Organizador:
HIGOR VINICIUS NOGUEIRA JORGE

Comentários ao

ESTATUTO DIGITAL DA CRIANÇA E DO ADOLESCENTE

Lei Felca (15.211/25)

Adair Dias de Freitas Júnior
Adriano Augusto Fidalgo
Alesandro Gonçalves Barreto
Antônio Wellington Brito Júnior
Carolina Nascimento Silva Aguiar
Cecilia Bijos
Christiany Pegorari Conte
Emerson Wendt
Francini Imene Dias Ibrahin
Hericson dos Santos
Higor Vinicius Nogueira Jorge
Jacqueline Valadares da Silva Alckmim
Jorge André Domingues Barreto
Leonardo Rocha Vieira
Marcello Doria Costa
Mariana Alves Machado Nascimento
Patrícia Pacheco Rodrigues Machida
Quésia Pereira Cabral
Tiago Lustosa Luna de Araújo

2026

EDITORA JusPODIVM
www.editorajuspodivm.com.br

CAPÍTULO IX – DAS REDES SOCIAIS

Alesandro Gonçalves Barreto

Delegado de Polícia Civil do Piauí. Mestre em Segurança da Informação e Continuidade de Negócio pela Universidade de Múrcia (Espanha). Especialista em investigação de crimes cibernéticos, fraudes eletrônicas e inteligência policial. Ex-coordenador do Laboratório de Operações Cibernéticas – CIBERLAB/SENASP/MJSP, com atuação destacada em grandes operações nacionais de combate ao crime digital. Autor de 14 livros publicados sobre investigação digital, cibersegurança e inteligência aplicada à segurança pública. Palestrante em eventos nacionais e internacionais, com foco em OSINT, cibercrime, fraudes eletrônicas e cooperação entre autoridades e empresas de tecnologia. delbarretoacademia@gmail.com

Quésia Pereira Cabral

Delegada de Polícia Civil do estado do Pará. Doutora e Mestra em Direitos Humanos pela Universidade Federal do Pará (2024), possui ampla experiência na aplicação da lei, tendo exercido o cargo de Coordenadora Adjunta do Laboratório de Operações Cibernéticas do Ministério da Justiça do Brasil, onde trabalhou ativamente na operação conhecida como “Escola Segura”. Anteriormente, ocupou funções de liderança na Polícia Civil do Estado do Pará, coordenando operações de inteligência e investigações de crimes cibernéticos. Atualmente, é pesquisadora convidada do Instituto Internacional de Criminologia Comparada da Universidade de Montreal, no Canadá, onde desenvolve pesquisa pós-doutoral sobre processos de radicalização online e ataques em escolas.

Art. 24. No âmbito de seus serviços, os provedores de produtos ou serviços direcionados a crianças e a adolescentes ou de acesso provável por eles deverão garantir que usuários ou contas de crianças e de adolescentes de até 16 (dezesseis) anos de idade estejam vinculados ao usuário ou à conta de um de seus responsáveis legais.

§ 1º Caso seus serviços sejam impróprios ou inadequados para crianças e adolescentes, os provedores de redes sociais deverão adotar medidas adequadas e proporcionais para:

I – informar de maneira clara, destacada e acessível a todos os usuários que seus serviços não são apropriados;

II – monitorar e restringir, no limite de suas capacidades técnicas, a exibição de conteúdos que tenham como objetivo evidente atrair crianças e adolescentes;

III – aprimorar, de maneira contínua, seus mecanismos de verificação de idade para identificar contas operadas por crianças e adolescentes.

§ 2º O grau de efetividade e o progresso dos mecanismos referidos no inciso III do § 1º deste artigo serão avaliados pela autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital, nos termos de regulamentação específica.

§ 3º Os provedores de redes sociais poderão requerer dos responsáveis por contas com fundados indícios de operação por crianças e adolescentes que confirmem sua identificação, inclusive por meio de métodos complementares de verificação, observado que os dados coletados deverão ser utilizados exclusivamente para verificação de idade.

§ 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.

> **§ 5º** Na ausência de usuário ou conta dos responsáveis legais, os provedores deverão vedar a possibilidade de alteração das configurações de supervisão parental da conta para um nível menor de proteção em relação ao padrão estabelecido nos arts. 3º e 7º desta Lei.

