar a pais, responsáveis legais, crianças e adolescentes, com acesso de forma independente da aquisição do produto, informações sobre os riscos e as medidas de segurança adotadas para esse público, incluídas a privacidade e a proteção de dados, em conformidade com o disposto no art. 14 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Parágrafo único. Na hipótese de tratamento de dados de crianças e de adolescentes, sobretudo quando realizado para fins que não os estritamente necessários para a operação do produto ou serviço, o controlador a que se refere o inciso VI do art. 5º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverá:	Inciso II: “relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais”.	A Autoridade deveria esclarecer o prazo e o formato do Relatório de Impacto, especificando quais informações deve conter e como a requisição pela autoridade administrativa irá funcionar. Sugestão: O Relatório de Impacto à Proteção de Dados Pessoais previsto no art. 5º, inciso XVII da LGPD deveria ser considerado como válido para cumprir com este artigo.

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
I – mapear os riscos e envidar esforços para mitigá-los; e II – elaborar relatório de impacto, de monitoramento e de avaliação da proteção de dados pessoais, a ser compartilhado sob requisição da autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital, na forma de regulamento.		
Art. 17, § 4º, V – controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação;	“controle sobre sistemas de recomendação personalizada” e forma de compatibilização do dispositivo com o oferecimento de conteúdo adequado à idade	A expressão não pode ser lida como se todos os sistemas de recomendação fossem homogêneos ou inerentemente arriscados. Sistemas de recomendação são categorias amplas de mecanismos algorítmicos com finalidades e impactos profundamente distintos: alguns são orientados à curadoria e adequação etária, enquanto outros têm como função promover engajamento contínuo ou impulsionar conteúdos. Tratar todas essas modalidades como equivalentes produz uma assimetria, pois desconsidera propriedades relevantes do caso (finalidade, arquitetura, impacto, intensidade de exposição) e gera soluções injustificadamente amplas, cujo resultado concreto contraria o próprio propósito protetivo da lei. Para evitar esse descompasso, as diretrizes regulamentares precisam explicitar que o dever de “controle” recai sobre sistemas de recomendação cuja finalidade ou design possa expor menores a riscos materiais. Por outro lado, recomendações personalizadas que funcionam como ferramentas de navegação, filtragem ou curadoria etária - por exemplo, mecanismos que auxiliam o usuário a encontrar conteúdo compatível com sua idade ou interesses legítimos - possuem natureza distinta e, em muitos casos, são parte da própria arquitetura de proteção. Desativá-los de maneira indiscriminada não apenas seria tecnicamente inadequado, como produziria um efeito regressivo: exporia crianças a resultados aleatórios,

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		conteúdos desconexos ou não classificados, justamente o oposto do que a lei pretende evitar. Assim, a regulamentação deve: (i) diferenciar sistemas de recomendação por finalidade e perfil de risco, reconhecendo que sistemas orientados à curadoria e adequação etária desempenham papel protetivo e não devem ser desativados automaticamente; (ii) permitir que a “opção de desativação” seja calibrada, de modo que o usuário possa desligar componentes associados a riscos, sem comprometer sistemas cuja função seja garantir classificação, filtragem e adequação etária; (iii) reconhecer que a personalização pode ser, ela própria, uma salvaguarda, especialmente quando utilizada para impedir que adolescentes acessem conteúdo destinado exclusivamente a adultos. O conceito de “controle sobre sistemas de recomendação personalizada” deve ser operacionalizado como controle sobre práticas de recomendação que criam ou ampliam riscos para menores, e não como um comando genérico para desligamento indiscriminado de toda e qualquer forma de personalização. A interpretação deve ser funcional, baseada em risco e guiada pelo princípio da proporcionalidade, garantindo que a norma opere como instrumento de proteção - e não como fator que, ao suprimir salvaguardas benéficas, aumente inadvertidamente a exposição de crianças e adolescentes a conteúdos impróprios.
Art. 17, § 4º, VIII – revisão regular das ferramentas de inteligência artificial, com participação de especialistas e órgãos competentes, com base em critérios técnicos que assegurem sua segurança e adequação ao uso por crianças e adolescentes,	“garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas” “funcionalidades não	O comando tem alto grau de abstração, que só produz resultados juridicamente consistentes se for interpretado de forma sistemática - evitando tanto a sobre inclusão quanto a subinclusão - e se for densificado por parâmetros funcionais. Lido literalmente, o dispositivo poderia ser entendido como autorização para desabilitar qualquer componente tecnológico acessório, o que deixaria de considerar propriedades decisivas do caso, como o papel da IA na moderação de conteúdo, na detecção de fraude, na curadoria

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
garantida a possibilidade de desabilitar funcionalidades não essenciais ao funcionamento básico dos sistemas;	essenciais ao funcionamento básico dos sistemas”	etária e na integridade da experiência. A desativação indiscriminada dessas funções produziria resultados incoerentes com o propósito protetivo da lei: aumentaria a exposição de menores a riscos, reduziria a capacidade de prevenção e comprometeria a segurança sistêmica. Para evitar essa distorção, é essencial que a regulamentação esclareça que “funcionalidades não essenciais” são apenas aquelas cuja presença ou ausência não afeta: (i) o funcionamento básico e contínuo do serviço; (ii) a segurança, integridade e confiabilidade da experiência do usuário; (iii) a adequação etária, proteção de menores e cumprimento das salvaguardas estabelecidas nesta Lei; (iv) a capacidade operacional mínima para prestação do serviço. Assim, a essencialidade não depende de o recurso ter sido implementado por meio de IA, mas de sua função no ecossistema da aplicação. Em muitas plataformas, modelos de IA são elementos estruturais para: detecção automática de conteúdo impróprio; filtragem de riscos; prevenção de fraude; identificação de padrões atípicos; curadoria e organização da informação; adequação etária; mecanismos de segurança e integridade transacional. Tais funcionalidades não podem ser consideradas “não essenciais”, sob pena de comprometer diretamente a capacidade de cumprir a própria lei. Nesse sentido, a desativação só pode recair sobre elementos cosméticos, acessórios ou recreativos, por exemplo: recursos supérfluos que não compõem o núcleo protetivo, operacional ou etário da aplicação. A regulamentação deve, portanto: (i) assegurar que as funcionalidades essenciais à proteção, à

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		adequação etária e à segurança permaneçam ativas e não possam ser desligadas sem comprometer a integridade do serviço; (ii) permitir que a “possibilidade de desativação” seja modulada conforme a natureza da funcionalidade e o risco envolvido; (iii) garantir que a exigência não gere obrigações tecnicamente inviáveis ou economicamente desproporcionais, especialmente em serviços de baixo risco ou arquitetura simples. Uma redação orientativa possível seria: <i>Para os fins do art. 17, §4º, VIII, consideram-se “funcionalidades não essenciais” apenas aquelas cuja desativação não comprometa o funcionamento básico do serviço, a segurança e a integridade da aplicação, a adequação etária, a moderação de conteúdo, a prevenção a fraudes, a filtragem de riscos, ou o atendimento das salvaguardas previstas nesta Lei.</i> A interpretação assegura que a norma opere como mecanismo de proteção, não de desmonte das salvaguardas, e reconhece que a IA, em muitos casos, é justamente a camada que viabiliza o cumprimento dos deveres legais.
Art. 17, §4º, IX – disponibilização, sempre que tecnicamente viável, de recursos ou de conexões a serviços de suporte emocional e de bem-estar, com conteúdo adequado à faixa etária e orientações baseadas em evidências, especialmente nos casos de interações com riscos psicossociais identificados.	“sempre que tecnicamente viável”	Para evitar distorções, a regulamentação deve estabelecer que a viabilidade técnica depende de três fatores cumulativos: (i) Disponibilidade objetiva de meios tecnológicos compatíveis com o tipo de serviço: é tecnicamente viável apenas o que pode ser implementado sem exigir monitoramento emocional do usuário, inferências sobre seu estado psicológico ou coleta de dados sensíveis que violem a LGPD. A viabilidade depende do que o serviço é, e não do que hipoteticamente poderia se construir à margem de sua lógica operacional. (ii) Compatibilidade com o modelo de negócio e a arquitetura de riscos da aplicação: serviços como marketplaces, classificados e intermediação de produtos não

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		geram ambientes de interação emocional, não exibem conteúdo sensível nem operam sistemas de “conversa”, “feed”, “thread”, ou “expressão pessoal”. Assim, a noção de gatilho psicossocial simplesmente não se aplica em termos técnicos. A viabilidade, portanto, não pode ser lida como obrigação de adicionar funcionalidades que desvirtuem o modelo do serviço, mas sim de integrar, quando cabível, interfaces externas (como links estáticos para canais públicos de apoio emocional) em contextos onde isso faça sentido, dados os potenciais riscos psicossociais. (iii) Proporcionalidade e razoabilidade técnica: a expressão “sempre que tecnicamente viável” não pode ser convertida em obrigação de criar sistemas de suporte emocional, contratar equipes especializadas, monitorar conversas ou desenvolver mecanismos de inferência comportamental, ou fornecer acesso adicional a sistemas. Isso violaria princípios da LGPD (minimização, limitação de finalidade) e estabeleceria um dever de cuidado impossível. A viabilidade, portanto, deve se referir a integrações simples e escaláveis, como links institucionais ou páginas informativas, quando o serviço efetivamente lida com situações nas quais o suporte emocional é relevante.
Art. 7 Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo mais protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerados a autonomia e o desenvolvimento progressivo do indivíduo e	“Modelo mais protetivo”	A expressão não oferece critérios sobre o que significa “mais protetivo”, qual é o parâmetro de comparação, como aferir disponibilidade técnica, quais elementos são essenciais versus opcionais, nem como equilibrar proteção com autonomia progressiva, privacidade, usabilidade e inovação. Para produzir resultados coerentes com a própria lei, o conceito precisa ser interpretado com base em critérios objetivos que permitam aplicação proporcional a serviços muito distintos — desde redes sociais até apps educacionais, jogos, streaming, marketplaces e serviços utilitários. O “modelo mais protetivo” não é um conjunto fixo e universal de controles. Ele deve ser lido de forma contextual e proporcional, considerando: (i) o tipo de serviço e sua arquitetura (social, audiovisual, transacional, educacional, utilitário);

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
justificado o melhor interesse da criança e do adolescente.		(ii) o perfil e intensidade dos riscos presentes; (iii) a sensibilidade do conteúdo ou das interações oferecidas; (iv) o grau de interferência do provedor sobre as experiências; (v) a maturidade técnica e disponibilidade de soluções compatíveis; (vi) a autonomia progressiva e o melhor interesse da criança, evitando controles excessivamente paternalistas. Assim, o “modelo mais protetivo” não é necessariamente o mais restritivo, mas sim o mais equilibrado, considerando riscos, proporcionalidade e garantias de privacidade. A regulamentação deveria estabelecer que: <i>O “modelo mais protetivo”, para fins do art. 7, é o conjunto de configurações iniciais que minimizam a exposição a riscos, reduzem coleta de dados, restringem contato potencialmente nocivo e organizam funcionalidades de forma segura, levando em conta o tipo de serviço, o risco apresentado, a disponibilidade técnica razoável e o desenvolvimento progressivo do usuário.</i>
Art. 7 §1 O produto ou serviço referido no <i>caput</i> deste artigo deverá, por padrão, operar com o grau mais elevado de proteção à privacidade e dos dados pessoais, observado que será obrigatória a disponibilização de informações claras, acessíveis e adequadas para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à	“Grau mais elevado de proteção da privacidade” “informações claras, acessíveis e adequadas”	A locução “grau mais elevado de proteção da privacidade” não pode ser interpretada de forma maximalista ou absoluta, pois desconsideraria que: diferentes serviços apresentam superfícies de risco distintas; nem todos os provedores têm o mesmo grau de interferência sobre a experiência do usuário; medidas excessivamente intrusivas podem violar princípios de minimização, necessidade e autonomia progressiva; proteção não equivale a eliminação total de funcionalidade ou coleta zero; a arquitetura técnica e o modelo de negócio influenciam o tipo de proteção viável. Assim, o “grau mais elevado de proteção da privacidade” deve ser interpretado como: a combinação, proporcional ao risco e ao contexto do serviço, de práticas de minimização de dados, limitação de tratamento, configuração restritiva como padrão e implementação de salvaguardas projetadas

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
eventual adoção de configurações menos protetivas		<i>para evitar exposição indevida de dados pessoais, especialmente sensíveis, de crianças e adolescentes, sempre compatível com o estado da técnica, com a finalidade do serviço e os melhores interesses.</i> A exigência de que menores e responsáveis recebam informações “claras, acessíveis e adequadas” também requer densificação, evitando que a obrigação seja interpretada como dever de: produzir relatórios extensos em linguagem jurídica; criar fluxos de onboarding complexos; implementar camadas intrusivas de consentimento; produzir conteúdos multimídia ou interfaces elaboradas, incompatíveis com serviços de baixo risco. O critério adequado deve ser funcional e proporcional ao risco, respeitando diferenças entre setores. Sugerimos que a regulamentação indique que consideram-se “informações claras, acessíveis e adequadas” aquelas fornecidas em linguagem simples, disponibilizadas em local de fácil acesso e suficientes para que menores e responsáveis compreendam, de forma proporcional ao risco, os efeitos de alterar configurações protetivas. Para serviços de baixo risco, a disponibilização de seção específica na política de privacidade ou centro de ajuda poderá ser suficiente para atender ao requisito.
Art. 22. Para além das demais disposições desta Lei, é vedada a utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e a adolescentes, bem como o emprego de análise emocional, de realidade aumentada, de realidade estendida e de realidade virtual para esse fim.	“publicidade comercial”	A ANPD deve esclarecer que a vedação ao uso de técnicas de perfilamento no ECA Digital é restrita à finalidade específica de direcionamento de publicidade comercial direcionada a crianças e adolescentes, nos termos da lei. O perfilamento permanece permitido para outras finalidades legítimas e necessárias, como segurança, prevenção à fraude, detecção de riscos, integridade de serviços e demais operações compatíveis com a proteção do interesse do usuário. Além disso, a lei também não proíbe a publicidade comercial em si de nenhuma maneira. A restrição estabelecida pelo artigo 22 limita-se ao uso da criação de perfis com o objetivo de direcionar publicidade comercial a menores. Diante de leituras expansionistas do dispositivo, é importante que a

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		ANPD esclareça o seu dispositivo e indique que está proibido, para fins de direcionamento de publicidade comercial - apenas o uso de “perfilamento” - definido no art. 2 como qualquer forma de tratamento de dados pessoais com o objetivo de avaliar determinados aspectos de um indivíduo para classificá-lo em um grupo ou perfil, fazendo assim inferências sobre seu comportamento, situação econômica, saúde, preferências pessoais, interesses, desejos de consumo, localização geográfica, movimentos, opiniões políticas ou outras características semelhantes. É igualmente importante definir com precisão o que se entende por publicidade comercial, distinguindo-a de outros tipos de comunicação digital — como mensagens institucionais, informativas ou de utilidade pública — e separar claramente as práticas de curadoria ou recomendação de conteúdo. Recomendações personalizadas que têm como objetivo melhorar a experiência do usuário e organizar o conteúdo disponível não devem ser confundidas com publicidade. Por fim, a ANPD deve esclarecer que a publicidade contextual — aquela baseada exclusivamente no conteúdo da página ou do vídeo que está sendo visualizado (ou baseada em dados demográficos e de localização), sem uso de perfil comportamental do usuário — é permitida, pois não envolve monitoramento prévio nem construção de perfis individuais.
Art. 28. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar aos usuários mecanismos de notificações acerca de violações aos direitos de	Segurança infantil vs. moderação de conteúdo	Os arts. 28 e 29 tratam, respectivamente, da obrigação de disponibilizar mecanismos de notificação de violações de direitos de crianças e adolescentes e da retirada de conteúdo ofensivo comunicada pela vítima ou seus representantes. No entanto, a redação atual não diferencia duas categorias regulatórias que, internacionalmente, são tratadas de maneira distinta por razões técnicas, operacionais e de proporcionalidade: (i) ameaças graves à segurança de crianças reais e identificáveis e (ii) conteúdos impróprios ou inadequados para determinadas faixas etárias.

