

LUCIANO ALVES ROSSATO
PAULO LÉPORE
RAFAEL MOTT FARAH
IGOR MORAES ROCHA

ECA DIGITAL
COMENTÁRIOS AO ESTATUTO
DIGITAL DA CRIANÇA E DO
ADOLESCENTE
LEI Nº 15.211/2025

2026

CAPÍTULO III

DA VEDAÇÃO AO ACESSO DE CRIANÇAS E DE ADOLESCENTES A CONTEÚDOS E SERVIÇOS IMPRÓPRIOS, INADEQUADOS OU PROIBIDOS POR LEI

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.

§ 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.

§ 3º Os provedores de aplicações de internet que disponibilizarem conteúdo pornográfico deverão impedir a criação de contas ou de perfis por crianças e adolescentes no âmbito de seus serviços.

CAPÍTULO IV

DOS MECANISMOS DE AFERIÇÃO DE IDADE

Art. 10. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar mecanismos para proporcionar experiências adequadas à idade, nos termos deste Capítulo, respeitadas a autonomia progressiva e a diversidade de contextos socioeconômicos brasileiros.

Art. 11. O poder público poderá atuar como regulador, certificador ou promotor de soluções técnicas de verificação de idade, observados os limites da legalidade, da proteção à privacidade e dos direitos fundamentais previstos em lei.

Parágrafo único. A atuação do poder público prevista no *caput* deste artigo deverá assegurar a participação social, por meio de consulta pública e de outros mecanismos de participação social, de forma a garantir transparência no processo regulatório.

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

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.

§ 2º A autorização para *download* de aplicativos por crianças e adolescentes dependerá de consentimento livre e informado dos pais ou responsáveis legais, prestado nos termos da legislação vigente, respeitada a autonomia progressiva, vedada a presunção de autorização na hipótese de ausência de manifestação dos pais ou responsáveis legais.

§ 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.

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.

Parágrafo único. Independentemente das medidas adotadas pelos sistemas operacionais e pelas lojas de aplicações, os fornecedores de que trata o *caput* deste artigo deverão implementar mecanismos próprios para impedir o acesso indevido de crianças e de adolescentes a conteúdos inadequados para sua faixa etária, nos termos do § 1º do art. 5º desta Lei.

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.

1. CONTEÚDOS E SERVIÇOS IMPRÓPRIOS, INADEQUADOS OU PROIBIDOS POR LEI

Na linha do que foi exposto anteriormente, o ECA Digital deixa nítida a inclusão de produtos ou serviços que não são especificamente direcionados às crianças e adolescentes, mas que, mesmo assim, ainda sejam de acesso provável por esse público.

Contudo, o art. 9º vai além dessa questão. O legislador determina que os produtos e serviços impróprios, inadequados ou proibidos para menores de 18 anos, possuam mecanismos efetivos que impeçam o acesso por esse público. Isto é, ainda que não sejam direcionados às crianças e adolescentes, os fornecedores possuem o dever de implementar medidas eficazes para impossibilitar o acesso ao conteúdo pelos indivíduos que não são seu alvo em razão da idade.

Uma interessante reflexão positivada apresenta-se no par. 1º do respectivo artigo, em que se veda o uso da autodeclaração para fins de conferência de idade para acesso do conteúdo.

A autodeclaração é um dos mecanismos mais comuns e, ao mesmo tempo, mais debatidos para a verificação de idade no ambiente digital. Ela funciona por meio da simples solicitação de que o usuário declare a sua data de nascimento ou afirme, por meio de uma caixa de seleção, que possui a idade mínima para acessar um determinado conteúdo. Seu principal objetivo é impedir que menores de idade tenham acesso a materiais restritos, como conteúdo adulto, jogos violentos ou redes sociais não adequadas à sua faixa etária.