A Lei 15.211/2025 consagra em seu bojo a passagem da obrigação exclusiva do Estado para um modelo de responsabilidade compartilhada entre os setores público e privado, trazendo institutos de afirmação de Direitos humanos no âmbito da proteção da criança e do adolescente na era digital. É certo que a própria Constituição da República Federativa do Brasil de 1988 (CRFB/88) já tenha previsão do que se convencionou chamar de princípio da proteção integral, previsto no art. 227, segundo o qual os direitos da criança do adolescente são deveres compartilhados entre a família, a sociedade e o Estado. No entanto, o ECA digital vai um pouco além, trazendo no conteúdo dos arts. 24 a 27 princípios de *soft law* globalmente reconhecidos no âmbito das responsabilidades das empresas em relação aos direitos humanos.

Os referidos princípios (UNGPs) foram historicamente previstos em documento das Nações Unidas (United Nations, 2011) e devidamente endossados pelo Conselho de Direitos Humanos, por meio da Resolução A/HRC/RES/17/4. É a partir desse documento que se tem fortemente estabelecido que a atividade empresarial, inclusive no ambiente digital, não pode ser incompatível com os direitos humanos, impondo-se uma mudança verdadeiramente paradigmática, na medida em que as grandes corporações deixam de ser vistas tão somente como agentes econômicos, passando a ser reconhecidas como portadores de deveres sociais e éticos. Nessa sistemática existem basicamente três pilares interdependentes: *protect, respect and remedy*.

O primeiro pilar atribui aos Estados o dever de proteger as pessoas contra abusos de direitos humanos cometidos por terceiros, inclusive por empresas. Por sua vez, o segundo impõe às empresas o dever de evitar causar ou contribuir para violações de direitos humanos em suas operações e cadeias de valor. Finalmente, o terceiro pilar reconhece que tanto Estados quanto empresas devem garantir meios eficazes de reparação às vítimas de abusos. Essa estrutura

não cria obrigações jurídicas diretas, mas define padrões de comportamento esperados, servindo como referência para legislações nacionais, políticas corporativas e mecanismos internacionais de regulação.

O elemento central do segundo pilar é o conceito de *human rights due diligence* (diligência devida em direitos humanos), previsto nos Princípios 17 a 21 (United Nations, 2011). Trata-se de um processo contínuo pelo qual as empresas devem identificar, prevenir, mitigar e prestar contas sobre os impactos reais ou potenciais de suas atividades nos direitos humanos. A diligência devida exige que as empresas conduzam avaliações de risco, adotem medidas corretivas e publiquem relatórios de transparência, evidenciando como estão gerindo riscos sociais, ambientais e de governança. Diferentemente do *compliance* tradicional, o enfoque dos UNGPs é preventivo e relacional: o objetivo é integrar a perspectiva dos direitos humanos em todas as etapas da operação empresarial, desde o design de produtos até a gestão de dados e algoritmos.

A partir de 2018, a aplicação desses princípios foi progressivamente expandida para o contexto digital, sobretudo com ênfase nas grandes empresas de tecnologia. O Alto Comissariado das Nações Unidas para os Direitos Humanos (OHCHR) lançou o *B-Tech Project*, justamente como objetivo de operacionalizar os UNGPs no setor tecnológico, detalhando como o princípio de *human rights due diligence* deve ser aplicado a plataformas digitais, especialmente em relação à moderação de conteúdo, publicidade comportamental e uso ético de dados (OHCHR, 2019; 2021). No mesmo sentido, o UNICEF desenvolveu a *Policy Guidance on AI for Children*, recomendando que as empresas de tecnologia adotem processos de *due diligence* específicos voltados à transparência, à verificação de idade, à proteção de dados pessoais e ao design seguro por padrão, de modo a garantir a segurança e o bem-estar de crianças e adolescentes no ambiente digital (UNICEF, 2021).

Esses parâmetros foram reforçados pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), cuja *Recommendation on Children in the Digital Environment* estabeleceu que as empresas devem conduzir avaliações contínuas dos riscos que seus sistemas e práticas representam para os direitos fundamentais, em consonância com os *UN Guiding Principles on Business and Human*

Rights (OECD, 2021). Por fim, instrumentos regionais, como a *Recommendation CM/Rec(2018)7* do Conselho da Europa, consolidaram a noção de que a *due diligence* digital envolve a moderação de conteúdos nocivos e a adoção de mecanismos de segurança por *design* e por *default*, assegurando que os serviços digitais respeitem, protejam e promovam os direitos da criança no ambiente online (COUNCIL OF EUROPE, 2018). Dessa forma, pode-se afirmar que o contexto dos arts. 24 a 27 da Lei nº 15.211/2025 reproduz essa mentalidade de governança compartilhada dos direitos humanos no ambiente digital.