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
crianças e de adolescentes. Parágrafo único. Notificados acerca de violações aos direitos de crianças e de adolescentes no âmbito de seus serviços, os fornecedores deverão, quando for o caso, oficializar às autoridades competentes para instauração de investigação, nos termos de regulamento. Art. 29. Para atender ao princípio da proteção integral, é dever dos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles proceder à retirada de conteúdo que viola direitos de crianças e de adolescentes assim que forem comunicados do caráter ofensivo da publicação pela vítima, por seus representantes, pelo Ministério Público ou por entidades representativas de defesa dos direitos de crianças e de adolescentes, independentemente de ordem judicial.		A ausência dessa distinção gera um problema hermenêutico relevante: o texto legal aproxima obrigações típicas de mitigação de riscos sistêmicos graves - como exploração, aliciamento, violência, assédio direcionado e situações de risco iminente - de obrigações próprias de moderação de conteúdo cotidiano, que envolvem adequação etária, classificação temática ou gestão de conteúdos genéricos e difusos. Tal fusão normativa cria uma lacuna: ao ignorar a diferença material entre esses dois fenômenos, a lei pode gerar obrigações desproporcionais para serviços de baixo risco, sobrecarga para autoridades públicas e perda de foco em ameaças reais à segurança infantil. Por essa razão, as orientações regulamentares precisam esclarecer que os arts. 28 e 29 se aplicam prioritariamente a situações em que há risco concreto, sério e individualizado à segurança, integridade ou bem-estar de uma criança ou adolescente, envolvendo vítimas reais, identificáveis ou identificáveis em potencial. Trata-se de casos como aliciamento, exploração sexual, violência dirigida, assédio reiterado, extorsão, bullying grave, exposição coercitiva ou condutas que criem risco iminente à vida ou à integridade psicofísica do menor. Nesses casos, a lógica é de “child safety”, alinhada à abordagem do NCMEC, das leis europeias sobre exploração infantil, do DSA e de padrões consolidados de governança internacional. Por outro lado, a lei não pretende, e não seria tecnicamente viável, exigir que provedores acionem autoridades competentes ou adotem procedimentos de remoção imediata em contextos de conteúdo genericamente inadequado, como temas sensíveis, linguagem inapropriada, imagens não recomendadas a determinadas idades ou conteúdos neutros cuja adequação depende de contexto ou classificação. Esses casos pertencem ao domínio ordinário da moderação de conteúdo, que deve ser tratada pelas políticas internas da plataforma, conforme regras próprias e proporcionais ao risco. A partir dessa distinção, recomenda-se que a regulamentação deixe claro que o art. 28 opera quando houver elementos que indiquem possível violação de direitos

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		envolvendo crianças reais, exigindo notificação às autoridades apenas quando a plataforma, com base nas informações recebidas, detectar risco grave, plausível e individualizado, e não meras discordâncias sobre conteúdo. De modo semelhante, o art. 29 deve ser interpretado como voltado à retirada célere de conteúdo que cause dano direto à vítima identificada, como cyberbullying, exposição indevida, conteúdo sexualizado envolvendo menores ou registros que possam perpetuar violência psicológica. A densificação confere racionalidade à aplicação dos dispositivos, evita que serviços de baixo risco - como marketplaces, aplicativos de funções utilitárias, streaming de música ou dispositivos conectados - fiquem sobrecarregados por obrigações descoladas de sua superfície de risco, e, ao mesmo tempo, fortalece a capacidade do Estado e das plataformas de atuarem nas situações realmente críticas. A regulamentação deve, portanto, estabelecer que os arts. 28 e 29 não se aplicam a todo e qualquer tipo de conteúdo inadequado, mas sim a condutas que “causem ou ameacem causar dano grave a uma criança real e identificável, ou criem risco iminente à sua vida, segurança ou bem-estar”. Isso permite que as plataformas continuem a tratar situações menos graves por meio de seus fluxos ordinários de moderação, mantendo proporcionalidade, eficiência e foco na proteção integral.
Art. 30, II. [No procedimento de retirada de conteúdo de que trata o art. 29 desta Lei, os fornecedores de produtos ou serviços deverão observar o direito de contestação da decisão, assegurando ao usuário que havia publicado o conteúdo:] II – o motivo e a fundamentação da retirada,	"Motivo e fundamentação da retirada"	A orientação sobre esta disposição deve esclarecer que a informação fornecida, bem como o nível de detalhe e tipo de informação, deve ser proporcional aos riscos inerentes à sua divulgação, e que os provedores podem ter flexibilidade em sua abordagem, dado o contexto de risco mais amplo. Em particular, os provedores precisam de flexibilidade em relação ao requisito de divulgar aos usuários os meios pelos quais se decidiu remover o conteúdo. Os provedores não devem ser obrigados a fornecer detalhes específicos sobre seus meios de detecção e análise de conteúdo. Fazer isso arrisca alertar malfeitores sobre como o conteúdo prejudicial é detectado, permitindo que burlem seus sistemas de proteção e ponham em perigo outros usuários. Esta informação, se exigida, só deve ser fornecida em

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
informando se a identificação do conteúdo removido decorreu de análise humana ou automatizada;		circunstâncias limitadas (por exemplo, quando o meio de detecção é relevante para a capacidade do usuário de exercer seu direito de recurso), permitindo descrição do fornecedor.
Art. 39. As obrigações previstas nos arts. 6º, 17, 18, 19, 20, 27, 28, 29, 31, 32 e 40 desta Lei aplicar-se-ão conforme as características e as funcionalidades do produto ou serviço de tecnologia da informação, moduladas de acordo com o grau de interferência do fornecedor do produto ou serviço sobre os conteúdos veiculados disponibilizados, o número de usuários e o porte do fornecedor. § 1º Os provedores dos serviços com controle editorial e os provedores de conteúdos protegidos por direitos autorais previamente licenciados de agente econômico responsável que não se confunda com usuário final estarão dispensados do cumprimento das obrigações previstas nos artigos referidos no caput deste artigo, desde que:	Serviços com controle editorial	Trata-se de um conceito que, sem densificação, permanece ambíguo e insuficiente para orientar a aplicação proporcional e coerente das obrigações do ECA Digital. A redação atual parece vincular a isenção ao <i>modo de seleção</i> de conteúdo (manual ou automatizado), mas essa não é a distinção relevante do ponto de vista do risco. O elemento central é se o serviço opera predominantemente com conteúdo profissional, curado, licenciado ou editorialmente controlado, ou com conteúdo gerado por usuários finais. Não se deve abranger mecanismos de buscas ou serviços de comunicação em tempo real, que podem permitir acesso a conteúdo gerado por usuário, mas que não cria e não exerce curadoria na mesma extensão que, por exemplo, uma plataforma de vídeo que exerce controle editorial. É essa distinção que determina o nível de risco para crianças e adolescentes e, portanto, o alcance das obrigações aplicáveis. Assim, a regulamentação deve esclarecer que o termo “serviços com controle editorial” se refere a serviços que disponibilizam principalmente conteúdo não gerado por usuários finais, cuja seleção, organização e disponibilização obedecem a critérios definidos previamente pelo provedor ou por agentes responsáveis pelos direitos autorais ou serviços como (mas não limitados a eles) mecanismos de buscas ou de comunicação em tempo real. O fato de o provedor utilizar mecanismos algorítmicos de triagem ou priorização não retira seu caráter editorial, desde que o processo permita excluir conteúdo que viole critérios pré-estabelecidos ou parâmetros de licenciamento, e que não haja espaço para postagem aberta de usuários finais. Plataformas de streaming, bibliotecas digitais, serviços de leitura, plataformas de vídeo com catálogo licenciado, players de música e serviços literários se enquadram nessa

Dispositivo	Conceito impreciso	Parâmetro interpretativo sugerido
		categoria quando não permitem upload público e mantêm curadoria ativa. A natureza editorial deriva da estrutura de controle sobre o <i>que entra</i> e o <i>que permanece</i> no catálogo, e não do modo técnico como esse controle é operacionalizado. No caso de serviços literários, a regulamentação deve reconhecer, de forma expressa, que livros e obras literárias tradicionalmente não se submetem a sistemas uniformes de classificação etária no Brasil. A tentativa de introduzir classificação obrigatória nesse contexto seria não apenas tecnicamente impraticável, mas contrária à proteção constitucional da liberdade artística e literária. Assim, serviços editoriais qualificados à isenção devem ser autorizados a utilizar classificações alternativas já adotadas pelo setor - categorias temáticas, sinalização de público-alvo, mecanismos robustos de controle parental - sem imposição de sistemas artificialmente importados ou desconectados da realidade editorial. O ajuste é coerente com o próprio espírito do art. 39: modular obrigações conforme características, tipo de conteúdo e grau de risco. A concretização do conceito de “controle editorial” deve enfatizar duas ideias centrais: primeiro, a isenção aplica-se a serviços que disponibilizam sobretudo conteúdo não gerado por usuários finais, profissionalmente produzido, licenciado ou curado; segundo, o controle editorial inclui tanto processos manuais quanto automatizados, desde que envolvam mecanismos claros de seleção, exclusão e conformidade com políticas de conteúdo. Por fim, em relação ao art. 39, § 1º, III, recomenda-se o esclarecimento do termo “mediação parental”, por se tratar de termo não definido ou mencionado em outros momentos ao longo do texto legal.

Submissão à Consulta Pública da ANPD sobre os conceitos fornecidos no ECA Digital

Dezembro de 2025

Sumário Executivo

A Meta parabeniza a ANPD pela iniciativa e agradece a oportunidade de contribuir para o diálogo com diversos atores da sociedade, visando uma regulamentação eficaz e proporcional do ECA Digital, baseada em soluções técnicas que promovem privacidade, segurança e proteção dos usuários. As principais contribuições são:

1. **Sistemas de recomendação personalizados (Art. 17, §4, V):** Defendemos controles parentais direcionados e proporcionais, priorizando riscos demonstráveis para menores, especialmente quanto a conteúdos inadequados à idade.
2. **Funcionalidades não essenciais (Art. 17, §4, VIII):** A IA é fundamental nos serviços digitais; desativá-la pode inviabilizar o serviço. Apenas recursos que possam ser desativados sem prejuízo funcional e que representem riscos a menores devem ser abrangidos.
3. **Sinal de Idade (Art. 12):** A verificação de idade via lojas de aplicativos e sistemas operacionais permite coleta mínima de dados e garante salvaguardas de privacidade.
4. **Alcance do Art. 9:** O conceito deve focar em plataformas voltadas a adultos ou que não adotem medidas efetivas para combater conteúdos inadequados, considerando apenas serviços classificados como "18+" pelo Ministério da Justiça.
5. **Escopo do Art. 1:** Solicitamos esclarecimento sobre "probabilidade suficiente de uso e atratividade" e "considerável facilidade de acesso e uso".
6. **Uso de dados pessoais para verificação de idade (Art. 13):** Defendemos que dados coletados para verificação de idade sejam usados para fins compatíveis (ex.: prevenção de fraudes, experiências apropriadas à idade), sempre com salvaguardas robustas e em conformidade com a LGPD.
7. **Publicidade Comercial (Art. 22):** O Art. 22 não proíbe publicidade comercial nem perfilamento em geral, apenas restringe o direcionamento de anúncios a crianças e adolescentes.

Submissão à Consulta Pública da ANPD sobre os conceitos fornecidos no ECA Digital

A Meta acolhe a oportunidade de contribuir para a consulta pública da Agência Brasileira de Proteção de Dados (ANPD) e, por meio desta submissão, oferece considerações sobre conceitos e parâmetros que podem ser abordados no escopo da Lei nº 15.211/2025 (ECA Digital). Nosso objetivo é aumentar a eficácia da lei e mitigar a incerteza jurídica. Encaminhamos também, como anexo, a submissão feita pela Meta à consulta pública do Ministério da Justiça sobre Mecanismos de Aferição de idade que pode auxiliar na compreensão de alguns dos pontos tratados a seguir.

Destacamos a importância de reconhecer que o risco está associado à ausência de um conjunto de ferramentas de controle e configuração, salvaguardas e limites aplicados de acordo com faixas etárias. Em linha com o ECA Digital e os princípios da LGPD, recomendamos que a regulamentação leve em conta as medidas de bem-estar digital e as características de design adequadas à idade disponibilizadas pelos provedores, considerando as melhores práticas, modelos de negócios diversos e diferentes tecnologias.

Assim, acreditamos que deve ser dada atenção especial aos seguintes conceitos dentro do ECA Digital:

1. "controle sobre sistemas de recomendação personalizados" (Art. 17, § 4º, V)

O conceito de "controle sobre sistemas de recomendação personalizados", conforme estabelecido nos Art. 17, § 4º, V do ECA Digital, requer uma interpretação cuidadosa para garantir a proteção eficaz dos menores online, sem impor requisitos desnecessários ou contraproducentes.

"Sistemas de recomendação personalizados" no contexto do ECA Digital devem se referir a funcionalidades que levem em conta as preferências e comportamentos dos usuários para garantir que o conteúdo que os usuários acessam e as experiências que têm, especialmente os adolescentes, seja apropriado à idade deles. Esses sistemas são frequentemente parte integrante do núcleo central dos serviços digitais, e a prerrogativa de desabilitá-los de maneira geral pode resultar na interrupção do funcionamento de recursos essenciais que não geram danos, e, pelo contrário, são elementos essenciais para assegurar o acesso a conteúdos relevantes ou apropriados para usuários brasileiros ou de regiões específicas. No contexto do ECA Digital, os controles parentais sobre esses sistemas devem ser especificamente voltados para proteger menores da exposição a conteúdos prejudiciais ou inadequados para a idade. Uma "exclusão" universal de toda personalização não é recomendada e nem exigida, pois pode degradar a experiência do usuário e obstaculizar o funcionamento de recursos que, na verdade, aumentam a segurança e a usabilidade.

O principal objetivo do ECA Digital é proteger crianças e adolescentes contra conteúdos inadequados e riscos online. Nesse sentido, quaisquer controles parentais sobre recomendações personalizadas devem ser proporcionais aos riscos reais enfrentados por menores, direcionados a danos demonstráveis, como exposição a material inadequado para a idade, e devem, sobretudo ser,

necessários para alcançar os objetivos de proteção estabelecidos pela Lei. Uma exigência geral de oferecer amplo controle ou "exclusão" universal sobre toda personalização vai além do espírito da lei e traria benefícios limitados de segurança, ao mesmo tempo em que exporia os adolescentes a experiências e conteúdos potencialmente mais problemáticos.

Para garantir a implementação eficaz e prática desse requisito, é necessário: (i) reconhecer a diversidade dos sistemas de recomendação e evitar comandos gerais para sua desativação; (ii) limitar os requisitos de controle a funcionalidades que representam riscos tangíveis para menores, como aquelas que podem expor crianças ou adolescentes a conteúdos inadequados à idade; e (iii) promover uma abordagem baseada em riscos e proporcional, que preserve capacidades essenciais de proteção e funcionalidade, ao mesmo tempo em que garante salvaguardas reforçadas onde os direitos e o bem-estar das crianças estão mais diretamente envolvidos.

Dessa forma, para cumprir a Lei, as plataformas podem focar na implementação de proteções padrão, utilizando ferramentas que visem "conteúdo inadequado para a idade". Além dessas medidas de proteção, e alinhadas com o desenvolvimento progressivo de capacidade dos menores, as plataformas também poderiam oferecer configurações personalizáveis para capacitar os adolescentes a controlar de maneira efetiva as recomendações e experiências de conteúdo, como silenciar ou esconder certos tipos de conteúdo, de acordo com sua idade e seu grau de maturidade. Ao combinar proteções padrão para conteúdos inadequados à idade com personalização controlada pelos próprios pais ou guardiães e/ou pelo próprio usuário, esses recursos proporcionam uma abordagem abrangente e flexível para proteger adolescentes online, respeitando também sua autonomia e capacidade de fazer escolhas informadas sobre seu ambiente digital. As plataformas também podem oferecer controles parentais, permitindo que os pais gerenciem a exposição a materiais potencialmente prejudiciais. Por exemplo, controles parentais que restringem o acesso a "conteúdo sensível" podem ajudar a limitar a visibilidade de material potencialmente prejudicial ou inadequado para adolescentes.