Em geral, o processo é bem direto. O usuário pode ser solicitado a digitar a sua data de nascimento em um formulário, e o sistema então calcula a idade para liberar ou negar o acesso. Outro método comum é a simples caixa de seleção com uma frase como “Eu declaro que tenho 18 anos ou mais”. Apesar de sua facilidade de implementação, a eficácia da autodeclaração é amplamente questionada. A barreira é facilmente superada, pois basta que um menor de idade forneça informações falsas para conseguir o acesso. Não há uma verificação real de identidade, e a responsabilidade de ser honesto recai inteiramente sobre o usuário.

Em um contexto amplo, a principal vantagem da autodeclaração é sua simplicidade. A implementação é rápida e de baixo custo, o que a torna uma escolha popular para muitos serviços online. Além disso, ela evita a

coleta de dados sensíveis, como documentos de identidade, que poderiam levantar preocupações de privacidade.

No entanto, as desvantagens são significativas e superam os benefícios em contextos de alta vulnerabilidade, como a proteção de crianças, pois caracterizam-se pela sua baixa confiabilidade e facilidade em ser burlada.

A autodeclaração pode ser vista como uma primeira camada de proteção. Ela cumpre o papel de informar o usuário sobre a restrição de idade e serve como um aviso formal sobre o tipo de conteúdo que está sendo acessado.

Para uma proteção mais robusta e legalmente defensável, a autodeclaração geralmente precisa ser combinada com outros mecanismos, como a verificação por meio de documentos, a validação por meio de dados de cartão de crédito (que geralmente exigem maior de 18 anos) ou até mesmo o uso de inteligência artificial para análise de comportamento.

Em resumo, a autodeclaração é um mecanismo de verificação de idade simples e barato, mas a sua baixa eficácia limita seu uso como única medida de proteção. Ela serve como um ponto de partida, mas para uma proteção real, deve ser complementada por métodos de verificação mais rigorosos¹. Justamente por esse motivo, o ECA Digital veda expressamente a autodeclaração como mecanismo para verificação de idade.

A redação dada pela Lei 15.211/25 ao artigo 9º é mais uma das mudanças em relação ao PL 2.628/22. Isso porque o legislador, bem como a sociedade como um todo, passou a entender que o espectro de conteúdo que o jovem deve ser protegido é bem mais amplo do que somente o conteúdo pornográfico em seu sentido estrito. Essa reformulação no texto aprovado acabou por se apresentar de maneira um pouco redundante por conta da explosão midiática do assunto.

É por esse motivo que alguns dispositivos se apresentam de maneira repetitiva ou mesmo óbvia, como é o caso do par. 3º do artigo 9: “os provedores de aplicações de internet que disponibilizarem conteúdo

1. Sobre a insuficiência dos mecanismos de autodeclaração, recomendamos a leitura de LIVINGSTONE, Sonia et al. **Children's Rights and Online Age Assurance Systems: the way forward**. The International Journal of Children's Rights, vol. 32, 2024, pp. 721-747. Disponível em http://eprints.lse.ac.uk/122731/5/chil-article-p721_009.pdf. Último acesso em 05 de outubro de 2025; e PASQUALE, Lilliane et al. **Digital Age of Consent and Age Verification: Can They Protect Children?** IEEE Software, doi: 10.1109/MS.2020.3044872, disponível em <https://arrow.tudublin.ie/aaschmedart/99/>. Último acesso em 05 de outubro de 2025.

pornográfico deverão impedir a criação de contas ou de perfis por crianças e adolescentes no âmbito de seus serviços”. Conforme uma interpretação mais atenta ao *caput*, nos parece que a criação de uma conta ou perfil em um site vedado a menores de 18 anos já é proibida por si só, uma vez que o seu acesso por si só já é proibido. Em que pese a redação aparentar uma obviedade, essa é uma discussão que se demonstra desnecessária.

2. MECANISMOS DE AFERIÇÃO DE IDADE

Em decorrência da fragilidade do sistema de verificação de idade da maioria dos produtos ou serviços digitais, o ECA Digital ressalta a importância dessa temática. Assim, o Capítulo IV da respectiva lei discorre através de 5 artigos (arts. 10 a 15) sobre os mecanismos de verificação de idade. Como outros pontos da lei, esse capítulo também surge como fruto das recentes discussões sobre o assunto, sendo, portanto, uma inovação quando comparado com o PL nº 2.628/2022.