Especificamente no âmbito do art. 24, é possível afirmar que a exigência de que contas de crianças e adolescentes de até 16 anos estejam vinculadas a um responsável legal traz consigo a internalização do princípio da *due diligence* corporativa em direitos humanos (OHCHR, 2021), reafirmando o modelo de responsabilidade compartilhada acima descrito. Além disso, a verificação de idade e o vínculo parental constituem mecanismos de *safety by design*, conceito amplamente difundido na regulação europeia (COUNCIL OF EUROPE, 2022) e nas diretrizes da OCDE (OECD, 2021), segundo o qual a proteção deve ser incorporada ao próprio desenho da plataforma. O §1º impõe obrigações de transparência, monitoramento e restrição de conteúdo, o que alinha o ECA Digital à lógica do Digital Services Act (EU, 2022) e das orientações do UNICEF (2021), que preveem mecanismos proativos de aviso, classificação etária e controle parental.

O §2º, por sua vez, traz uma norma de eficácia limitada e caráter instrumental, já que aponta a necessidade de regulamentação posterior específica para a mensuração do grau de efetividade e progresso dos mecanismos de controle estabelecidos nos dispositivos antecedentes. Em termos de *human rights due diligence*, essa previsão desloca o debate da mera existência formal de controles para a mensuração de resultados (*outputs* e *outcomes*), alinhando-se à exigência de monitoramento contínuo e prestação de contas (OHCHR, 2019; 2021). Dessa forma, questiona-se acerca de qual regulamentação realmente seria capaz de especificar indicadores verificáveis como tempo médio de resposta e acessibilidade para responsáveis, além de processos de auditoria independentes e até mesmo relatórios periódicos de transparência pública. Aferir a efetividade das medidas

com parâmetros auditáveis e comparáveis de fato será um grande desafio.

O §3º autoriza requisições de confirmação aos responsáveis quando houver "fundados indícios" de operação por menores, inclusive com "métodos complementares". À luz da Lei nº 13.709/2018 (LGPD, arts. 6 e 14), esse tipo de requisição exige base legal adequada, finalidade específica ("exclusivamente para verificação de idade"), minimização de dados e estrita proporcionalidade dos meios. Para atender aos parâmetros da *due diligence*, estas requisições em comento deveriam: (i) hierarquizar técnicas de menor intrusão (declaração assistida, verificação por responsável, checagem documental ofuscada), (ii) impor limites temporais de retenção e proibições de reutilização (sem perfilamento ou publicidade), e (iii) prever testes de impacto quando houver uso de biometria ou IA (UNICEF, 2021; OHCHR/B-Tech, 2021). Atendendo a estes parâmetros, ter-se-ia garantida a proteção da criança com não-exacerbação de riscos (vazamentos, vigilância excessiva), preservando-se transparência e direito de explicação dos processos automatizados (OECD, 2021).

O § 4º prevê suspensão do acesso diante de "fundados indícios" de violação etária, condicionada à abertura de procedimento célere e acessível para apelação e prova de idade pelo responsável. Em termos de UNGPs, trata-se de articular mitigação de risco imediato (proteção da criança) com garantias procedimentais (*access to remedy*) (OHCHR, 2019; 2021). No entanto, o problema é que tanto o §3º, quanto o §4º deixam em aberto o que de fato seria considerado um "fundado indício". Assim, como não se tem uma clara delimitação do que seja o padrão de "fundado indício", torna-se de suma importância a notificação clara do usuário com os fundamentos e meios de impugnação, com prazos para decisão, canais inclusivos, utilizando linguagem simples e acessível. Além disso, é importante prever como se daria a reversibilidade em caso de erro. Todos esses parâmetros poderiam reduzir as possibilidades de *over-blocking* (CRC/GC 25, 2021; OECD, 2021).