Ao combinar proteções padrão robustas com personalização orientada pelo usuário, as plataformas podem oferecer uma abordagem abrangente para proteger menores online, respeitando sua autonomia e apoiando seu desenvolvimento progressivo. Uma abordagem restrita e baseada em riscos efetivos para controlar sistemas de recomendação personalizada é essencial para proteger menores online. Ao focar nos riscos demonstráveis e capacitar pais e adolescentes com controles adequados, as plataformas podem cumprir o ECA Digital, mantendo recursos essenciais de serviço e apoiando o desenvolvimento saudável dos jovens usuários.

2. "funcionalidades não essenciais ao funcionamento básico dos sistemas" (Art. 17, § 4º, VIII)

Atualmente, as funcionalidades da inteligência artificial permeiam diversas características em produtos e serviços de tecnologia da informação, o que não deve ser interpretado necessariamente

como um risco inerente para crianças e adolescentes. Como é conhecido e será discutido com mais detalhes em legislações futuras e em futuras interpretações do próprio ANPD, sistemas e modelos de inteligência artificial podem envolver diferentes níveis de risco. Ou seja, a mera existência de um sistema/modelo de inteligência artificial em um produto ou serviço não deve, por si só, justificar automaticamente permitir que tal sistema/modelo seja desativado sob o ECA Digital. Sistemas/modelos de IA não são apenas um "recurso" que se implementa em um produto; a IA tem se convertido na infraestrutura e na interface do usuário que fazem o produto funcionar.

De acordo com o princípio da modulação estabelecido no Artigo 39 do ECA Digital, quando um sistema de inteligência artificial serve como parte do núcleo central de uma aplicação ou é essencial para o seu funcionamento, o sistema deve ser reconhecido como uma "funcionalidade essencial". Nesses casos, sua remoção/desativação efetivamente tornaria a aplicação inoperante ou obsoleta. Portanto, esses tipos de sistemas devem estar isentos de requisitos de desativação, pois desativá-los prejudicaria o propósito e a usabilidade do serviço. Essa abordagem garante que as obrigações regulatórias sejam aplicadas proporcionalmente e não comprometam a funcionalidade central dos produtos digitais contemporâneos. Também é essencial que novas funcionalidades de IA não sejam tratadas automaticamente como meros complementos, mas sim como aspectos integrais do serviço como um todo quando for o caso. Caso contrário, a regulamentação corre o risco de forçar rapidamente os usuários brasileiros a acessarem serviços obsoletos em comparação com consumidores em todo o mundo.

Em vez disso, o requisito de "possibilidade de desativar" deve se aplicar a funções que possam expor menores a riscos, que possam ser desativadas sem afetar o serviço central e que possam ser desativadas com segurança. Quando combinada com os requisitos do Artigo 12 (como consentimento parental para adolescentes baixarem aplicativos), configurações padrão e ferramentas adicionais de supervisão parental, como limites de tempo de engajamento e controles de conteúdo, essa abordagem oferece empoderamento abrangente dos pais e proteção dos jovens, mantendo a funcionalidade central dos serviços digitais.

3. "Sinal de idade" (Art. 12)

O Artigo 12 do ECA Digital do Brasil (Lei 15.211/2025) estabelece exigências claras para verificação de idade em ambientes digitais, visando proteger crianças e adolescentes online. A lei determina que os provedores de lojas de aplicativos e sistemas operacionais de terminais implementem medidas proporcionais, auditáveis e tecnicamente seguras para verificar a idade ou o grupo etário dos usuários. Além disso, exige que esses provedores habilitem APIs seguras para fornecer "sinais de idade" aos provedores de aplicações de internet, estritamente para conformidade com a lei e com as salvaguardas técnicas adequadas.

Um "Sinal de Idade" do sistema operacional ou de uma loja de aplicativos é uma combinação de uma faixa etária para o usuário e informações sobre onde essa faixa etária foi obtida e/ou

confirmada. Uma faixa etária deve ser composta por dois valores, um limite inferior e um limite superior. O limite superior pode ser nulo para representar "ou mais antigo". O limite inferior e superior deve ter pelo menos dois anos de diferença: 18+ (18, nulo), 16+ (16, nulo), 12-16 (12, 16), 9-18 (9, 18), 0-9 (0, 9).

Para permitir flexibilidade para diferentes jurisdições e necessidades de aplicativos, os aplicativos devem poder solicitar, por usuário, um conjunto de limites etários possíveis (até três limites, que correspondem a até 4 faixas etárias possíveis). Todos os limiares de idade devem estar abaixo de 18 anos, pois não é necessária granularidade de idade acima de 18 anos. Por exemplo, um aplicativo pode solicitar: limiar 12 e 16, permitindo saber se um usuário está 0-12, 13-15 ou 16+, ou limiares 9, 13, 18, permitindo que ele saiba se um usuário está localizado nas faixas 0-8, 9-12, 13-17 ou 18+.

O "sinal de idade" da loja de aplicativos/sistema operacional deve servir como o ponto de entrada principal para a verificação de idade. Para aplicativos não legalmente proibidos para usuários menores de 18 anos, a coleta de informações pessoais adicionais deve ser limitada, com foco em garantir a confiabilidade do sinal de idade recebido por meio de seus próprios mecanismos de garantia de idade.

Essa abordagem oferece uma implementação mais nuançada e eficaz de experiências adequadas à idade, pois permite um tratamento diferenciado com base no estágio de desenvolvimento e status legal do usuário. Também está alinhada com os princípios de transparência e responsabilidade, pois fornece critérios claros sobre quando e como recursos específicos de supervisão por idade devem ser disponibilizados.

4. "produtos ou serviços de tecnologia da informação que disponibilizarem conteúdo, produto ou serviço cuja oferta ou acesso seja impróprio, inadequado ou proibido para menores de 18 (dezoito) anos de idade" (Art. 9)

O Artigo 9 do ECA Digital do Brasil estabelece um regime mais restritivo para produtos e serviços de tecnologia da informação que disponibilizam conteúdos, produtos ou serviços considerados inadequados, inadequados ou proibidos para menores de dezoito anos, ou seja, serviços destinados a adultos.

A redação principal do Artigo 9 também usa o termo "*proibido para pessoas menores de 18 anos de idade*". Em outras palavras, embora o Artigo 9, parágrafo 2, parece exigir uma avaliação do conteúdo proibido por lei em geral, essa redação também se refere a conteúdo proibido para menores de 18 anos. A legislação brasileira não fornece uma lista abrangente de conteúdos que menores não podem acessar. Em vez disso, estabelece proibições específicas para menores (como restrições a anúncios de jogos de azar, armas de fogo ou álcool), mas não uma lista exaustiva.

O Artigo 9 pretende regular plataformas, serviços e produtos que são efetivamente direcionados a usuários maiores de 18 anos. Outros provedores cujo negócio principal não está relacionado a essas proibições, e que banem esse conteúdo inadequado em suas políticas empresariais e implementam

controles rigorosos para mitigar o risco de que tal conteúdo possa ser apresentado a crianças ou adolescentes, não devem estar incluídos no escopo do Artigo 9.

Os serviços mencionados no Artigo 9 devem ser limitados àqueles claramente rotulados, projetados e operados como **"18+"**, quando tal categorização resulte de classificação formal pelo Ministério da Justiça de acordo com o sistema de classificação etária. Essa delimitação é essencial para preservar a coerência entre o ECA Digital e o sistema jurídico brasileiro mais amplo, bem como para garantir a consistência regulatória, já que o Ministério da Justiça tem autoridade para atribuir classificações etárias indicativas a plataformas e serviços de acordo com os grupos etários, eixos e a justificativa estabelecida na Portaria de Classificação Etária (Portaria nº 1048/2025).

5. "probabilidade suficiente de uso e atratividade" + "considerável facilidade de acesso e utilização" (Art. 1, par. único, I e II)

O conceito de "probabilidade suficiente de uso e atratividade" combinado com "considerável facilidade de acesso e uso", conforme referenciado no Art. 1, par. único, I e II, destaca a importância de se avaliar tanto o apelo quanto a acessibilidade de produtos ou serviços digitais, especialmente ao considerar seu impacto potencial sobre menores. Na prática, isso significa que plataformas, aplicativos ou recursos que provavelmente atrairão e serão usados por crianças ou adolescentes (devido ao seu design, conteúdo ou popularidade) devem ser analisados não apenas pelo seu apelo inerente, mas também pela facilidade com que menores podem acessá-los e interagir com eles.

Ambos os conceitos (ou seja, "probabilidade suficiente de uso e atratividade" e "considerável facilidade de acesso e uso") devem ser esclarecidos por meio de regulações adicionais. Em vez de definir requisitos técnicos rigorosos, a orientação deve focar no objetivo final da proteção, capacitando os serviços a selecionar e implementar soluções adequadas para seus casos de uso específicos e considerações de risco.

De qualquer forma, ao avaliar esses critérios, é essencial considerar as ferramentas por padrão e os mecanismos de controle parental disponíveis para restringir o acesso de menores. Muitas plataformas agora oferecem controles parentais embutidos, processos de verificação de idade e configurações de privacidade personalizáveis que permitem aos responsáveis limitar ou monitorar as atividades online de seus filhos. Essas ferramentas foram projetadas para reduzir o risco de menores acessarem conteúdos ou recursos que possam não ser apropriados para sua faixa etária, atendendo assim tanto a dimensão acerca da atratividade quanto da facilidade de acesso.

6. "Os dados coletados para a verificação de idade de crianças e de adolescentes poderão ser utilizados unicamente para essa finalidade, vedado seu tratamento para qualquer outro propósito." (art. 13)

O Artigo 13 do ECA Digital deve ser interpretado em harmonia com os princípios gerais da LGPD e o padrão de "melhor interesse da criança", permitindo usos secundários compatíveis dos dados

coletados para verificação de idade. Importante destacar que este artigo não deve ser interpretado no sentido de proibir o uso das informações de idade em si, mas sim como regulando, por exemplo, o uso de documentos de identificação – como documentos de identidade emitidos pelo governo – especificamente para fins de verificação de idade. O foco, nesse caso ilustrativo, está em garantir que os documentos usados para verificar a idade sejam processados adequadamente, e não em restringir o uso de dados de idade verificados para outros fins legítimos e compatíveis, como se explica a seguir.

Especificamente, o processamento de informações etárias indispensáveis para garantir que crianças e adolescentes recebam experiências legalmente compatíveis e adequadas à idade, bem como para prevenir e combater fraudes que possam comprometer essas proteções, deve ser tratado como intrinsecamente conectado ao propósito original da verificação de idade, e não como um propósito novo incompatível, à luz da LGPD e do ECA Digital. Essa interpretação alinha limitação de propósito com os princípios da necessidade, proporcionalidade e minimização de dados, reconhecendo que, sem conhecer e aplicar a idade verificada, os provedores não podem implementar efetivamente as salvaguardas que motivaram a verificação inicialmente.

Para operacionalizar essa abordagem, os provedores devem poder processar dados de verificação de idade para fins compatíveis, tais como efetuar controles de acesso adequados à idade, bloqueio de conteúdo e recursos (*feature gating*), medidas de segurança por design, além de prevenção de fraudes que protejam menores, desde que salvaguardas robustas estejam em vigor e a LGPD seja cumprida. Esse arcabouço calibrado preserva a intenção protetora do Artigo 13, ao mesmo tempo em que permite aos provedores cumprir seus deveres legais de oferecer experiências adequadas, seguras e em conformidade com o melhor interesse da criança e do adolescente.

Além disso, as plataformas devem manter apenas os dados mínimos necessários relacionados à idade (como faixa etária e fonte de dados) ao longo do ciclo de vida da conta do usuário, estritamente para fins de garantia de idade e conformidade regulatória. Essa retenção é essencial para evitar coletar repetidamente informações pessoais e documentação a cada acesso ou interação, além de permitir a aplicação consistente de experiências apropriadas à idade, bloqueios de conteúdo e medidas de segurança desde o projeto. Ao reter informações derivadas da idade, em vez de cópias de documentos de verificação em estado bruto, por exemplo, as plataformas podem cumprir mandatos legais de forma eficiente, mantendo os princípios de privacidade e minimização de dados.

Essa abordagem calibrada permite que as plataformas melhorem continuamente seus mecanismos de garantia de idade, entreguem experiências seguras e em conformidade, e equilibrem medidas robustas de segurança com o imperativo de proteger a privacidade do usuário.

7. "Publicidade comercial" (art. 22)

De acordo com o ECA Digital, "perfilamento" é definido como qualquer forma de tratamento de dados pessoais destinada a avaliar certos aspectos de um indivíduo com o objetivo de classificá-lo em um grupo ou perfil, fazendo inferências sobre seu comportamento, situação econômica, saúde, preferências pessoais, interesses, desejos dos consumidores, localização geográfica, movimentos, opiniões políticas ou outras características semelhantes. O artigo 22 do ECA Digital proíbe especificamente o uso de técnicas de perfilamento para direcionar publicidade comercial a crianças e adolescentes. Além disso, a Lei não estabelece uma proibição total de todas as formas de publicidade direcionadas a menores (incluindo anúncios comerciais de vários tipos). Em vez disso, a restrição estabelecida no Artigo 22 é estritamente limitada ao uso de técnicas de perfil para fins de divulgação comercial para menores. Esclarecer o escopo do art. 22 é essencial para garantir a adequada interpretação e aplicação da Lei como uma questão de segurança jurídica e como forma de equilibrar a segurança e proteção dos jovens com uma atividade econômica de suma importância para as empresas brasileiras (especialmente as PMEs).

ANEXO

Submissão da Meta à Consulta Pública do Ministério da Justiça sobre Aferição de Idade (Novembro de 2025)

Índice

Sumário Executivo.....	5
Aferição de idade nas Lojas de Aplicativo e Sistemas Operacionais: Uma Visão Prática.....	6
Camadas de proteção sob o ECA Digital.....	6
Por que a verificação de idade e a aprovação dos pais no nível do SO/App Store são a melhor solução?.....	7
Implementação Técnica: A API de Idade para Compartilhamento Transparente de Sinais de Idade.....	7
Outros Mecanismos de Garantia de Idade.....	10
Abordagem da Meta sobre aferição de idade.....	11
Predição de Idade como uma ferramenta viável de garantia de idade para aplicativos.....	13
Retenção de Dados e Limitação de Finalidade.....	14
Capacitando Famílias: Aprovação Parental, Vinculação de Contas e Controles Parentais.....	16
Aprovação Parental e Estabelecimento do Vínculo Pais-Filho no Nível da Loja de Aplicativos/Sistema Operacional	16
Garantindo que Pais e Responsáveis tenham mais de 18 anos.....	17
Abordando Preocupações com o Compartilhamento de Dispositivos.....	18
Projetando para a Segurança: Contas para Adolescentes e Ferramentas de Supervisão Parental para Proteger Adolescentes nas Plataformas da Meta.....	19
Conclusões.....	22
Anexo A: abordagem aplicativo por aplicativo versus abordagem centrada nas lojas de aplicativos.....	23
Anexo B : API de Verificação de Idade.....	25
Anexo C: Exemplos de Vinculação Parental.....	28

Sumário Executivo

Brasil na vanguarda: Estabelecendo um Padrão Global

A Meta saúda a oportunidade de contribuir para a consulta pública do Ministério da Justiça do Brasil (“MJ”) sobre mecanismos de comprovação de idade. Com a publicação da Lei nº 15.211/2025 (“ECA Digital”), **o Brasil deu um passo legislativo inovador ao estabelecer uma estrutura robusta de aferição de idade, que inclui uma primeira camada no nível da loja de aplicativos/sistema operacional**. Esta nova lei exige que as lojas de aplicativos e sistemas operacionais verifiquem a idade do usuário e implementem Interfaces de Programação de Aplicativos (“APIs”) seguras e com privacidade por padrão para transmitir a idade ou faixa etária do usuário a provedores de aplicativos como a Meta. Este sistema inovador e baseado em mitigação de risco reconhece a diversidade do ecossistema digital e distribui responsabilidades de forma proporcional e coordenada, ao mesmo tempo que exige que serviços como a Meta utilizem os sinais de idade para implementar suas próprias medidas de aferição de idade e coloquem os adolescentes em experiências apropriadas para a idade.