Apesar da inserção do artigo 10 no Capítulo IV, ele pouco dispõe propriamente sobre mecanismos de verificação de idade, refletindo muito mais o conteúdo relativo ao Capítulo II – dos produtos e serviços de tecnologia da informação.

Além disso, cabe registrar que a ANPD publicou o Radar Tecnológico nº 5, intitulado “Mecanismos de Aferição de Idade”, que reúne estudos técnicos e discussões sobre técnicas de verificação etária em ambientes digitais, suas limitações práticas e implicações para privacidade e proteção de dados de crianças e adolescentes.

De todo modo, o primeiro ponto que surge como uma questão é logo no art. 10, que dispõe que devem ser respeitadas a “autonomia progressiva e a diversidade de contextos socioeconômicos brasileiros” para fins de adoção de mecanismos que proporcionem experiências adequadas à idade. Essa exigência de “diversidade de contextos socioeconômicos” encontra ecos nas recomendações da ANPD, que alerta para o risco de que métodos de verificação de idade sofisticados (como biometria facial ou validação documental) acabem excluindo usuários em zonas remotas ou com dispositivos obsoletos, como debatido no Radar Tecnológico nº 5.

Relativamente à autonomia progressiva, a interpretação não gera muitas questões, pois remete à ideia do desenvolvimento contínuo da criança

e do adolescente. Todavia, o ponto de maior questionamento surge quanto à “diversidade de contexto socioeconômicos brasileiros”.

Nota-se, portanto, que o artigo 10 da lei aborda um ponto crucial e, ao mesmo tempo, bastante complexo: como desenvolver produtos e serviços digitais que respeitem a diversidade de contextos socioeconômicos do Brasil, garantindo uma experiência adequada para todos? Essa exigência vai muito além de apenas criar um produto e torna o desafio de inclusão digital ainda mais profundo.

O Brasil é um país de enormes desigualdades. Milhões de crianças e adolescentes vivem em áreas com acesso precário à internet, com conexões lentas ou com dispositivos mais antigos, como smartphones básicos². Diante disso, a lei impõe aos fornecedores o dever de ir além da simples disponibilidade, exigindo que a experiência digital seja funcional e segura para todos.

Em suma, a legislação reconhece que a inclusão digital não é apenas sobre ter acesso à internet, mas sim sobre garantir que a experiência digital seja justa, equitativa e segura para todos.

Já o art. 11 passa a retratar de maneira mais precisa sobre os mecanismos de aferição da idade, funcionando como uma abertura para a intervenção do poder público na regulação desse tema. O mais interessante, contudo, apresenta-se no parágrafo único, que dispõe que a atuação do poder público deve assegurar a participação social, por meio de consulta pública ou outros mecanismos similares, garantindo a transparência nesse processo.

Sob outra perspectiva, cumpre ressaltar a inclusão de obrigações a figuras imprescindíveis para que a lei exerça efeito reais, os “provedores de **lojas** de aplicações de internet e de **sistemas operacionais** de terminais”³.

2. Esse cenário é demonstrado em recente pesquisa realizado pelo CETIC.br, a TIC Domicílios (2024). Disponível em <https://cetic.br/pt/tics/domicilios/2024/domicilios/>. Último acesso em 07.10.2025.

3. 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

Trata-se de sujeito diverso do “fornecedor”, amplamente mencionado em outros dispositivos do ECA Digital.

A norma direciona a responsabilidade para os grandes *players* do mercado, buscando garantir a proteção de crianças e adolescentes desde o ponto de entrada no mundo digital.

Primeiramente no inciso I, a lei exige que esses provedores tomem medidas proporcionais, auditáveis e tecnicamente seguras para aferir a idade ou a faixa etária dos usuários. Essa determinação caminha em direção a uma verificação de idade mais robusta, que vai além da simples autodeclaração. A ideia é que essas empresas implementem mecanismos eficazes, transparentes e que possam ser fiscalizados, seguindo os princípios de proteção de dados previstos na Lei Geral de Proteção de Dados (LGPD).