Finalmente, o § 5º complementa o sistema protetivo do artigo 24 ao vedar a diminuição do nível de proteção configurado por padrão na ausência de conta vinculada a responsável legal. Essa disposição concretiza o princípio de *safety by default*, princípio consagrado nas

diretrizes internacionais de governança digital (COUNCIL OF EUROPE, 2022; OECD, 2021), segundo o qual a configuração inicial de qualquer serviço acessível a crianças deve assegurar máximo grau de proteção e privacidade, cabendo aos responsáveis ajustar restrições de forma consciente e informada. Trata-se de grande evolução legislativa que dá uma nova roupagem ao princípio da proteção integral a criança e ao adolescente. Na perspectiva da *human rights due diligence*, essa norma traduz a etapa de prevenção estrutural dos riscos, isto é, a incorporação da proteção da infância ao próprio design da plataforma (OHCHR, 2019; UNICEF, 2021). Ao impedir que usuários menores manipulem configurações de supervisão parental, o dispositivo reduz vulnerabilidades ligadas à exposição a conteúdos impróprios, coleta excessiva de dados e contato indevido com terceiros. Trata-se, portanto, de um mecanismo normativo que fortalece a proteção integral no ambiente digital, convertendo em dever jurídico o que antes era mera recomendação ética de design seguro.

Ainda no âmbito do art. 24, observa-se que o legislador elevou o patamar etário para a obrigatoriedade de controle parental, estabelecendo o limite de 16 anos, acima do padrão internacionalmente adotado por diversas plataformas digitais e legislações estrangeiras. Nos Estados Unidos, a *Children's Online Privacy Protection Act* (COPPA) aplica-se à coleta de dados de crianças com menos de 13 anos, exigindo consentimento parental. Nos países da União Europeia, conforme o art. 8.º do *General Data Protection Regulation* (GDPR), o limiar padrão para consentimento por parte da própria criança é de 16 anos, cabendo aos Estados-membros definir idades inferiores, porém nunca abaixo dos 13 anos. Essa diferenciação permite afirmar que o Brasil, ao adotar o limite de 16 anos para vinculação de conta de criança ou adolescente a usuário responsável, alinha-se ao extremo superior desse intervalo e reflete uma escolha normativa voltada ao fortalecimento da supervisão parental e da proteção integral na era digital, em consonância com as diretrizes de *human rights due diligence* do Alto Comissariado das Nações Unidas para os Direitos Humanos (OHCHR, 2019; 2021) e com as recomendações da Organização para a Cooperação e Desenvolvimento Econômico sobre segurança infantil online (OECD, 2021).

Todavia, essa elevação etária suscita dilemas práticos relevantes, sobretudo no que diz respeito às contas antigas ou pré-existentes,

criadas antes da entrada em vigor da Lei nº 15.211/2025. Como vincular retroativamente essas contas aos pais ou responsáveis sem violar o princípio da minimização de dados e o consentimento informado previsto no art. 14 da Lei nº 13.709/2018 (LGPD – BRASIL, 2018)? Essa tensão entre a necessidade de conformidade regulatória e o respeito à privacidade demonstra o desafio de implementar uma política de adequação progressiva, guiada por critérios de proporcionalidade e risco. O Alto Comissariado das Nações Unidas para os Direitos Humanos (OHCHR, 2021) e o UNICEF (2021) recomendam que as plataformas adotem procedimentos graduais de verificação parental, com prazos razoáveis, comunicações educativas e mecanismos de correção voluntária antes da aplicação de sanções automáticas, a fim de evitar violações à boa-fé e ao direito à autodeterminação informativa. Outro ponto de alta complexidade é a efetividade técnica da verificação etária. A lei impõe às plataformas o dever de informar, monitorar, restringir e verificar a idade dos usuários, mas a execução prática dessas medidas permanece um desafio global. Em plataformas de *streaming* de conteúdo adulto ou redes com alto potencial de exposição, surge a dúvida sobre como identificar e limitar o acesso de menores de forma proporcional e não invasiva.

A verificação por documentos oficiais é vulnerável à falsificação e contraria o princípio da minimização de dados; a biometria facial e o reconhecimento de idade por inteligência artificial, por sua vez, levantam questões de acurácia e proteção de dados sensíveis (OECD, 2021; COUNCIL OF EUROPE, 2022; UNICEF, 2021). Nesse cenário, as soluções mais adequadas envolvem métodos híbridos de autenticação contextual, combinando sinais de uso, histórico de navegação e consentimento parental supervisionado (OHCHR, 2019; OECD, 2021). Em última análise, a eficácia da norma dependerá da capacidade técnica e da boa-fé corporativa das plataformas, monitoradas pela autoridade administrativa autônoma prevista no § 2º do próprio artigo.