A Meta apoia totalmente esta abordagem, que posiciona o Brasil na vanguarda dos esforços globais para proteger os menores online através de um design equilibrado que promove o acesso, a supervisão parental e a inovação. A estrutura de aferição de idade no ECA Digital aumenta significativamente a privacidade, permitindo que os usuários passem pelo processo de verificação de idade uma única vez com um provedor confiável. **Isso elimina a necessidade de jovens e suas famílias enviarem repetidamente documentação sensível** — como documentos de identidade emitidos por órgãos governamentais, selfies ou outros dados pessoais — para múltiplos aplicativos e serviços. Uma abordagem aplicativo por aplicativo imporia ônus consideráveis de tempo, privacidade e segurança às famílias.

É importante esclarecer que o apoio da Meta à abordagem da loja de aplicativos/sistema operacional não diminui nossa responsabilidade de garantir experiências seguras e apropriadas para a idade dos adolescentes em nossos serviços. Em vez disso, essa estratégia reconhece a realidade prática de jovens que acessam, no Brasil, a Internet majoritariamente por dispositivos móveis, usam inúmeros aplicativos e o contexto regulatório mais amplo da comprovação de idade. Em razão disso, **a verificação de idade no nível da loja de aplicativos/sistema operacional é a solução mais eficiente, consistente e sustentável** (Mais detalhes no [Anexo A](#)).

A Meta também reconhece e apoia a ênfase do ECA Digital em uma abordagem de “ecossistema completo”, conforme refletido no Artigo 15, que estabelece responsabilidade compartilhada e solidária entre todos os atores digitais para garantir experiências seguras e apropriadas para crianças e adolescentes. Isso exige esforços contínuos de todas as empresas para melhorar os métodos de aferição de idade e colaborar na adoção de soluções eficazes e alinhadas com o objetivo de proteger a privacidade. Para a Meta, isso significa prontidão para utilizar os sinais de idade da loja de aplicativos/sistema operacional em apoio a nossa abordagem em camadas de aferição de idade (conforme o descrito abaixo). Além disso, a Meta advoga pelo compartilhamento também em sentido contrário, enviando de volta ao nível das lojas de aplicativo e sistemas operacionais qualquer informação de idade mais confiável descoberta através de seus próprios processos de comprovação, permitindo que todo o ecossistema trabalhe de maneira conjunta.

A Meta continuará a agir de forma responsável, investindo em novas ferramentas e em nossa abordagem multi-camadas para entender a idade dos usuários e aumentar a precisão e a segurança com que o fazemos. **No entanto, acreditamos ser essencial que o Ministério da Justiça forneça orientação clara de que o sinal de idade da loja de aplicativos/sistema**

operacional deve servir como o ponto de partida principal para a verificação de idade. Para aplicativos legalmente permitidos para usuários menores de 18 anos, a coleta de informações pessoais adicionais deve ser limitada, com o foco em garantir a possibilidade de utilizar o sinal de idade e manter mecanismos contínuos de aferição de idade através de seus próprios mecanismos.

Este sistema minimiza o número de entidades que lidam com informações sensíveis, reduzindo o risco de vazamento ou uso indevido de dados e limitando a exposição de informações pessoais em todo o ecossistema digital. APIs seguras são especificamente projetadas para transmitir apenas as informações necessárias da faixa etária, e não dados detalhados ou de identificação, o que simplifica a experiência do usuário e mantém os princípios de minimização de dados e de privacidade desde a concepção (privacy by design). Isso garante que a comprovação da idade seja eficaz e respeitosa à privacidade do usuário.

No contexto da abordagem de “ecossistema completo”, também incentivamos o Ministério a considerar mecanismos que permitam aos aplicativos fornecer sinais de idade mais confiáveis, baseados em seus próprios métodos, para o sistema operacional ou loja de aplicativos. Tal fluxo de informações recíproco exemplificaria o espírito colaborativo e multisetorial do ecossistema, resultando em experiências mais seguras e apropriadas para jovens usuários.

Em resumo, a verificação de idade eficaz no Brasil depende da implementação consistente dos mecanismos estabelecidos pelo ECA Digital. As lojas de aplicativos devem transmitir de forma confiável os sinais de idade e aprovação parental para as plataformas, o que lhes permite aplicar - de partida - salvaguardas apropriadas para menores. O recebimento de informações precisas sobre a idade permite às plataformas adaptar melhor seus serviços, garantir o cumprimento da regulamentação brasileira e aprimorar a segurança para jovens usuários.

Aferição de idade nas Lojas de Aplicativo e Sistemas Operacionais: Uma Visão Prática

Camadas de proteção sob o ECA Digital

O arcabouço de aferição de idade do ECA Digital oferece proteção abrangente para crianças e adolescentes por meio de múltiplas proteções coordenadas. A base deste sistema é estabelecida no nível das lojas de aplicativos e dos sistemas operacionais, onde a verificação de idade e a aprovação dos pais são necessárias antes de acessar serviços digitais. Este ponto de controle universal garante que a maioria das responsabilidades de garantia de idade seja tratada antecipadamente, simplificando a conformidade e a segurança antes que os usuários interajam com aplicativos individuais.

Para a maioria dos aplicativos, particularmente aqueles não sujeitos aos requisitos específicos do Artigo 9, isso significa que a utilização dos sinais de idade e aprovação parental fornecidos pela loja de aplicativos ou pelo sistema operacional é um passo inicial fundamental em seus processos de aferição de idade. Este sistema ajuda a reduzir a proliferação de superfícies de processamento de dados pessoais e apoia práticas robustas de privacidade e minimização de dados em todo o ecossistema.

O ECA Digital reconhece que a proteção eficaz para menores pode exigir trabalho contínuo. A Meta reconhece que aplicativos como redes sociais devem continuar a promover experiências seguras para adolescentes e devem estar preparados para implementar medidas suplementares de garantia de idade, incluindo mecanismos para detectar e

responder casos em que os usuários tenham contornado os controles no nível da loja de aplicativos. No entanto, isso deve ser feito *depois* que o acesso tenha sido concedido com a aprovação/consentimento dos pais, em vez de um pré-requisito para a entrada inicial.

Por que a verificação de idade e a aprovação dos pais no nível do SO/App Store são a melhor solução?

A abordagem do Brasil concentra a aferição de idade no ponto de convergência em que os usuários acessam um dispositivo ou plataforma pela primeira vez, considerando que os dispositivos móveis são a principal porta de entrada à Internet pelos jovens. Ao implementar a verificação de idade e os controles parentais nesta camada, a informação da idade pode ser capturada com precisão e aplicada de forma consistente em todos os aplicativos e serviços instalados no dispositivo. Este sistema centralizado oferece uma base sólida para uma garantia de idade eficaz e supervisão parental desde o início da experiência online de uma criança.

- **Experiência Simplificada para Famílias.** Pais e responsáveis só precisam verificar a idade do filho uma vez, no nível do dispositivo ou da loja de aplicativos, eliminando a necessidade de verificações de idade repetidas vezes em vários aplicativos. As famílias são poupadas de ter que enviar documentos sensíveis (como documentos de identidade oficiais ou selfies) a inúmeros provedores de serviços diferentes.
- **Controle Parental Reforçado.** Mecanismos centralizados de verificação de idade e aprovação parental dão aos pais mais supervisão e controle sobre as experiências digitais de seus filhos. O sistema apoia o envolvimento parental contínuo, permitindo que os pais revisem, aprovem ou revoguem o acesso a aplicativos conforme necessário.
- **A capacidade existe e já é conhecida pelos desenvolvedores de aplicativos.** Google e Apple já conhecem a data de nascimento do usuário e as conexões parentais, e têm ferramentas de aprovação parental em suas lojas de aplicativos. Ambos têm APIs de Idade já implementadas ou em lançamento dentro de 2 meses. Tais APIs são mais simples para os desenvolvedores de aplicativos integrarem. Isso resulta em ferramentas eficazes de aferição de idade ao alcance sobretudo de aplicativos pequenos ou com menos recursos, alavancando o cumprimento do ECA Digital de maneira abrangente.
- **Privacidade e Segurança de Dados Aprimoradas.** APIs seguras e com privacidade desde a concepção garantem que apenas as informações necessárias (como a idade ou faixa etária) sejam compartilhadas com os aplicativos, em vez de dados detalhados ou de identificação pessoal. Essa abordagem mantém os princípios de minimização de dados e privacidade do usuário, reduzindo o risco de vazamento ou uso indevido de dados.
- **Apoio a um Ecossistema Digital Saudável e Competitivo.** A garantia de idade centralizada diminui as barreiras de conformidade para desenvolvedores novos e menores, que não precisam mais criar sistemas duplicados de verificação de idade para cada aplicativo.

Implementação Técnica: A API de Idade para Compartilhamento Transparente de Sinais de Idade

A importância do foco nas lojas de aplicativos e sistemas operacionais, bem como da API de Idade é corroborada pelo fato de que 96% da juventude brasileira de 9 a 17 anos acessa a Internet via celular (CETIC 2025). Desses, 78% ficam online várias vezes ao dia e 12% pelo menos uma vez ao dia. Em contraste, apenas 18% usam laptops, 16% usam computadores fixos e 16% acessam a Internet via videogames. Essa realidade centrada no celular torna a API de Idade especialmente relevante para o cenário de segurança online da juventude brasileira.

A API de Idade é uma interface a nível de sistema que fornece automaticamente a faixa etária e a fonte dos dados de idade do usuário do dispositivo para os aplicativos que ele escolheu usar. A faixa etária é calculada com base na data de nascimento da conta do dispositivo, e os limites para as categorias de idade podem ser personalizados para atender aos requisitos de diferentes jurisdições e necessidades de aplicativos.

Uma característica fundamental é que a data de nascimento do usuário é informada na no registro do sistema operacional. Dessa forma, a faixa etária é calculada automaticamente e compartilhada com os aplicativos. Por exemplo, se a conta do dispositivo representa uma criança de 10 anos, a API categorizará o usuário na faixa etária apropriada (como por exemplo "menor de 12 anos") e compartilhará apenas essa faixa com os aplicativos – não a idade exata ou a data de nascimento. Essa abordagem favorece a privacidade ao minimizar a quantidade de informações potencialmente invasivas transmitidas.

Funcionalmente, a API de Idade opera de forma muito semelhante a outras APIs fornecidas pelo sistema operacional. Os aplicativos podem se integrar facilmente com a API de Idade usando apenas algumas linhas de código, permitindo acesso transparente às informações de idade. O sistema operacional compartilha esses dados diretamente com o aplicativo no dispositivo, garantindo que terceiros não estejam envolvidos no processo. Além disso, usuários e responsáveis mantêm o controle e a transparência sobre seus dados, pois podem revisar quais aplicativos receberam informações de faixa etária por meio das configurações do dispositivo.

A API de Idade foi projetada para funcionar em conjunto com mecanismos de aprovação parental. Antes que um aplicativo receba informações de sinal de idade, a loja de aplicativos confirma a idade do jovem usuário e garante que um pai ou responsável tenha concedido permissão para a instalação do aplicativo. Esse processo reforça a supervisão parental e otimiza a conformidade para as famílias.

Essa API não é apenas um conceito teórico – ela já existe na prática. A Apple lançou sua *Declared Age Range API* em setembro de 2025, que oferece suporte à idade declarada pelo responsável globalmente. Em janeiro de 2026, a Apple expandirá a API para incluir a idade verificada pelo dispositivo no Texas, EUA. Da mesma forma, o Google está atualmente testando uma versão beta da *Play Age Signals API* e planeja lançá-la em janeiro para o Texas, EUA. Esses lançamentos representam um progresso significativo e devem ser estendidos ao Brasil para apoiar os requisitos regulatórios locais e aumentar a segurança online para menores.

Para mais informação, ver:

- Apple's Declared Age Range API: <https://developer.apple.com/videos/play/wwdc2025/299>;
- Next steps for apps distributed in Texas: <https://developer.apple.com/news/?id=2ezb6jihj>;
- Google Play Age Signals API:
[https://developer.android.com/google/play/age-signals/overview?fbclid=IwY2xjawODWzdleHRuA2FlbQlxMQBicmlkETF3bmJ5WWU1MktxdlZHSjZUc3J0YwZhchBfaWQBMAABHmOUvnixifJCbsyCrVKyJl8BzMd8ZdDYX_-vgqRdOGQaxC6LWBHWUiRYNCpb_aem_DAXX3hhWjFJm0x39Tb69lQ](https://developer.android.com/google/play/age-signals/overview?fbclid=IwY2xjawODWzdleHRuA2FlbQlxMQBicmlkETF3bmJ5WWU1MktxdlZHSjZUc3J0YwZhchBfaWQBMAABHmOUvnixifJCbsyCrVKyJl8BzMd8ZdDYX_-vgqRdOGQaxC6LWBHWUiRYNCpb_aem_DAXX3hhWjFJm0x39Tb69lQ;);
- Changes to Google Play for Upcoming App Stores Bills in the US:
<https://support.google.com/googleplay/android-developer/answer/16569691?hl=en>.

Os aplicativos já fazem requisições para milhares de outras APIs do sistema, tornando a integração da API de Idade uma extensão natural das práticas de desenvolvimento existentes. A API é projetada para ser flexível e adaptável a diferentes requisitos legais e necessidades de aplicativos, suportando dispositivos individuais e compartilhados.

Embora a API de Idade seja um passo significativo, atualmente ela está focada em plataformas móveis e pode não alcançar todos os usuários imediatamente. A cobertura se expandirá ao longo do tempo, e os aplicativos devem estar preparados para usar métodos alternativos de comprovação de idade quando a API não estiver disponível, ou se as empresas obrigadas a fornecê-la estiverem em desacordo com a lei.

Ao simplificar a conformidade para desenvolvedores, reduzir a carga e a redundância para as famílias e aprimorar a privacidade e a segurança para menores, a API de Idade apoia uma abordagem consistente e em todo o ecossistema para a aferição de idade. Ela ajuda aplicativos e plataformas a cumprir com as regulamentações emergentes sobre globalmente, não apenas no Brasil, e incentiva as melhores práticas internacionais. Conforme o referido acima, Google e Apple já se comprometeram a implantar essas soluções para cumprir com o *Texas App Store Accountability Act*, que entrará em vigor em 1º de janeiro de 2026.

Considerações sobre Privacidade

A API de Idade (API de Idade) foi projetada com privacidade e segurança em sua essência, garantindo que o compartilhamento do sinal de idade ocorra estritamente no dispositivo entre o sistema operacional e os aplicativos que o usuário escolhe instalar. Apenas a informação mínima necessária para experiências apropriadas para a idade é compartilhada—especificamente, a faixa etária e sua fonte de dados. Nenhuma outra informação do usuário, nem mesmo a data de nascimento, é transmitida para os aplicativos.

Principais salvaguardas de privacidade incluem:

- **Prevenção de Inferência de Aniversário:** O dispositivo lembra a faixa etária anterior fornecida aos aplicativos e continua a fornecer o mesmo sinal de idade por um tempo adicional aleatório após o aniversário do usuário. Isso impede que os aplicativos infiram a data de nascimento exata.
- **Controle do Usuário:** Os usuários podem forçar uma faixa etária atualizada através das configurações do dispositivo, caso prefiram não esperar pela atualização automática.
- **Limites de Configuração do Aplicativo:** Os aplicativos são restritos a no máximo de quatro faixas etárias, cada uma com pelo menos dois anos de diferença e todas abaixo de 18 anos. Essas faixas só podem ser alteradas cerca de uma vez por ano, reduzindo o risco de manipulação.
- **Limitação de Finalidade:** Os aplicativos podem usar o sinal de idade apenas para impor experiências apropriadas para a idade.

Essa abordagem centrada na privacidade garante que a API de Idade forneça um sinal de idade instantâneo e de alta confiança, o que é mais eficaz e menos intrusivo do que exigir verificação de identidade para todos OS USUÁRIOS. Para mais detalhes, consulte [Apple's Declared Age Range API](#).