Em seguida, o inciso II estabelece que os provedores devem permitir que pais e responsáveis configurem mecanismos de supervisão parental. Embora a lei não exima a responsabilidade dos pais no acompanhamento dos filhos, ela reconhece que esse dever só pode ser exercido de forma efetiva se as ferramentas para tal forem disponibilizadas pelas plataformas. Sem essas funcionalidades, a supervisão se torna um fardo oneroso e, em muitos casos, inviável. Portanto, a lei cria uma corresponsabilidade, onde o dever dos pais é complementado pela obrigação dos provedores em fornecer os recursos necessários para o controle parental.

Por fim, o artigo aborda um ponto essencial para a interoperabilidade entre as diferentes plataformas. Os provedores de lojas de aplicativos devem possibilitar, por meio de uma API segura e pautada pela proteção da privacidade, o fornecimento de um “sinal de idade” para outros provedores. A API (Interface de Programação de Aplicação) funciona como um conector que permite que um sistema, como uma loja de aplicativos, comunique a idade de um usuário de forma segura a um aplicativo externo. Esse mecanismo é vital para garantir que, uma vez que a idade do usuário seja verificada em uma plataforma (por exemplo, na loja de aplicativos), essa informação possa ser utilizada por outros serviços, como um jogo ou

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.

uma rede social, sem a necessidade de uma nova verificação. Tudo isso deve ser feito com o foco na privacidade do menor.

Ademais, nos termos da redação do § 1º, é vedado o compartilhamento contínuo, automatizado e irrestrito de dados pessoais de crianças e adolescentes. Essa vedação tem como propósito a aplicação do princípio da minimização de dados.

O princípio da minimização de dados é um conceito central e fundamental na área de proteção de dados pessoais, atuando como uma bússola que guia a coleta e o tratamento de informações. Em sua essência, ele determina que uma organização deve coletar, processar e armazenar apenas os dados pessoais que são estritamente necessários, adequados e relevantes para atingir uma finalidade específica e legítima. Em outras palavras, a regra é: se você não precisa, não colete.

A aplicação desse princípio começa já no planejamento de qualquer operação que envolva dados. Um bom exemplo é a criação de um formulário de cadastro. Em vez de solicitar informações como estado civil, renda ou afiliação política para um serviço que não as exige, a minimização de dados impõe a coleta apenas do nome, e-mail e, talvez, um número de telefone: ou seja, o mínimo para cumprir a promessa do serviço. Esse pensamento se estende a todas as fases do ciclo de vida dos dados, desde a coleta até o armazenamento e o descarte, garantindo que o excesso seja sempre evitado.

A importância da minimização de dados transcende a mera conformidade legal. Ela representa uma abordagem proativa para a gestão de riscos. Quanto menos dados uma empresa detém, menor é o impacto de um possível incidente de segurança. Um ataque cibernético ou um vazamento de dados que afete uma base de dados minimizada causa danos significativamente menores do que um que atinja um vasto acervo de informações sensíveis e desnecessárias. Portanto, a minimização não é apenas uma obrigação, mas uma estratégia inteligente de segurança.

Além disso, esse princípio fortalece a confiança dos usuários. Ao perceber que uma empresa valoriza sua privacidade e não coleta informações além do necessário, o usuário se sente mais seguro e confiante para interagir com o serviço. Essa transparência e responsabilidade criam uma relação de longo prazo, baseada em respeito mútuo, o que é um ativo valioso na economia digital.

Em nosso cenário brasileiro, a Lei Geral de Proteção de Dados (LGPD) elevou a minimização de dados de uma boa prática a um requisito legal. O Artigo 6º, inciso III, da lei, estabelece explicitamente o “princípio da minimização”, definindo-o como a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação à finalidade do tratamento de dados”. Isso significa que as empresas não só são encorajadas, mas são legalmente obrigadas a adotar essa postura. O não cumprimento pode resultar em sanções e multas, reforçando a seriedade do tema.