> **Art. 25.** Os provedores de redes sociais deverão prever regras específicas para o tratamento de dados de crianças e de adolescentes, definidas de forma concreta e documentada e com base no seu melhor interesse.

O artigo 25 traduz para o plano normativo nacional os princípios de proteção de dados pessoais e de governança ética da informação consagrados no Regulamento Geral de Proteção de Dados da União Europeia (GDPR, art. 8º) e na Lei nº 13.709/2018 (LGPD – BRASIL, 2018, art. 14). Ao determinar que o tratamento de dados de crianças e adolescentes seja regido pelo melhor interesse do titular, a norma concretiza a diretriz segundo a qual a coleta, o tratamento e o armazenamento de dados de menores somente se legitimam quando possuírem finalidade protetiva, educativa ou de bem-estar social, afastando qualquer uso econômico ou publicitário. Essa exigência reflete as recomendações do UNICEF (2021) e do OHCHR (2019), que compreendem a *due diligence* digital como um processo preventivo de avaliação e mitigação de riscos informacionais, especialmente os que envolvem exposição indevida, perfilamento ou exploração de vulnerabilidades emocionais.

Em comparação com o art. 14 da LGPD, o artigo 25 amplia o alcance protetivo: enquanto a LGPD limita-se a exigir consentimento dos pais e tratamento em benefício da criança, o ECA Digital introduz um padrão positivo de governança corporativa, impondo às plataformas o dever de documentar, auditar e comprovar a legitimidade e a finalidade protetiva de todas as operações de dados envolvendo menores. Trata-se de um modelo de responsabilização ativa, coerente com os princípios de *accountability* e *transparency by design* do GDPR (2016) e da OECD (2021). Assim, plataformas que não demonstrem políticas concretas de controle, revisão periódica e mitigação de riscos poderão ser presumidas negligentes, configurando violação ao dever de diligência corporativa.

> **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.

O artigo 26 materializa uma das inovações mais relevantes do Estatuto Digital da Criança e do Adolescente, ao proibir o uso de dados de crianças e adolescentes para fins de publicidade comportamental. Trata-se de uma resposta direta à lógica da *economia da*

atenção, que se baseia na observação, classificação e predição de comportamentos com vistas à maximização de engajamento e lucro. A lógica descrita como *economia da atenção* foi originalmente desenvolvida Simon (1971), segundo o qual a quantidade excessiva de informação traz consigo a pobreza da capacidade de atenção. O referido conceito foi posteriormente por autores como Davenport et al. (2001), os quais aplicaram a ideia na gestão e marketing digital, bem como por Wu (2016), que descreveu como a disputa pela atenção humana transformou-se no eixo central das indústrias de mídia e tecnologia. No campo crítico, Zuboff (2019) introduziu o conceito de *capitalismo de vigilância*, destacando que o modelo de negócios das *big techs* se estrutura exatamente na observação, classificação e predição de comportamentos humanos para fins de lucro. De modo semelhante, Bucher (2018) e Srnicek (2017) analisaram como plataformas como Facebook, Google e TikTok constroem sistemas de engajamento contínuo por meio de algoritmos projetados para maximizar o tempo de exposição e monetizar dados comportamentais. Estas preocupações estão presentes a nível internacional em relatórios da UNESCO (2023) e do OECD (2021) reconhecem formalmente a *economia da atenção* como risco estrutural à autonomia e ao bem-estar digital, especialmente de crianças e adolescentes, por estimular práticas de manipulação emocional e publicidade personalizada com base em dados sensíveis.

Voltando ao texto do art. 26, resta claro que a norma impede que plataformas coletem, tratem ou analisem dados pessoais ou grupais de crianças e adolescentes, inclusive os obtidos nos processos de verificação de idade, com o objetivo de exibir anúncios personalizados, o que representa uma ruptura com o modelo de monetização (OHCHR, 2021; OECD, 2021). O referido dispositivo reflete uma proibição absoluta, sem margem para consentimento parental ou justificativas contratuais, pois a exploração econômica da atenção infantil é, por essência, incompatível com o princípio do melhor interesse da criança. A vedação harmoniza-se com o art. 227 da CRFB/88, que impõe dever absoluto à família, à sociedade e ao Estado de proteger crianças e adolescentes contra qualquer forma de exploração econômica e manipulação, e com o art. 17 do ECA (Lei 8069/90), que assegura o direito à privacidade, à imagem e à preservação da identidade. Também dialoga diretamente com o art. 14 da

Lei Geral de Proteção de Dados (LGPD), que veda o tratamento de dados de crianças para finalidades comerciais.