Como os aplicativos podem usar o API de Idade de forma eficaz?

Os aplicativos podem aproveitar o API de Idade para aprimorar a proteção de adolescentes e simplificar a conformidade com as regulamentações de garantia de idade. Veja como:

- **Consultar o API de Idade no Lançamento do Aplicativo:** Os aplicativos devem verificar o sinal de idade sempre que um usuário começar a usar o aplicativo e usá-lo para aplicar proteções relevantes para o adolescente, tais

como:

- Bloquear a criação de conta abaixo da idade mínima do aplicativo
- Restringir o acesso a recursos ou conteúdo com limite de idade, o que pode ser aplicado mesmo antes de um usuário ter criado uma conta no serviço.
- Configurar configurações padrão apropriadas para a idade
- **Ferramenta Complementar na Caixa de Ferramentas de Aferição de Idade:** O API de Idade deve ser visto como uma ferramenta entre muitas. Os aplicativos continuam responsáveis pela garantia abrangente de idade e devem:
 - Usar padrões conservadores além de métodos alternativos de garantia de idade quando o API de Idade não estiver disponível
 - Continuar monitorando outros sinais e tomar medidas se informações de idade conflitantes forem detectadas (por exemplo, verificar novamente os usuários para confirmação adicional)
- **Personalizar para Necessidades Locais:** Os aplicativos devem personalizar as faixas etárias com base nas regulamentações locais e em suas necessidades específicas. Por exemplo, aplicativos mais simples podem exigir menos categorias de idade.

Integração do Ecossistema e Supervisão Parental

Conforme ilustrado nos diagramas no [Anexo B](#), a loja de aplicativos compartilha informações básicas de sinal de idade com aplicativos de terceiros somente depois que um pai ou responsável dá permissão e a loja de aplicativos confirma a idade do jovem usuário. Essas informações geralmente indicam se uma conta pertence a um adulto ou a um adolescente, ou se um adolescente está abaixo de uma certa idade— descrevendo a idade dentro de um intervalo em vez de especificar a idade exata do usuário.

A API de Idade oferece uma solução de alta confiança e preservação de privacidade para garantia de idade, permitindo que os aplicativos forneçam experiências mais seguras e apropriadas para a idade dos jovens usuários. Embora não seja uma "solução milagrosa", é uma ferramenta crítica no ecossistema mais amplo de proteção à juventude, especialmente em mercados mobile-first como o Brasil.

Outros Mecanismos de Garantia de Idade

O Ministério está estudando, com razão, outros mecanismos de aferição de idade que podem ser utilizados no nível da loja de aplicativos/sistema operacional e em outras superfícies, para garantir que, com o tempo, o sistema se torne mais forte e robusto. Tal objetivo está alinhado com o "Radar Tecnológico 5" da ANPD, que fornece uma avaliação abrangente dos diferentes mecanismos de garantia de idade disponíveis hoje. O documento destaca o papel crucial das lojas de aplicativos e sistemas operacionais nas soluções de aferição de idade, em conformidade com a Lei nº 15.211/2025 do Brasil (ECA Digital). O Radar Tecnológico considera a abordagem no nível da loja de aplicativos/sistema operacional como parte da "5ª Geração" (a mais atual) de mecanismos de aferição de idade, que se baseiam na integração da aferição e verificação de idade diretamente no nível estrutural do ecossistema tecnológico, permitindo que os aplicativos nas camadas superiores recebam apenas as informações necessárias sem ter que processar de maneira redundante dados pessoais do usuário, alinhando-se assim com os princípios de privacidade por design e minimização de dados (o que não é necessariamente o caso de outros mecanismos descritos na Consulta Pública do Ministério da Justiça).

A noção de uma "5ª Geração" de mecanismos de aferição de idade indica que a abordagem no nível da loja de

aplicativos/sistema operacional pode de fato ser conciliada com muitas outras soluções propostas para verificação de idade (por exemplo: Credenciais Digitais e soluções baseadas em carteira), e serve como uma porta de entrada preferencial nesta jornada para a construção de um ecossistema robusto de aferição etária no Brasil. No entanto, também é importante ressaltar que essas diferentes abordagens alternativas e complementares servem a propósitos distintos, com a solução no nível da loja de aplicativos/sistema operacional desempenhando um papel importante nesse mosaico de proteções disponíveis. A abordagem centralizada do sistema operacional reduz a duplicação de esforços, fazendo com que os adultos verifiquem sua idade apenas uma vez durante a configuração da conta, permitindo que os aplicativos aproveitem esse sinal de verificação mais tarde. Isso contrasta com soluções baseadas em credenciais e carteiras (para citar apenas dois exemplos), que envolvem maior atrito e complexidade para os desenvolvedores, exigindo processos como "troca de chave de assinatura" ou integração com muitos terceiros diferentes – desafios que aplicativos com menos capacidade operacional podem não ser capazes de arcar ou gerenciar. Embora essas soluções possam funcionar de forma integrada, uma implantação progressiva deve ser iniciada identificando o ponto de convergência comum em todos os produtos e serviços de TIC. Ao avançar, solicitamos gentilmente ao Ministério da Justiça que equilibre esses fatores com os objetivos que o ECA Digital está tentando alcançar em termos de proteção de crianças e adolescentes.

Abordagem da Meta sobre aferição de idade

Conforme descrito na Seção 1 acima, os sinais de idade das lojas de aplicativos e dos sistemas operacionais — juntamente com a aprovação parental para downloads de aplicativos — formam a camada fundamental e mais significativa de garantia de idade para jovens usuários no Brasil. Esses mecanismos estabelecem um patamar de proteção que assegura um grau básico de uniformidade em todo o sistema. Embora forneçam salvaguardas essenciais, a Meta reconhece que podem ser complementados por medidas adicionais dentro de aplicativos individuais. É importante ressaltar que, no nível do aplicativo, tais medidas devem ser consideradas não apenas pela ótica da aferição de idade apenas, mas como parte de um compromisso mais amplo com a segurança e com a privacidade, incluindo supervisão parental e outras proteções que contribuem para experiências seguras e apropriadas para a idade de menores. Abaixo, descrevemos como a Meta já está agindo para abordar a segurança desses usuários.

A verificação da idade do usuário é um desafio complexo e de todo o setor, que exige soluções ponderadas. Ao elaborarmos nossos métodos de aferição de idade, levamos em consideração 4 pontos principais enraizados nos *“melhores interesses da criança”*:

- **Privacidade:** queremos minimizar a coleta de dados adicionais para verificar a idade, a menos que seja proporcional ao risco;
- **Eficácia:** queremos garantir que os métodos que implementamos tenham resultados suficientemente confiáveis e que estamos tomando medidas para tornar nossos sistemas difíceis de contornar;
- **Equidade:** queremos fornecer transparência significativa ao usuário e oferecer ferramentas de apelação acessíveis por diversas populações globais; e
- **Proporcionalidade:** para quaisquer medidas de garantia de idade que implementarmos, queremos garantir que sejam proporcionais ao risco do erro considerando o impacto potencial tanto para o adolescente não detectado quanto para o adulto categorizado incorretamente.

A Meta tem investido recursos substanciais para aprimorar sua compreensão da idade das pessoas, e adotamos uma abordagem contínua e multifacetada para refinar nossa compreensão da idade ao longo de toda a jornada online. A realidade é que nenhum método funcionará 100% das vezes para todos os usuários. Assim, em vez de depender de um processo de etapa única, acreditamos que é mais eficaz construir e investir em um conjunto de ferramentas. Por exemplo, a Meta implementa as seguintes medidas em suas plataformas:

- **Coleta de idade no momento do cadastro:** Quando novos usuários se inscrevem, solicitamos a data de nascimento no registro da conta por meio de uma tela neutra em relação à idade. Usamos essa informação como linha base e a aplicamos em conjunto com outros sinais de idade disponíveis na grande maioria dos casos de uso. Esses sinais adicionais incluem idade prevista (com base na atividade e nos padrões do usuário), informações de idade de contas vinculadas e admissões de idade expressas, quando aplicável. A introdução do sinal de idade da loja de aplicativos no Brasil aprimorará significativamente essa abordagem multifacetada.
- **Deteção proativa de idade mínima:** Usamos tecnologia de análise de texto no Instagram e no Facebook para encontrar proativamente possíveis contas de menores de idade e removê-las de nossas plataformas.
- **Desenvolvimento de IA para detectar a idade do usuário:** Investimos na previsão de idade desenvolvida com IA para detectar prováveis adolescentes e garantir que recebam experiências apropriadas para a idade em uma variedade de casos de uso (por exemplo, restringir que adultos enviem mensagens para adolescentes que não os seguem).
- **Menu de opções de verificação de idade:** Em alguns casos, os usuários serão obrigados a verificar sua idade (por exemplo, se tivermos motivos para acreditar que estão mentindo sobre sua idade ou se tentarem editar a idade declarada anteriormente). Quando os usuários precisam verificar sua idade, empregamos diferentes opções para fazê-lo.
 - Atualmente, oferecemos verificação de identidade (Ex. RG) globalmente como uma forma dos usuários verificarem sua idade. No entanto, reconhecendo que nem todos têm acesso a documentação formal ou se sentem confortáveis em compartilhar esses dados online, oferecemos uma variedade de alternativas.
 - Fornecemos uma opção de estimativa de idade facial (também conhecida como "selfie em vídeo") por meio da Yoti para os usuários verificarem sua idade. A estimativa de idade facial refere-se à tecnologia que analisa características faciais para estimar a idade. Para a tecnologia da Yoti, os rostos nas selfies em vídeo não são rostos, são apenas um padrão de pixels. E pixels são apenas números. A tecnologia usa os padrões que reconhece nos números para estimar a idade. A Yoti estima a idade apenas a partir da selfie e não compartilhamos nenhuma outra informação sobre o usuário com a Yoti. A Yoti usa a selfie apenas para estimar a idade e sua tecnologia não consegue identificar o usuário. Assim que a estimativa de idade é concluída, a Meta e a Yoti excluem a selfie¹.
- **Denúncias da comunidade:** Qualquer pessoa pode denunciar contas suspeitas de menores de idade no Instagram e Facebook, e temos canais dedicados para revisar essas denúncias.
- **Treinamento de revisores de conteúdo:** Nossos revisores de conteúdo também são treinados para sinalizar contas denunciadas que parecem ser usadas por menores de idade. Se essas pessoas não puderem comprovar que atendem aos nossos requisitos de idade mínima, excluimos suas contas.
- **Educação de pais:** Lembramos aos pais sobre a idade mínima no [Guia para Pais do Instagram](#) e em nossa Central de Educação para Pais no IG.

¹ Meta: novas formas de verificação de idade no Instagram, 23 de julho de 2022.

<https://about.instagram.com/pt-br/blog/announcements/new-ways-to-verify-age-on-instagram>

- Em abril de 2025, publicamos um novo [recurso na Central da Família](#) para pais, da Psicóloga Pediátrica Dra. Lockhart, para compartilhar dicas sobre como ter conversas com seus adolescentes sobre a importância de fornecer a idade correta online e verificar e confirmar a idade de seus adolescentes em nossos aplicativos.

Predição de Idade como uma ferramenta viável de garantia de idade para aplicativos

A Meta está empenhada em promover tecnologias de aferição de idade para criar experiências online mais seguras para jovens usuários. Uma das abordagens mais promissoras é o uso de modelos de predição de idade, que utilizam inteligência artificial para estimar a idade de um usuário com base em uma variedade de sinais. Estamos continuamente aprimorando nossos modelos de predição de idade para aumentar sua precisão e confiabilidade. Esses modelos são projetados para se adaptar a novos padrões e dados, garantindo que nossos sistemas permaneçam eficazes à medida que os comportamentos dos usuários e os recursos da plataforma evoluem.

A predição de idade nos ajuda a fornecer experiências adequadas à idade para o maior número possível de usuários. O trabalho do nosso modelo de predição de idade (Classificador de Adultos) é ajudar a identificar se alguém é um adulto ou um adolescente². Usamos essa tecnologia para impedir que adolescentes acessem recursos destinados a adultos, como o *Facebook Dating*, impedir que adultos não conectados enviem mensagens a adolescentes que não os seguem, ajudar a evitar que adolescentes recebam conteúdo de anúncios restritos e garantir que o conteúdo que os adolescentes veem seja adequado à idade, mesmo que eles listem uma data de nascimento adulta.

A predição de idade, alimentada por IA, é uma ferramenta robusta e escalável para garantia de idade. Ela complementa outros mecanismos, como sinais de idade da loja de aplicativos e aprovação parental, e permite que as plataformas respondam dinamicamente a possíveis declarações falsas de idade, ajudando a manter jovens usuários seguros online. Da perspectiva de privacidade e proteção de dados, estamos focados em usar dados existentes para informar nossa tecnologia de inteligência artificial, o que nos fornece uma camada adicional de aferição de idade sem ter que solicitar mais dados para verificar a idade, a menos que seja proporcional a potenciais riscos. Se um tipo de sinal é incluído em nosso modelo, esse será determinado caso a caso por meio de um processo de revisão rigoroso, que avalia a proporcionalidade dos dados do sinal e identifica quaisquer salvaguardas de privacidade e proteção de dados que devamos implementar.

A Parte D do Relatório de Teste de Tecnologia de Garantia de Idade da Austrália conclui que a predição de idade “é um método de aferição de idade flexível e de baixa fricção que oferece uma maneira prática e de preservação da privacidade para avaliar se um indivíduo provavelmente atende a um determinado limite de idade – sem a necessidade de documentos formais de identidade ou datas de nascimento declaradas. Ela fornece aos provedores de serviços, reguladores e usuários uma ferramenta rápida e não intrusiva para avaliar a elegibilidade de idade, particularmente em ambientes de menor risco e/ou alto volume, como redes sociais, lojas de aplicativos e gateways de acesso a conteúdo.” Seus principais benefícios incluem:

- **Baixa Fricção para o Usuário:** Diferentemente da verificação baseada em documentos (que exige que os usuários carreguem uma identificação governamental), a predição de idade oferece uma experiência rápida e contínua. Isso reduz as taxas de desistência no momento da inscrição ou nos pontos de acesso, tornando-a uma escolha prática

² Como a Meta utiliza IA para entender melhor as idades das pessoas em nossas plataformas
<https://tech.fb.com/artificial-intelligence/2022/06/adult-classifier/>

para serviços de alto volume como as redes sociais.

- **Inclusão:** A predição de idade é uma opção mais inclusiva para os aproximadamente um bilhão de pessoas que globalmente não possuem documentos formais de identidade (por exemplo, passaportes, carteiras de identidade). Ela oferece um método alternativo para que acessem serviços adequados à idade.
- **Apoio à Conformidade Regulatória:** Reguladores como o ICO e Ofcom do Reino Unido reconhecem a predição de idade como um método de aferição de idade válido e "altamente eficaz" quando implementado de forma apropriada e proporcional ao risco. Ela permite que as plataformas apliquem salvaguardas e filtros de conteúdo adequados à idade para cumprir leis como a Lei de Segurança Online, que exige a proteção de menores no ambiente virtual.
- **Abordagem em Camadas:** A predição de idade é frequentemente usada como parte de uma estratégia de aferição de idade em camadas e "baseada em risco" (uma abordagem em "cascata"). Ela serve como uma primeira verificação, leve e sutil. Se a idade de um usuário for estimada como próxima a um limite (dentro de uma "zona de amortecimento"), o sistema pode então solicitar um método secundário e mais robusto, como consentimento parental ou verificação de documentos, garantindo um equilíbrio entre precisão e conveniência.

Retenção de Dados e Limitação de Finalidade

Os princípios da **finalidade** e **necessidade** são fundamentais para a verificação de idade e garantia de identidade. Embora todos os métodos de verificação de idade exijam algum nível de tratamento de dados pessoais, é crucial esclarecer que retemos dados da idade verificada unicamente para os propósitos expressos de verificação de idade e conformidade regulatória. Estes dados não serão usados para fins comerciais. O foco deve ser em assegurar que o tratamento permaneça proporcional ao risco e ao contexto, minimizado ao estritamente necessário, retido apenas por um período apropriado, e protegido em todos os momentos por medidas de segurança robustas.