Em suma, a minimização de dados é a materialização da ideia de que menos é mais no universo da privacidade. É um princípio que combina ética, segurança e estratégia de negócios, orientando as organizações a serem mais responsáveis, transparentes e, em última análise, mais seguras em sua relação com os dados pessoais.

É justamente para evitar que uma verificação de idade se transforme em coleta indiscriminada de dados, que o Radar Tecnológico nº 5 da ANPD enfatiza a necessidade de arquiteturas que permitam verificação sem transferência massiva de dados – por exemplo, usando criptografia, sinais agregados ou provas de conhecimento zero (*zero-knowledge proofs*).

Ainda nessa linha sobre os deveres dos provedores, o § 2º do art. 12, dispõe que a autorização para download de aplicativos por crianças e adolescentes dependerá de consentimento livre e informado dos pais ou responsáveis. Contudo, tal autorização não poderá ocorrer de maneira presumida em substituição da autorização expressa.

Em que pese a intenção máxima do legislador ao dispor sobre a autorização informada pelos pais ou responsáveis, as formas como isso podem ocorrer geram dúvidas e reflexões sobre quais são as técnicas suficientes para o cumprimento da norma.

Uma simples vinculação da conta dos sujeitos responsáveis com a conta da criança ou adolescente seria suficiente para se entender como autorizado o download? Dentro dessa hipótese ainda, haverá a necessidade dos responsáveis em criar uma conta no mesmo local? Ou será que seriam sempre necessárias reafirmações, seja por mecanismos de senha, identificação ou afins, para que se autorize o download?

De todo modo, seria inviável que o legislador antecipasse todas as formas de averiguação de consentimento. Sendo assim, resta nítida que é uma norma que dependerá de futuras complementações, a fim de que se

estabeleça de maneira objetiva como essa disposição ocorrerá na prática. Os requisitos mínimos de transparência, segurança e interoperabilidade devem ser, contudo, reguladas por ato do Poder Executivo.

O art. 13, por sua vez, reforça a ideia de que a coleta de dados para verificação de idade deve ser estritamente limitada a essa finalidade, proibindo qualquer tratamento posterior que extrapole esse objetivo. Essa disposição concretiza, na prática, os princípios da necessidade e da finalidade previstos na LGPD, ao mesmo tempo em que impede o uso indevido dessas informações: por exemplo, para fins de marketing, perfilamento ou qualquer outra atividade que envolva interesses comerciais. O dispositivo, portanto, busca resguardar a confiança dos usuários e garantir que o processo de aferição de idade não se torne uma nova via de exploração de dados de crianças e adolescentes.

Na sequência, o art. 14 amplia o dever de diligência dos fornecedores de produtos e serviços digitais voltados ao público infantojuvenil, exigindo a adoção de medidas técnicas e organizacionais capazes de assegurar a correta recepção e gestão das informações de idade.

Mesmo quando sistemas operacionais ou lojas de aplicativos já implementam mecanismos de controle, a norma impõe aos próprios fornecedores a responsabilidade de criar barreiras internas contra o acesso indevido a conteúdos inadequados.

Trata-se de um modelo de corresponsabilidade reforçada, que culmina no art. 15 ao dispor que o cumprimento dessas obrigações por um agente não exime os demais da cadeia digital – desenvolvedores, plataformas, distribuidores ou provedores de serviço – de seus deveres legais. Em outras palavras, a proteção integral de crianças e adolescentes no ambiente digital é uma tarefa coletiva e solidária, que requer a cooperação de todos os envolvidos na oferta, mediação e operação dos serviços tecnológicos.

CAPÍTULO V

DA SUPERVISÃO PARENTAL

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:

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:

I – disponibilizar configurações e ferramentas acessíveis e fáceis de usar que apoiem a supervisão parental, considerados a tecnologia disponível e a natureza e o propósito do produto ou serviço;

II – fornecer, em local de fácil acesso, informações aos pais ou responsáveis legais sobre as ferramentas existentes para o exercício da supervisão parental;

III – exibir aviso claro e visível quando as ferramentas de supervisão parental estiverem em vigor e sobre quais configurações ou controles foram aplicados; e

IV – oferecer funcionalidades que permitam limitar e monitorar o tempo de uso do produto ou serviço.