No contexto internacional, o artigo 26 alinha-se às restrições do Regulamento Geral de Proteção de Dados da União Europeia (GDPR, art. 8º e considerando 38) e às recomendações do UNICEF (2021) e da OCDE (2021), que classificam o *behavioral advertising* dirigido a menores como prática intrinsecamente lesiva aos direitos humanos digitais. Essas diretrizes reconhecem que o poder preditivo dos algoritmos, ao capturar padrões de consumo e preferências, cria ambientes de manipulação comportamental e de reforço de vulnerabilidades psicológicas. Por fim, o dispositivo impõe às plataformas o dever contínuo de revisar seus sistemas de recomendação, assegurando que o conteúdo apresentado a crianças e adolescentes seja neutro, não comercial e livre de vieses exploratórios. Essa obrigação traduz, no plano técnico, o princípio do *safety by design and by default*, exigindo que a arquitetura dos algoritmos e dos fluxos de dados seja construída para proteger e não explorar. O artigo 26, portanto, consagra um modelo de governança ética da informação infantil, ancorado na ideia de que a proteção de dados pessoais de menores é um direito fundamental indisponível e um imperativo de justiça digital.

CAPÍTULO X – DA PREVENÇÃO E COMBATE A VIOLAÇÕES GRAVES CONTRA CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL

Alesandro Gonçalves Barreto

Delegado de Polícia Civil do Piauí. Mestre em Segurança da Informação e Continuidade de Negócio pela Universidade de Múrcia (Espanha). Especialista em investigação de crimes cibernéticos, fraudes eletrônicas e inteligência policial. Ex-coordenador do Laboratório de Operações Cibernéticas – CIBERLAB/SENASP/MJSP, com atuação destacada em grandes operações nacionais de combate ao crime digital. Autor de 14 livros publicados sobre investigação digital, cibersegurança e inteligência aplicada à segurança pública. Palestrante em eventos nacionais e internacionais, com foco em OSINT, cibercrime, fraudes eletrônicas e cooperação entre autoridades e empresas de tecnologia. delbarretoacademia@gmail.com

Quésia Pereira Cabral

Delegada de Polícia Civil do estado do Pará. Doutora e Mestra em Direitos Humanos pela Universidade Federal do Pará (2024), possui ampla experiência na aplicação da lei, tendo exercido o cargo de Coordenadora Adjunta do Laboratório de Operações Cibernéticas do Ministério da Justiça do Brasil, onde trabalhou ativamente na operação conhecida como "Escola Segura". Anteriormente, ocupou funções de liderança na Polícia Civil do Estado do Pará, coordenando operações de inteligência e investigações de crimes cibernéticos. Atualmente, é pesquisadora convidada do Instituto Internacional de Criminologia Comparada da Universidade de Montreal, no Canadá, onde desenvolve pesquisa pós-doutoral sobre processos de radicalização online e ataques em escolas.

> **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.
>
> **§ 1º** Os relatórios de notificação de conteúdos de exploração, de abuso sexual, de sequestro e de aliciamento de crianças e de adolescentes deverão ser enviados à autoridade competente, observados os requisitos e os prazos estabelecidos em regulamento.
>
> **§ 2º** Os fornecedores deverão reter, pelo prazo estabelecido no art. 15 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), os seguintes dados associados a um relatório de conteúdo de exploração e de abuso sexual de criança ou de adolescente:
>
> **I –** conteúdo gerado, carregado ou compartilhado por qualquer usuário mencionado no relatório e metadados relacionados ao referido conteúdo;
>
> **II –** dados do usuário responsável pelo conteúdo e metadados a ele relacionados.
>
> **§ 3º** O prazo de que trata o § 2º deste artigo poderá ser superior ao estabelecido no art. 15 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), desde que formulado requerimento na forma do § 2º do art. 15 da referida Lei.