As plataformas, entretanto, devem ser capazes de reter o mínimo necessário de dados relacionados à idade, como faixa etária e fonte de dados, durante todo o ciclo de vida da conta de um usuário. Esta retenção é essencial para evitar a coleta repetida de documentação sensível em cada acesso ou interação, especialmente quando os usuários permanecem logados em várias sessões ou usam a verificação de idade para múltiplos recursos, como acessar conteúdo, comunicar-se com outros usuários ou fazer compras. Ao reter informações de idade derivadas — em vez de documentos brutos de verificação —, as plataformas podem aplicar decisões de verificação de idade de forma consistente e eficiente em conformidade com mandatos legais, enquanto mantêm os princípios de privacidade e minimização de dados.

Embora concordemos em princípio com a exclusão de documentos brutos de verificação o mais rápido possível, na prática é importante retê-los por um período limitado — como 30 dias — para medir e melhorar a eficácia do sistema de verificação de idade. Por exemplo, se um usuário envia um documento de identidade falso sofisticado que passa na verificação inicial e é imediatamente excluído, mas é posteriormente sinalizado por outros sistemas como representando incorretamente sua idade, torna-se desafiador depurar por que o sistema de verificação de identidade falhou e melhorar sua capacidade de detectar tais falsificações. Reter documentos brutos por um período curto e de finalidade limitada permite a análise pós-verificação e a melhoria do sistema, garantindo que o processo de verificação de idade permaneça robusto e adaptável. Quaisquer documentos retidos devem ser altamente seguros e estritamente limitados à finalidade de fornecer e melhorar o sistema de verificação de idade, com salvaguardas robustas para garantir que sejam excluídos dentro de um prazo claramente definido.



Manter apenas o mínimo necessário de dados relacionados à idade, e reter documentos brutos apenas por um período curto e justificado, permite que os serviços melhorem continuamente seus mecanismos de verificação de idade, monitorem como as métricas mudam ao longo do tempo e ajustem seus sistemas para melhor proteger os adolescentes. Esta abordagem garante que as plataformas possam fornecer conteúdo e experiências adequadas à idade, ao mesmo tempo em que equilibram a necessidade de medidas de segurança robustas com o imperativo de proteger a privacidade do usuário.

Capacitando Famílias: Aprovação Parental, Vinculação de Contas e Controles Parentais

Aprovação Parental e Estabelecimento do Vínculo Pais-Filho no Nível da Loja de Aplicativos/Sistema Operacional

A aprovação parental para downloads de aplicativos (Artigo 12, § 2º) é um elemento central do arcabouço de aferição de idade do ECA Digital). Ao tornar obrigatória a aprovação dos pais ou responsáveis antes que menores possam baixar aplicativos, o Brasil reafirma o papel vital das famílias em orientar e gerenciar as experiências dos jovens online. Isso capacita os pais a fazerem escolhas informadas e reforça o propósito protetivo, colaborativo e dialógico do sistema de aferição de idade, assegurando que as famílias permaneçam ativamente envolvidas.

A obrigatoriedade da aprovação parental para downloads de aplicativos também apoia a conformidade com o Artigo 24 do ECA Digital, que exige que as contas de usuários menores de 16 anos sejam vinculadas a um pai ou responsável. Um processo único e confiável de aprovação parental garante que essa vinculação seja clara e consistente em todo o ecossistema.

Além dos requisitos legais para aprovação parental, o sistema de classificação indicativa do Brasil, Classind, também desempenha um papel importante em guiar as famílias sobre conteúdo apropriado para a idade. **No entanto, é importante reforçar que o Classind tem natureza indicativa, não obrigatória. Dito de outro modo, embora o Classind forneça recomendações valiosas sobre conteúdo apropriado para a idade, os pais mantêm a autoridade para decidir o que é adequado para seus filhos.** Isso garante que as famílias possam fazer escolhas que reflitam seus próprios valores. Assim como os pais podem permitir que um filho assista a um filme com uma classificação etária mais alta com base na maturidade de seu filho, a aprovação parental permanece o elemento fundamental para determinar o acesso a aplicativos, respeitando os diversos contextos da gestão familiar. Esse equilíbrio entre orientação regulatória, por um lado, e autonomia familiar, por outro, é central na abordagem trazida pelo ECA Digital, garantindo que os pais permaneçam os tomadores de decisão finais nas experiências digitais de seus filhos.

A Meta apoia fortemente a integração da aprovação parental com o sinal de verificação de idade da loja de aplicativos/sistema operacional. Esses dois elementos são pilares essenciais para criar um ambiente seguro para menores: o sinal de idade da loja de aplicativos fornece um método confiável e padronizado para as plataformas receberem informações de idade, e a aprovação parental garante que a decisão final caiba àqueles mais bem posicionados para apoiar seus filhos. A maneira mais eficaz de oferecer experiências online seguras e apropriadas para crianças e adolescentes é exigir que os guardiões do ecossistema — lojas de aplicativos e sistemas operacionais — verifiquem a idade e exijam a aprovação parental para que usuários menores de 16 anos baixem um aplicativo, garantindo que o usuário seja colocado em experiências apropriadas para sua idade.

Existem várias abordagens práticas para estabelecer a vinculação pais-filho exigida para a aprovação parental, cada uma com seu próprio conjunto de particularidades (Ver [Anexo C](#) para recursos visuais):

- **Vinculação remota com mínimas implicações:** Qualquer conta verificada como 18+ pode se tornar o "pai/responsável" vinculado com mínimas implicações para qualquer uma das pessoas, e essa vinculação pode ser

feita remotamente (sem que as duas pessoas estejam presentes na mesma sala). Esse método é direto e conveniente, mas seus requisitos mínimos podem permitir que pessoas que não são pais (como amigos maiores de 18 anos) atuem como o "pais/responsáveis", potencialmente enfraquecendo a garantia de um verdadeiro relacionamento pai-filho.

- **Vinculação no dispositivo, feita presencialmente, usando ferramentas do sistema operacional (OS):** A vinculação é realizada presencialmente no dispositivo, aproveitando ferramentas existentes como o Google Family Link ou o Apple Family Sharing (Compartilhamento Familiar da Apple). O pai/mãe confirma a data de nascimento da criança e gerencia as aprovações de download de aplicativos. Para certas idades, os pais podem impor controles ou restrições adicionais, que não podem ser desativados até que a criança ultrapasse a idade limite. Esta abordagem está em linha com as práticas atuais da indústria, com a configuração presencial adicionando uma fricção que ajuda a dissuadir a declaração falsa de idade. No entanto, ainda existe risco de que um “amigo” maior de 18 anos possa atuar como o aprovador, o que enfraquece principalmente o consentimento parental para downloads de aplicativos, em vez das proteções gerais de idade.
- **Verificação explícita da relação familiar:** Este método exige a verificação explícita da relação legal entre pai/mãe e filho(a), potencialmente utilizando bases de dados nacionais para confirmar criptograficamente os laços familiares. Embora isso ofereça a garantia mais forte de relações corretas, introduz desafios significativos: cobertura limitada onde as bases de dados estão incompletas, complexidade social em casos de divórcio ou famílias mistas, aumento da fricção para o usuário e obstáculos técnicos no emparelhamento de contas de usuário em diferentes sistemas. Esta abordagem ainda não é padrão na indústria e exigiria exploração adicional antes de ser implementada.

Garantindo que Pais e Responsáveis tenham mais de 18 anos

Um aspecto crucial dessas abordagens é garantir que o pai ou responsável seja, de fato, um adulto.

O método para verificar se o titular de uma conta tem 18 anos ou mais é, em última análise, determinado pelos provedores de sistema operacional. Diferentemente da maioria dos aplicativos individuais, as plataformas de sistema operacional e lojas de aplicativos estão em uma posição única para oferecer uma variedade de métodos de verificação robustos. Por exemplo, os provedores de sistema operacional frequentemente associam dispositivos a planos de telefonia de operadoras, e os contratos de telefone geralmente exigem que o proprietário tenha pelo menos 18 anos. As lojas de aplicativos também processam pagamentos com cartão de crédito, o que geralmente exige um titular de conta adulto. Cada vez mais, os provedores de sistemas operacionais estão adicionando suporte para credenciais digitais em carteiras de dispositivos; essas credenciais são mais propensas a serem detidas por adultos e muitas vezes incluem a capacidade de verificar se um usuário está acima ou abaixo de 18 anos. No Brasil, a integração com o sistema [Gov.br](https://gov.br) oferece um caminho adicional para a verificação de adultos.

É importante notar que essas soluções são adequadas para uma verificação única durante a configuração do dispositivo. No entanto, por si só, elas não são suficientes para abordar os desafios e riscos mais amplos que surgem quando a verificação deve ser repetida em muitos aplicativos. Questões como experiência do usuário, privacidade e segurança, e a necessidade de apoiar a autonomia progressiva dos adolescentes e faixas etárias granulares exigem uma abordagem mais abrangente. Por essa razão, é essencial combinar esses métodos técnicos com uma idade informada pelos pais como parte de uma solução geral de sistemas operacionais ou lojas de aplicativos.

Este processo de verificação de status 18+ é principalmente sobre restringir o acesso a experiências adultas. É distinto do desafio de fornecer experiências granulares e apropriadas para a idade de menores – um problema que muitos aplicativos devem resolver separadamente.

Finalmente, é importante reconhecer que nenhum método de verificação é perfeito, e sempre haverá algum esforço necessário para que os adultos verifiquem suas contas. No entanto, os reguladores devem incentivar fortemente a verificação robusta de adultos para garantir a integridade dos controles parentais e dos sistemas de aferição de idade.

Olhando para o futuro, é possível que, se bancos de dados nacionais sejam desenvolvidos para verificar criptograficamente a relação legal entre uma criança e seu pai ou responsável, o ecossistema possa se tornar ainda mais robusto e consistente.. Embora isso represente uma visão de longo prazo para o futuro, a Meta propõe um ponto de partida prático: alavancar estruturas de sistemas operacionais existentes e amplamente adotadas, como o Apple Family Sharing (Compartilhamento Familiar da Apple) e o Family Link do Google. Embora esses sistemas não verifiquem a relação legal, o atrito inerente – exigindo que um adulto se comprometa formalmente a compartilhar métodos de pagamento e gerenciar a conta da criança ou do adolescente – cria um forte vínculo familiar *de fato*. Essa abordagem é uma melhoria significativa em relação ao *status quo* e serve como uma base razoável e prática para avançar a aprovação parental e o vínculo familiar no ecossistema digital.

Abordando Preocupações com o Compartilhamento de Dispositivos

Ao discutir o vínculo parental e as proteções para jovens, frequentemente surgem preocupações sobre compartilhamento de dispositivos (por exemplo, um *tablet* que pode ser usado tanto pelos pais como pelos filhos). No entanto, o verdadeiro desafio não é o compartilhamento de *dispositivos*, mas o compartilhamento de *contas*. Os fabricantes de dispositivos devem oferecer suporte à troca entre contas / perfis de usuário em um único dispositivo, por exemplo, inserindo diferentes PINs/senhas ou reconhecendo diferentes impressões digitais/*Face IDs* na tela de bloqueio do dispositivo.

A título de exemplo, se um pai compartilha sua senha em um serviço de *streaming* como a Netflix com um filho menor, o filho obtém acesso a conteúdo e recursos destinados a adultos. A Netflix aborda isso permitindo a troca fácil entre múltiplos perfis de usuários ou contas, cada um dos quais pode ser protegido por PIN ou senha. Essa abordagem garante que as crianças usem seu próprio perfil apropriado para a idade, enquanto os pais mantêm o controle sobre o conteúdo adulto.

Esse conceito de troca de conta/perfil de usuário não é novo — computadores suportam múltiplas contas de usuário há décadas, e muitos telefones Android oferecem funcionalidade semelhante hoje. A Apple também oferece suporte a múltiplas contas para escolas e empresas, mas deve ser incentivada a estender esse suporte para as famílias em geral.

Quando os fabricantes de dispositivos incluem suporte avançado para a troca de conta/perfil de usuário, o compartilhamento de dispositivos se torna um benefício para famílias que podem reduzir o custo de acesso à internet, mantendo sua própria experiência privada, personalizada e apropriada para a idade. E os pais desempenham um papel crucial na configuração e gestão dessas contas ou perfis separados para cada membro da família. Por exemplo:

- Se um pai compartilha uma única conta/perfil com um adolescente em múltiplos dispositivos, as proteções de idade e os controles parentais podem ser contornados, minando a eficácia do sistema.
- Se um pai garante que cada usuário tenha sua própria conta ou perfil em um dispositivo compartilhado — e os

provedores de sistemas operacionais tornam isso um recurso de primeira classe, fácil de usar — então as proteções apropriadas para a idade permanecem intactas, mesmo em um único dispositivo.

Para apoiar o vínculo parental seguro e eficaz, plataformas e sistemas operacionais devem:

1. Incentivar ou exigir o uso de contas/perfis individuais para cada usuário, especialmente em dispositivos compartilhados.
2. Fornecer ferramentas para os pais gerenciarem e supervisionarem contas/perfis, incluindo proteção por PIN/senha e monitoramento de atividades.
3. Fornecer aos aplicativos um sinal de idade para o perfil atualmente ativo, permitindo que ofereçam experiências apropriadas para a idade.

Ao focar nas proteções em nível de conta e capacitar os pais para configurar e gerenciar perfis individuais, as plataformas podem abordar os riscos reais associados ao compartilhamento de contas — ao mesmo tempo em que tornam o compartilhamento de dispositivos seguro e prático para as famílias.

Projetando para a Segurança: Contas para Adolescentes e Ferramentas de Supervisão Parental para Proteger Adolescentes nas Plataformas da Meta

O ECA Digital já prevê múltiplas camadas de proteção que atuam em conjunto para garantir o melhor interesse da criança e do adolescente. Por exemplo, quando uma criança ou adolescente tenta acessar um aplicativo, ele já terá passado por pelo menos duas camadas protetivas, a de aferição de idade e a de autorização parental, além das salvaguardas implementadas pelo próprio aplicativo para impedir o acesso a conteúdo inadequado. Além disso, as ferramentas de supervisão parental devem, por padrão, adotar o mais alto nível de proteção (Artigo 17, §4º), ao mesmo tempo em que ainda permitem que os pais apliquem restrições adicionais conforme previsto no Artigo 18. Medidas excessivas ou sobrepostas poderiam ter efeitos contraproducentes: podem restringir indevidamente o acesso, impactar negativamente os direitos de crianças e adolescentes, interferir na experiência e nos direitos de outros usuários, ou dificultar o bom funcionamento dos serviços online e do ecossistema mais amplo da internet. É, portanto, essencial que quaisquer novas regras se baseiem, em vez de extrapolarem, o novo arcabouço estabelecido pelo ECA Digital.

Nos últimos anos, a Meta tem se concentrado em uma série de investimentos voltados à proteção dos adolescentes. Como afirma o Comentário Geral da Convenção das Nações Unidas sobre os Direitos da Criança (**UNCRC**) sobre os Direitos da Criança no Ambiente Digital, “[o] melhor interesse da criança é um conceito dinâmico que requer uma avaliação apropriada ao contexto específico³”. Na prática, exige que as organizações façam uma avaliação baseada no contexto específico de seus serviços e equilibrem o direito dos jovens à identidade; liberdade de associação; liberdade de expressão, incluindo a liberdade de buscar, receber e transmitir informações; o direito à educação e o direito de brincar e participar de uma ampla gama de atividades — para que não haja consequências indesejadas para o jovem. Na Meta, desenvolvemos um processo para nos ajudar a traduzir a política para a prática. Referimo-nos a isso internamente como Abordagem do Melhor Interesse da Criança da Meta⁴, que resume a abordagem de melhores interesses em seis considerações principais para as equipes de produto.