§ 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.

§ 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.

§ 3º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles poderão submeter à apreciação da autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital mecanismos de supervisão parental, observado que isso não será pré-requisito para a utilização desses mecanismos ou para a disponibilização de produtos ou serviços ao público, nos termos de regulamento.

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

I – restrição à comunicação com crianças e adolescentes por usuários não autorizados;

II – limitação de recursos para aumentar, sustentar ou estender artificialmente o uso do produto ou serviço pela criança ou pelo adolescente, como reprodução automática de mídia, recompensas pelo tempo de uso, notificações e outros recursos que possam resultar em uso excessivo do produto ou serviço por criança ou adolescente;

III – oferta de ferramentas para acompanhamento do uso adequado e saudável do produto ou serviço;

IV – emprego de interfaces que permitam a imediata visualização e limitação do tempo de uso do produto ou serviço;

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

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

VII – promoção da educação digital midiática quanto ao uso seguro de produtos ou serviços de tecnologia da informação;

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;

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.

Art. 18. As ferramentas de supervisão parental deverão permitir aos pais e responsáveis legais:

I – visualizar, configurar e gerenciar as opções de conta e privacidade da criança ou do adolescente;

II – restringir compras e transações financeiras;

III – identificar os perfis de adultos com os quais a criança ou o adolescente se comunica;

IV – acessar métricas consolidadas do tempo total de uso do produto ou serviço;

V – ativar ou desativar salvaguardas por meio de controles acessíveis e adequados;

VI – dispor de informações e de opções de controle em língua portuguesa.

§ 1º As informações sobre as ferramentas de supervisão parental deverão ser disponibilizadas de maneira clara e apropriada às diferentes idades, capacidades e necessidades de desenvolvimento,

sem incentivar a desativação ou o enfraquecimento das salvaguardas.

§ 2º É vedado ao fornecedor projetar, modificar ou manipular interfaces com o objetivo ou efeito de comprometer a autonomia, a tomada de decisão ou a escolha do usuário, especialmente se resultar no enfraquecimento das ferramentas de supervisão parental ou das salvaguardas.

1. SUPERVISÃO PARENTAL

A supervisão parental em produtos e serviços digitais voltados a crianças e adolescentes constitui uma das áreas mais sensíveis da regulação contemporânea da tecnologia. O núcleo central desse debate é a busca por equilíbrio entre a proteção integral da criança e do adolescente, princípio constitucional que orienta toda a normativa sobre infância e juventude no Brasil (art. 227 da Constituição Federal), e o respeito ao desenvolvimento progressivo da autonomia do menor, reconhecendo-o como sujeito de direitos e não apenas como objeto de tutela.

O marco legal estabelecido pelo Capítulo V do ECA Digital avança ao positivar obrigações específicas para fornecedores de produtos ou serviços de tecnologias da informação voltadas ao uso de crianças e adolescentes – ou, como é sempre bom reforçar, de acesso provável por esse público – exigindo que tais fornecedores incorporem em seus produtos e serviços ferramentas de segurança, transparência e controle, voltadas não apenas aos pais e responsáveis, mas também às próprias crianças e adolescentes, de acordo com a sua capacidade de compreensão.

2. O DEVER DE INFORMAÇÃO E A CENTRALIDADE DA PRIVACIDADE

O artigo 16 do ECA Digital impõe aos fornecedores a obrigação de informar, de forma acessível e independente da aquisição do produto ou serviço, os riscos e as medidas de segurança aplicáveis. Essa disposição está em consonância com o artigo 14 da Lei Geral de Proteção de Dados, que prevê um regime especial de tratamento de dados pessoais de crianças e adolescentes, fundado no princípio do melhor interesse.

Inclusive, sempre que houver tratamento de dados de crianças e adolescentes, o ECA Digital reforça a obrigação dos fornecedores de mapear