O artigo 27 representa um marco normativo de integração entre a responsabilidade corporativa e a investigação cibernética, ao estabelecer uma obrigação legal expressa de dupla natureza: remover e comunicar conteúdos relacionados à exploração sexual, ao abuso, ao sequestro ou ao aliciamento de crianças e adolescentes. Essa previsão converte em dever jurídico vinculante o que, até então, figurava apenas como uma obrigação moral ou de boa-fé cooperativa das plataformas digitais. Em consonância com o modelo de *human rights due diligence* delineado pelo Alto Comissariado das Nações Unidas para os Direitos Humanos (OHCHR, 2011; 2019; 2021) e com o terceiro pilar dos UN Guiding Principles on Business and Human Rights (*access to remedy*), o dispositivo impõe às empresas a criação de mecanismos internos permanentes de vigilância, reporte

e preservação de provas digitais, contribuindo para respostas mais céleres e eficazes diante de violações graves contra crianças e adolescentes.

A norma também inaugura no Brasil uma etapa de compliance digital obrigatório, ao determinar que os provedores de tecnologia mantenham fluxos institucionais padronizados para notificação e retenção de evidências, com base em padrões internacionais de *accountability* e rastreabilidade (UNODC, 2021). O §1º reforça essa padronização ao prever relatórios de notificação que deverão observar prazos e requisitos definidos em regulamento, assegurando transparência, auditabilidade e interoperabilidade entre empresas e autoridades. Essa estrutura se alinha a práticas internacionais já consolidadas em sistemas como o National Center for Missing and Exploited Children (NCMEC, 2023), nos Estados Unidos, à SaferNet Brasil (2023) e à rede global de cooperação coordenada pela INTERPOL (2022), que padronizam os fluxos de comunicação entre plataformas, autoridades nacionais e organismos internacionais para enfrentamento do abuso sexual infantil online.

Os §§2º e 3º, ao preverem a retenção temporária de conteúdos e metadados associados às notificações, garantem a preservação de provas digitais indispensáveis à persecução penal e à cooperação internacional. Essa obrigação é coerente com o art. 15 do Marco Civil da Internet (Lei nº 12.965/2014) e dialoga com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), que exige proporcionalidade, limitação de finalidade e minimização de dados. O ECA Digital, contudo, amplia o alcance desses dispositivos, permitindo que o prazo de retenção seja estendido mediante justificativa, equilibrando eficiência investigativa e proteção de direitos fundamentais. Essa harmonização reflete as obrigações já previstas em tratados internacionais como a Convenção de Budapeste sobre o Cibercrime (COUNCIL OF EUROPE, 2001) e a Convenção de Lanzarote (COUNCIL OF EUROPE, 2007), que impõem deveres de preservação de dados e cooperação interestatal em crimes contra crianças.

Ao consolidar essas exigências, o artigo 27 institucionaliza a cooperação público-privada como instrumento de defesa dos direitos humanos digitais. As plataformas deixam de atuar apenas como intermediárias técnicas e passam a exercer papel ativo de vigilância

ética e resposta imediata a conteúdos ilícitos, transformando o antigo dever moral de colaboração em obrigação jurídica estruturante. Essa mudança de paradigma reflete o modelo de governança compartilhada consagrado pelos UN Guiding Principles (OHCHR, 2011) e reconhecido pela Organização para a Cooperação e Desenvolvimento Econômico (OECD, 2021), segundo o qual as empresas de tecnologia são coautoras do dever de proteção e corresponsáveis pela garantia do melhor interesse da criança e do adolescente no ambiente digital.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da União*, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). *Diário Oficial da União*, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 15.211, de 2025. Institui o *Estatuto Digital da Criança e do Adolescente*. *Diário Oficial da União*, Brasília, DF, 2025.

BUCHER, Taina. *If... Then: Algorithmic Power and Politics.* New York: Oxford University Press, 2018.

COUNCIL OF EUROPE. *Convention on Cybercrime (Budapest Convention).* Budapest: Council of Europe, 2001.

COUNCIL OF EUROPE. *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention).* Strasbourg: Council of Europe, 2007.

COUNCIL OF EUROPE. *Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.* Strasbourg: Council of Europe, 2018.

COUNCIL OF EUROPE. *Recommendation CM/Rec(2022)4 on the Protection of Children's Rights in the Digital Environment.* Strasbourg: Council of Europe, 2022.

DAVENPORT, Thomas H.; BECK, John C. *The Attention Economy: Understanding the New Currency of Business.* Boston: Harvard Business School Press, 2001.

EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*