³ Convenção das Nações Unidas sobre os Direitos da Criança, “Comentário Geral n.º 25 (2021) sobre os direitos das crianças em relação ao ambiente digital”, <https://digitallibrary.un.org/record/3906061?ln=en&v=pdf>

⁴ Abordagem do Melhor Interesse da Criança da Meta: <https://www.ttclabs.net/news/metabest-interests-of-the-child-framework>

Aplicando este processo, desenvolvemos proteções robustas para jovens, a fim de proteger sua privacidade e segurança de uma forma apropriada para a idade. Colocamos centenas de milhões de adolescentes em Contas para Adolescentes no Instagram, Facebook e Messenger. As Contas para Adolescentes já foram lançadas globalmente no Instagram e estão em processo de expansão para Facebook e Messenger globalmente.⁵

O desenvolvimento dos recursos das Contas para Adolescentes foi orientado por uma pesquisa abrangente e consultas com mais de 600 partes interessadas, 300 adolescentes e 270 pais e responsáveis de mais de 35 países. Este trabalho confirmou que a adolescência é um período de transição em que os adolescentes estão aprendendo a se expressar, bem como a construir comunidades – seja online ou offline – desempenhando um papel importante em seu desenvolvimento. Adolescentes podem usar espaços online para se conectar e descobrir novidades, e queremos preservar esses ambientes para eles ao considerar novas experiências protegidas. Também sabemos que os adolescentes querem que suas experiências online sejam positivas. Recebemos os seguintes feedbacks dos adolescentes:

- Eles tendem a procurar suporte contínuo em aplicativos de mídia social, incluindo ferramentas para lidar com situações em que percebem que estão perdendo tempo, quando encontram conteúdo desagradável ou entram em contato com pessoas que os deixam desconfortáveis.
- Eles estão interessados em maneiras pelas quais os serviços digitais podem fornecer transparência e controles para ajudar a impulsionar experiências apropriadas para a idade.
- Eles reconhecem o valor de seus pais terem mais informações à disposição. Os adolescentes consideram as ferramentas de supervisão úteis, pois suas mudanças de comportamento podem ser usadas como evidência para mostrar aos pais ou responsáveis que estão prontos para assumir mais responsabilidades, escolhas e controle no decorrer do tempo.⁶

Com este pano de fundo, desenvolvemos os seguintes recursos para Contas de Adolescentes no Instagram:

- **Contas privadas:** Com contas privadas por padrão para adolescentes novos e existentes, os adolescentes precisam aceitar novos seguidores, e as pessoas que não os seguem não podem ver o seu conteúdo nem interagir com eles. Esta é a configuração por padrão para todas as contas de adolescentes novas e existentes (menores de 18 anos), sendo a única exceção as contas de adolescentes mais velhos (16-17 anos) que podem manter o seu *status* de privacidade da conta e não serão alteradas para privado se tiverem previamente convertido a sua conta para pública. Esta abordagem reflete a importância de garantir a autonomia e independência dos adolescentes mais velhos na tomada de decisões relacionadas com a privacidade, reconhecendo que são mais capazes de fazer escolhas informadas sobre a sua presença online.
- **Restrições de mensagens:** Os adolescentes são colocados nas configurações de mensagens mais restritas, para que só possam receber mensagens de pessoas que sigam ou com as quais já estejam ligados.
- **Restrições de conteúdo sensível:** Os adolescentes são automaticamente colocados numa configuração estrita do nosso “controle de conteúdo sensível”, que limita o tipo de conteúdo sensível (como conteúdo que mostra pessoas

⁵ <https://about.fb.com/news/2025/09/millions-teens-now-teen-accounts-plus-more-support-schools/> No Brasil, por exemplo, nossas equipes vêm organizando workshops de co-criação desde 2022 (dos quais participam pais e adolescentes) para coletar informações sobre ferramentas de controle e supervisão parental, verificação de idade, o que funciona e o que não funciona em termos de transparência, etc. Vários Ministérios e membros da ANPD juntaram-se a nós como observadores e participaram de mesas-redondas para discutir as descobertas de um jam de co-criação organizado em Brasília em abril de 2024.

⁶ Meta, “Como a pesquisa e a consulta informaram as contas adolescentes do Instagram: uma nova experiência protegida para adolescentes, orientada pelos pais”, Trust, Transparency & Control Labs, 17 de setembro de 2024., https://www.tlclabs.net/site/assets/files/12047/how_research_consultation_informed_instagram_teen_accounts.pdf

brigando ou que promova procedimentos estéticos) que os adolescentes veem em locais como Explorar e Reels. Continuamos a explorar novas formas de personalizar o conteúdo para adolescentes na nossa plataforma dando mais controle aos pais para customizar a experiência de conteúdo dos seus filhos adolescentes.

- Anunciamos recentemente que as Contas de Adolescentes do Instagram nos EUA, Reino Unido, Canadá e Austrália serão, por padrão, orientadas por uma configuração atualizada de 13+ e não poderão optar por sair sem permissão parental. Além disso, introduzimos uma configuração mais rigorosa para os pais que preferem uma experiência mais restritiva para os seus filhos adolescentes. Estas proteções garantem que as famílias permanecem ativamente envolvidas em decisões importantes sobre as experiências online dos seus filhos adolescentes. Milhares de pais de todo o mundo compartilharam o seu feedback conosco, ajudando a moldar estas alterações e a garantir que os nossos esforços reflitam suas expectativas e valores. À medida que continuamos a adaptar e a melhorar nossa abordagem, esperamos trabalhar em estreita colaboração com o Ministério da Justiça para esclarecer como estas novas configurações se alinham com as classificações etárias estabelecidas no Brasil e apoiam as famílias na tomada de decisões informadas.
- **Interações limitadas:** Os adolescentes só podem ser identificados ou mencionados por pessoas que eles sigam. Também ativamos automaticamente a versão mais restritiva da nossa funcionalidade anti-bullying, *Palavras Ocultas*, para que palavras e frases ofensivas sejam filtradas dos comentários e pedidos de DM dos adolescentes.
- **Lembretes de limite de tempo:** Os adolescentes recebem notificações para saírem da aplicação após 60 minutos de utilização por dia.
- **Modo de descanso ativado:** O modo de suspensão é ativado entre as 22h e as 7h, o que silencia as notificações durante a noite e envia respostas automáticas a DMs.

Em julho, anunciamos novos recursos de segurança para contas de adolescentes, a fim de protegê-los de contatos potencialmente inseguros e indesejados em mensagens diretas. Esses recursos fornecem aos adolescentes mais informações sobre as contas com as quais estão trocando mensagens (por exemplo, o mês e o ano em que a conta se cadastrou no Instagram ou se a conta é estrangeira), ajudando-os a identificar possíveis golpistas, além da capacidade de bloquear e denunciar mensagens diretas ao mesmo tempo, facilitando o processo de denúncia⁷.

Mais importante, as Contas de Adolescentes são projetadas em torno da autonomia progressiva: usuários menores de 16 anos não podem alterar suas configurações padrão sem autorização dos pais. Isso garante diferenciação apropriada para a idade com base nos níveis de maturidade e oferece às famílias oportunidades de supervisão aprimorada por meio da vinculação de contas. Os adolescentes permanecerão protegidos no nível mais alto pelos princípios de design de proteção da Meta. .

⁷ Meta, “Expandindo as proteções para contas de adolescentes e os recursos de segurança infantil”, Sala de imprensa, 23 de julho de 2025, <https://about.fb.com/news/2025/07/expanding-teen-account-protections-child-safety-features>

Conclusões

A abordagem pioneira do Brasil em relação à garantia de idade coloca provedores de lojas de aplicativo e de Sistema Operacional no centro de uma estrutura robusta para proteger menores online. Este sistema permite que adolescentes e crianças sejam colocados em experiências adequadas à idade em todos os aplicativos que usam. Fornecer e verificar, no nível do aplicativo ou do dispositivo, é a **solução mais eficiente, que preserva a privacidade e é sustentável**, eliminando a necessidade de jovens e suas famílias enviarem repetidamente informações pessoais confidenciais em vários aplicativos.

Reforçamos que essa abordagem não exime a Meta da responsabilidade de adotar e aprimorar seus próprios mecanismos para identificar a idade dos usuários, conforme detalhado ao longo deste documento. O ponto central é assegurar um modelo sustentável, capaz de acomodar a multiplicidade de atores envolvidos, promovendo a proteção efetiva de menores sem sobrecarregar usuários ou comprometer a privacidade.

Este modelo afirma que **a aprovação parental para downloads de aplicativos é o fator decisivo** na determinação do acesso de menores a serviços digitais, capacitando as famílias e, ao mesmo tempo, mantendo os padrões regulatórios. A Meta apoia totalmente a integração de sinais de aprovação parental com a verificação de idade das lojas de aplicativos e do sistemas operacionais, reconhecendo que estes dois pilares – garantia de idade centralizada e controle parental fortalecido – formam a base de ambientes digitais seguros.

Para garantir o sucesso da estrutura Digital do ECA, pedimos ao Ministério da Justiça que forneça orientação clara de que:

- **O sinal de idade das lojas de aplicativos e do sistemas operacionais deve servir como fonte primária e inicial de conhecimento de idade.**
- Para aplicativos que não são legalmente proibidos para menores, a coleta de informações pessoais adicionais deve ser **estritamente limitada**, aderindo aos princípios de minimização de dados e limitação de finalidade.

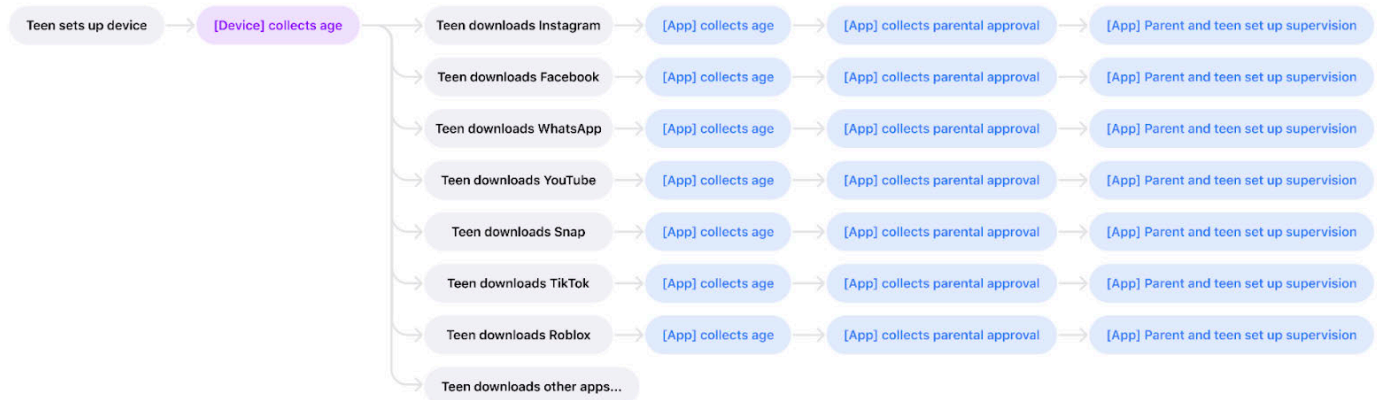
A Meta está totalmente comprometida com uma abordagem de aferição de idade que envolva todo o ecossistema. Estamos preparados para receber sinais de idade das lojas de aplicativo e sistemas operacionais e trabalharemos ativamente para compartilhar qualquer informação de idade mais confiável que descobrirmos com os sistemas operacionais para retroalimentar o esforço de proteção das diversas partes do ecossistema. Através desta visão colaborativa e da aplicação consistente do ECA Digital, o Brasil está preparado para estabelecer um novo padrão global para a segurança e privacidade online de crianças.

Anexo A: Abordagem aplicativo por aplicativo *versus* abordagem centrada nas lojas de aplicativos e sistemas operacionais

SITUAÇÃO ATUAL

A experiência atual, aplicativo por aplicativo, é:

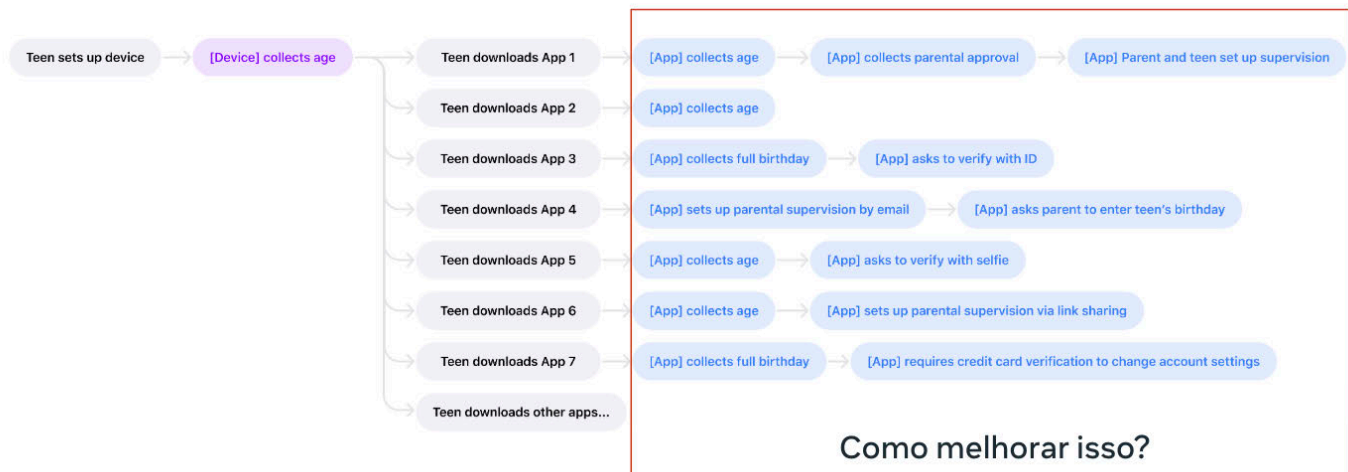
- ***duplicada***: adolescentes usam mais de 40 aplicativos por semana, em média
- ***inconsistente***: aplicativos aplicam suas próprias verificações e padrões de idade
- ***fricção alta***: várias etapas e partes envolvidas



SITUAÇÃO ATUAL

A experiência atual, aplicativo por aplicativo, é:

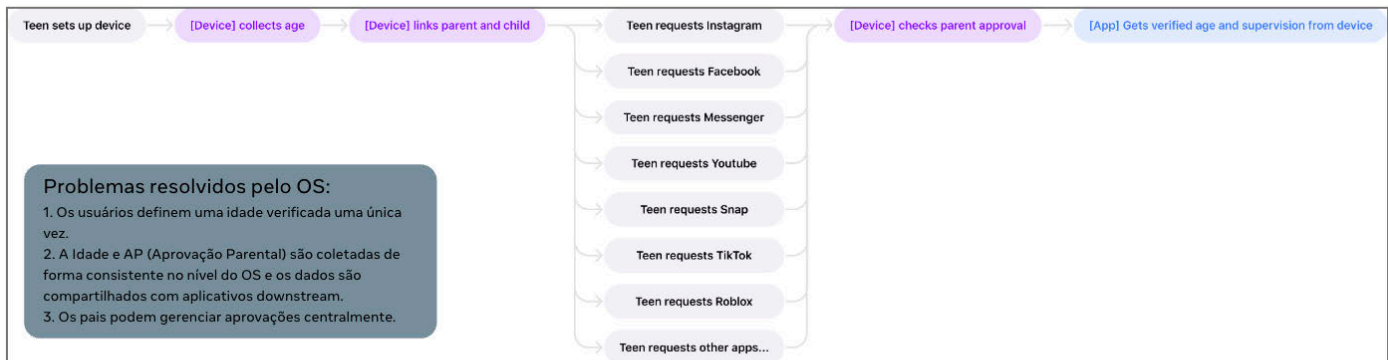
- **duplicada:** adolescentes usam mais de 40 aplicativos por semana, em média
- **inconsistente:** aplicativos aplicam suas próprias verificações e padrões de idade
- **fricção alta:** várias etapas e partes envolvidas



EM 2026

A solução das lojas de aplicativos e sistemas operacionais é:

- **unificada:** a conta do dispositivo já possui todas as informações relevantes
- **consistente** — os usuários entendem melhor quando há um padrão
- **menor atrito** — devido a etapas simplificadas



Anexo B : API de Verificação de Idade



Exemplo para adolescentes: configuração única de conta

Vamos analisar um exemplo de uma adolescente de 13 anos que está ganhando seu primeiro celular. Seu pai ou responsável senta-se com ela para configurá-lo juntamente com uma nova conta do Google ou da Apple.

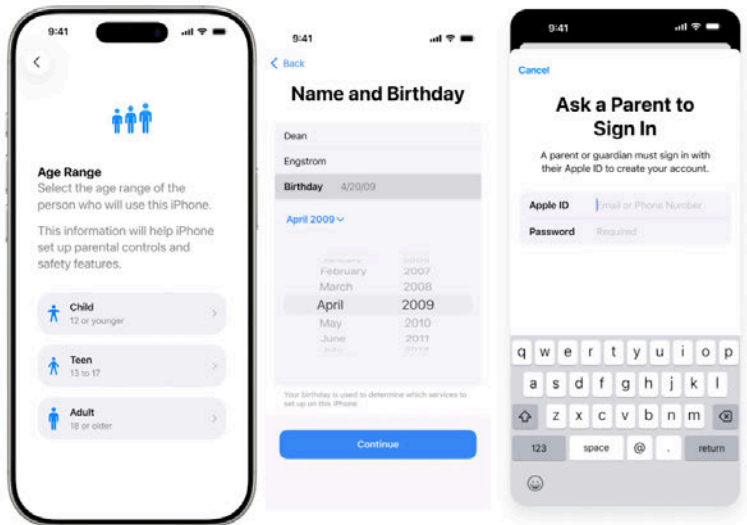
A adolescente preenche seu nome e data de nascimento. (O Google e a Apple já coletam a data de nascimento completa do usuário ao criar uma conta.)

Como ela tem menos de 18 anos, ela deve vincular sua conta a um responsável maior de 18 anos que confirmará se a data de nascimento está correta.

(O Google e a Apple exigem a vinculação dos pais para crianças de 12 anos ou menos atualmente. Isso mudará para 18 anos ou menos no Texas em janeiro e deverá ser o mesmo no Brasil.)

Pronto — a conta da adolescente está pronta para a API de Idade.

Observação: a criação de uma conta de adulto maior de 18 anos exigiria verificação



Exemplo para adolescentes: aprovação para download de aplicativo

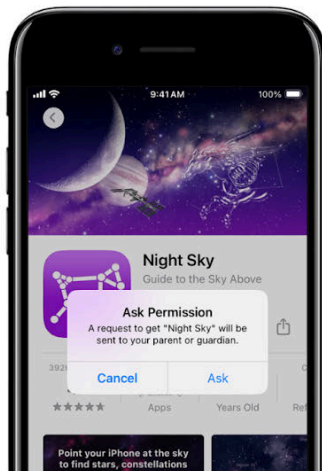
O Artigo 12 da ECA Digital exige aprovação dos pais para baixar aplicativos. O Google e a Apple também possuem recursos muito semelhantes que podem ser usados para isso.

Quando o adolescente encontra um aplicativo que deseja usar em uma loja de aplicativos, ele toca em um botão para solicitar o download.

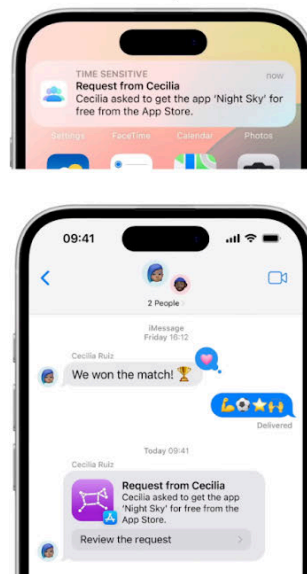
Isso envia automaticamente uma notificação para o responsável vinculado, que pode revisar a solicitação em seu dispositivo.

Os pais teriam a possibilidade de revogar posteriormente o acesso a aplicativos específicos.

Teen's phone:



Parent's phone:



Exemplo para adolescentes: API de idade

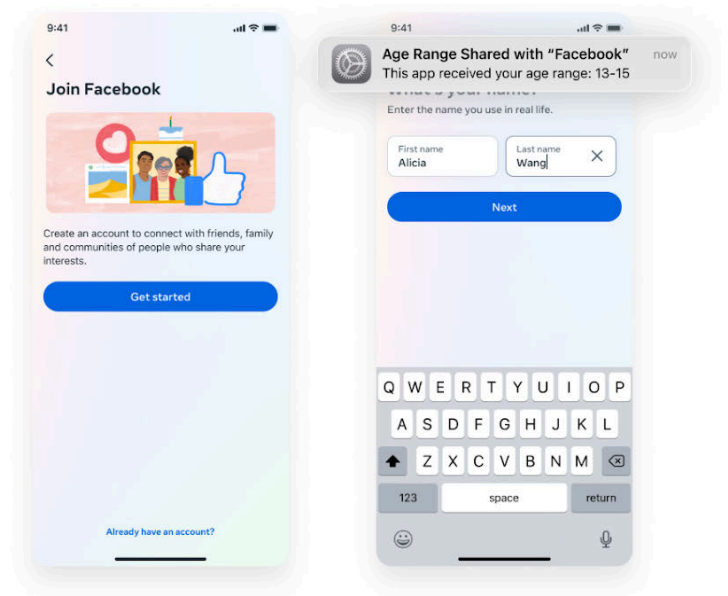
Agora o aplicativo está instalado e pronto para uso pela primeira vez.

O adolescente abre o aplicativo e acessa um recurso que precisa de verificação de idade, como o cadastro de uma nova conta.

O aplicativo pode então solicitar as faixas etárias relevantes e aplicar a verificação automaticamente.

Para cada aplicativo, a configuração de idade é mais fácil para o adolescente, e os pais podem confiar que a conta será configurada de forma apropriada para a idade, sem precisar intervir a cada vez.

Existem várias opções para lidar com a interação do usuário. Aqui, estou destacando a opção de compartilhar a faixa etária automaticamente e informar o usuário sobre o que o aplicativo aprendeu.

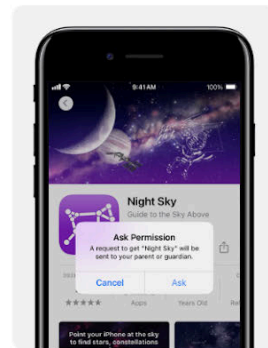
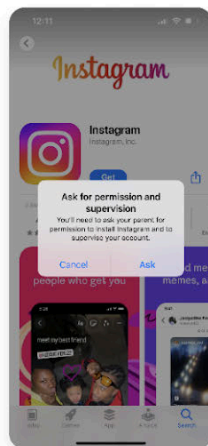


Anexo C: Exemplos de Vinculação Parental

Aprovação dos pais para download de apps

A possibilidade de os pais aprovarem o download de aplicativos individuais já existe em muitos sistemas operacionais atualmente.

Além de receber uma notificação quando um adolescente solicita permissão para baixar um aplicativo, os pais também poderão revogar a aprovação posteriormente por meio dos controles do Link Pais-Filhos.

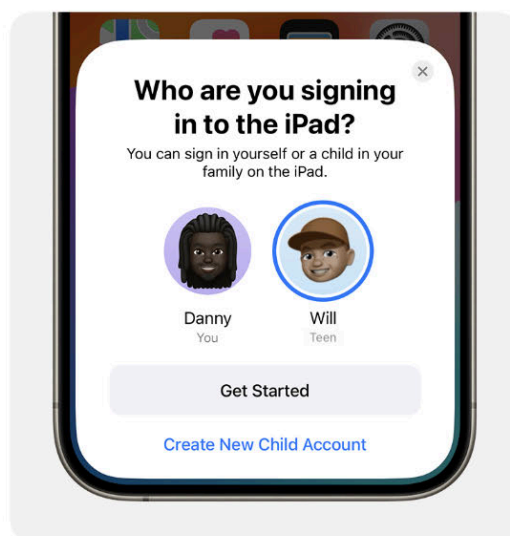


Troca de usuário

O suporte de primeira classe para alternância de contas/perfis por fabricantes de dispositivos permite o compartilhamento seguro de dispositivos entre famílias. As famílias se beneficiam ao reduzir o custo de acesso à internet, mantendo experiências privadas, personalizadas e adequadas à idade para cada membro. Os pais desempenham um papel fundamental ao configurar e gerenciar contas ou perfis separados para cada membro da família.

- Conta compartilhada única: Se um pai compartilha uma conta com um adolescente em vários dispositivos, as proteções de idade e os controles parentais podem ser burlados, comprometendo os recursos de segurança.
- Contas/perfis individuais: Quando cada usuário tem sua própria conta/perfil — e os sistemas operacionais tornam isso fácil de usar — as proteções adequadas à idade permanecem intactas, mesmo em dispositivos compartilhados.

Ao focar em proteções a nível de conta e empoderar os pais para gerenciar perfis individuais, as plataformas podem enfrentar os riscos do compartilhamento de contas — tornando o compartilhamento de dispositivos seguro e prático para famílias.



Tomada de Subsídios ANPD: Conceitos descritos na ECA Digital (Estatuto da Criança e do Adolescente)

1. A **Tools for Humanity (TFH)** parabeniza a Agência Nacional de Proteção de Dados (ANPD) pela iniciativa de promover a Tomada de Subsídios sobre os conceitos descritos no ECA Digital, pois entendemos que trata-se de um tema de grande relevância para a proteção de crianças e adolescentes e para o fortalecimento da confiança e segurança no ambiente online.

2. A **TFH** opera uma infraestrutura de credenciais digitais projetada para permitir a verificação de atributos pessoais de maneira segura, interoperável e autônoma, compatível com vários sistemas de autenticação digital — desde soluções públicas, como o Gov.br, até credenciais privadas. Tecnicamente, a infraestrutura conta com criptografia avançada, assinaturas digitais, autenticação local e técnicas de privacidade. Esses mecanismos permitem que o compartilhamento de dados seja restrito ao mínimo necessário: simples confirmação de que o usuário atende a um critério (por exemplo, ter mais de 18 anos), sem expor dados confidenciais, como data de nascimento, número de previdência social ou quaisquer outros metadados. O controle total permanece com o usuário, cujas credenciais são armazenadas exclusivamente em seus próprios dispositivos ou carteiras digitais, eliminando a dependência de bancos de dados centralizados e reduzindo o risco de vazamento de dados.

3. O desenvolvimento desta tecnologia é regido por uma abordagem ética e técnica rigorosa, fundamentada em quatro pilares essenciais:

- a) **Minimização de Dados:** a coleta e o tratamento de dados são orientados pela minimização, reduzindo drasticamente a circulação desnecessária de dados pessoais na rede;
- b) **Anonimato:** o sistema impede que diferentes interações do mesmo usuário sejam correlacionadas. Isso viabiliza comprovações seletivas — como confirmar a idade sem expor o documento de identidade — e impede a criação de perfis de usuário, protegendo a privacidade;
- c) **Autocustódia:** o modelo assegura que os usuários detenham o controle integral sobre suas credenciais, podendo gerenciar, revogar ou atualizar seus atributos a qualquer momento, sem a necessidade de recorrer a intermediários;
- d) **Alta Aferição:** a arquitetura oferece grau de aferição elevada de segurança e resistência a fraudes. Assinaturas digitais são usadas para permitir que terceiros validem os atributos apresentados, usando padrões internacionais, sem depender de uma autoridade central ou de um único banco de dados.

4. Entendemos que termos como “mecanismos de verificação de idade” e “mecanismos de aferição de idade” mencionados ao longo do texto legal, especialmente no Capítulo IV, constituem um conceito aberto, que pode ser detalhado posteriormente, para garantir a adoção de soluções robustas e que preservem a privacidade. Para esse fim, entendemos que a ANPD deve priorizar o estabelecimento de diretrizes técnicas para a adoção de mecanismos de verificação de idade por fornecedores de produtos ou serviços de tecnologia da informação, tais como: preferir verificações que operam com sinais binários (“sim/não”), limitar o uso de dados sensíveis, evitar que um método se torne obrigatório por padrão e favorecer arquiteturas que reduzam o risco de rastreamento ou

reidentificação. A adoção de tais critérios pode preservar a privacidade e aumentar a confiabilidade das verificações, evitando que um único sistema seja imposto a todos os contextos.

5. Também acreditamos ser importante esclarecer o conceito do que seria entendido como “medidas adequadas ou proporcionais” a serem adotadas para cada atividade acessível a crianças e adolescentes (artigos 3º e 12º), uma vez que, ao fazê-lo, a ECA Digital não define como a proporcionalidade deve ser avaliada caso a caso. Assim, acreditamos que a ANPD deve estabelecer parâmetros objetivos a serem considerados para essa avaliação de proporcionalidade, tais como: sensibilidade do serviço, possibilidade de interação entre usuários, risco de exposição a conteúdo impróprio, volume de dados processados e potencial de danos resultantes de falhas sistêmicas. Acreditamos que esses seriam alguns dos fatores que permitiriam um marco regulatório flexível, possibilitando que diferentes agentes em diferentes contextos — redes sociais, jogos, plataformas educacionais, comércio eletrônico — adotassem métodos diferentes, sem impor um modelo único para todo o ecossistema.

6. Além disso, acreditamos que é extremamente importante diferenciar claramente entre “verificação/afirmação de idade” e “verificação de identidade”, uma vez que o texto legal não faz explicitamente essa distinção, embora seja fundamental para a proteção de dados, uma vez que a comprovação de idade não requer a identificação completa do usuário, e a ANPD pode reforçar esse princípio, evitando interpretações que resultem em coleta e processamento excessivos ou desproporcionais de dados. Esse esclarecimento favorece o uso de credenciais anônimas, por exemplo, que são compatíveis com a LGPD.

7. As salvaguardas exigidas pela LGPD e pela ECA Digital podem ser incorporadas diretamente ao projeto técnico do sistema. A coleta, idealmente, poderia ser limitada ao necessário para formar a credencial, e o compartilhamento poderia ser restrito ao resultado da verificação, não aos dados brutos. As principais ameaças à privacidade nos processos de verificação de idade decorrem da possibilidade de reidentificar o usuário ou criar repositórios centralizados que correlacionam múltiplas interações. Uma arquitetura que impeça fluxos desnecessários de informações reduz substancialmente esses riscos.

8. Além disso, enfatizamos que a regulamentação deve definir parâmetros transparentes para os mecanismos de certificação (artigo 11). Esses mecanismos devem se concentrar nos resultados — robustez, preservação da privacidade, mitigação de riscos — e não prescrever tecnologias específicas. Processos de certificação flexíveis permitirão que as credenciais emitidas por autoridades públicas e soluções privadas interoperem e evoluam com o estado da arte, mantendo as regulamentações estáveis ao longo do tempo. A adoção de credenciais anônimas no Brasil pode avançar com uma combinação de recursos públicos e privados. O país já possui uma infraestrutura nacional de identificação que pode servir como ponto de partida para a autenticação dos cidadãos, sem a necessidade de rastreamento ou compartilhamento excessivo de dados. A emissão de credenciais verificáveis que expressam apenas atributos específicos — como comprovação de idade — permitiria que diferentes carteiras digitais e soluções privadas incorporassem essas informações de maneira interoperável. Nesse ambiente, sistemas como o desenvolvido pela **TFH** agregam valor ao permitir verificações seletivas de maneira segura e compatível com os padrões internacionais.

8. Por fim, destacamos a importância de que as definições e requisitos estabelecidos nos regulamentos preservem a exigência de interoperabilidade (artigo 12, §3º), permitindo que uma verificação de idade obtida em um sistema seja aceita em diferentes plataformas, públicas ou privadas, sem múltiplos registros ou etapas redundantes. Isso reduz as barreiras de acesso, amplia a inclusão digital e, especialmente, protege os usuários menos familiarizados com a tecnologia.

9. Neste contexto, é essencial que os regulamentos sejam baseados em princípios e resultados, e não sejam exaustivos ou prescritivos em termos tecnológicos, para que entendamos

que, em vez de detalhar tecnologias específicas, a ANPD será mais eficaz se mantiver seu foco em princípios, salvaguardas e resultados esperados. Isso garantirá que o Brasil adote soluções modernas e seguras, como credenciais verificáveis, modelos descentralizados e técnicas avançadas de preservação da privacidade, ao mesmo tempo em que assegura a proteção integral de crianças e adolescentes no ambiente digital.