

CIBERESPAÇO E DIGNIDADE SEXUAL: DESAFIOS PARA A PROTEÇÃO DE CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL

**CYBERSPACE AND SEXUAL DIGNITY: CHALLENGES FOR THE PROTECTION
OF CHILDREN AND ADOLESCENTS IN THE DIGITAL ENVIRONMENT**

Ciências Humanas • 09/10/2026

REGISTRO DOI: [10.70773/revistatopicos/791519316](https://doi.org/10.70773/revistatopicos/791519316)

Ana Maria de Alencar Silva¹

Clara Isadora Soares de Freitas²

Jhon Kennedy Teixeira Lisbino³

RESUMO

O presente artigo analisa os desafios jurídicos para a proteção da dignidade sexual de crianças e adolescentes no ambiente virtual. Em decorrência do aumento do acesso precoce às plataformas digitais por crianças e adolescentes, resultando no crescimento de condutas ilícitas como o *grooming* e a exploração sexual infantil, o estudo examina a eficácia das normas brasileiras, com destaque para o Estatuto da Criança e do Adolescente (ECA), o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), a recente Lei nº 15.211/2025 (Lei Felca) e a Lei nº 15.487/2026. Discutem-se os principais óbices à aplicabilidade da tutela jurídica, tais como o anonimato digital, a jurisdição transnacional e a responsabilidade das plataformas. A pesquisa adota metodologia qualitativa e bibliográfica, com análise documental e doutrinária. Conclui-se que a tutela efetiva dos vulneráveis no ciberespaço exige a articulação entre o rigor normativo, a atuação ativa dos provedores e o aprimoramento de políticas públicas de prevenção.

Palavras-chave: Ciberespaço; Dignidade sexual; Proteção integral; Crimes virtuais; Estatuto da Criança e do Adolescente.

ABSTRACT

This article analyzes the legal challenges regarding the protection of the sexual dignity of children and adolescents in the virtual environment. In light of the increased early access to digital platforms by children and adolescents, leading to a rise in illicit conducts such as grooming and child sexual exploitation, the study examines the effectiveness of Brazilian legal frameworks, particularly the Statute of the Child and Adolescent (ECA), the Brazilian Internet Bill of Rights, the General Personal Data Protection Law (LGPD), and the recent Law nº 15.211/2025 (Digital Statute of Children and Adolescents), and Law nº 15.487/2026. The main obstacles to the

applicability of legal protection are discussed, including digital anonymity, transnational jurisdiction, and platform liability. The research adopts a qualitative and bibliographical methodology, incorporating legal document and doctrine analysis. It concludes that effective protection for vulnerable individuals in cyberspace requires alignment between regulatory rigor, active engagement from service providers, and the improvement of public policies for traceability and prevention.

Keywords: Cyberspace; Sexual dignity; Comprehensive protection; Cybercrimes; Digital Statute of Children and Adolescents.

1. INTRODUÇÃO

A análise desenvolvida neste estudo busca examinar de que modo o ambiente virtual ampliou os riscos relacionados à segurança e à proteção da dignidade de crianças e adolescentes. Os avanços tecnológicos possuem grande relevância para a sociedade contemporânea, especialmente no que se refere à ampliação das formas de comunicação e interação social. No entanto, o uso crescente dessas ferramentas digitais também revela aspectos preocupantes, sobretudo diante do acesso cada vez mais precoce de menores a plataformas digitais, como Instagram e TikTok, além de jogos online que possibilitam interações em tempo real. A pesquisa TIC *Kids Online Brasil* (CGI.br, 2026, p.23), realizada em 2025 e divulgada em 2026, indica que 92% das crianças e dos adolescentes brasileiros de 9 a 17 anos são usuários de internet, o que corresponde a cerca de 24 milhões de pessoas. O acesso à internet já faz parte da rotina da maioria dos jovens brasileiros, o que amplia sua exposição a riscos no ambiente digital.

Dados recentes reforçam essa preocupação. Segundo a *SaferNet Brasil*, houve crescimento significativo nas denúncias de crimes virtuais envolvendo crianças e adolescentes nos últimos anos, entre janeiro e julho de 2025, o Canal Nacional de Denúncias de Crimes Cibernéticos da *SaferNet Brasil* registrou 49.336 denúncias anônimas de abuso e exploração sexual infantil, correspondendo a 64% do total de notificações no período, que foi de 76.997 denúncias. Além disso, segundo dados da UNICEF *Innocenti*, no Brasil, em apenas um ano, uma a cada cinco crianças e adolescentes de 12 a 17 anos (19%) foi vítima de exploração e/ou abuso sexual facilitados pela tecnologia. Tal dado representa um universo aproximado de 3 milhões de crianças e adolescentes afetados por violência sexual no contexto digital. As dinâmicas de violação não se restringem ao ciberespaço, podendo desdobrar-se em interações mistas (virtuais e presenciais) ou ocorrer principalmente no meio físico, hipótese na qual os recursos tecnológicos passam atuar como ferramentas para a gravação, propagação e perpetuação do dano.

Esse cenário evidencia a crescente vulnerabilidade desse público e reforça a necessidade de mecanismos eficazes de proteção. Diante dessa realidade, o ordenamento jurídico brasileiro tem buscado estabelecer instrumentos normativos voltados à proteção de crianças e adolescentes no ambiente virtual. Destacam-se, nesse sentido, o Estatuto da Criança e do Adolescente (ECA), instituído pela Lei nº 8.069/1990, que consagra o princípio da proteção integral; a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que regula o tratamento de dados pessoais e assegura a privacidade; o Marco Civil da Internet, Lei nº 12.965/2014, que estabelece princípios, garantias e direitos para o uso da internet no Brasil; a Lei nº 15.211/2025 (EDCA) que protege e ampara crianças e adolescentes no ambiente virtual e a Lei nº 15.487/2026 que endurece as punições

e amplia as medidas de repressão aos crimes de violência sexual contra esses vulneráveis.

Mas como o ambiente digital amplia a vulnerabilidade de crianças e adolescentes à prática de crimes contra a dignidade sexual, e quais os desafios para a efetividade dos mecanismos jurídicos de proteção e responsabilização previstos no ordenamento brasileiro?

Pressupõe-se que o ambiente digital, ao combinar anonimato, facilidade de acesso e ausência de supervisão, amplifica significativamente a vulnerabilidade de crianças e adolescentes à prática contra a dignidade sexual. Embora o ordenamento jurídico disponha de diplomas como ECA, LGPD e a Lei nº 15.211/2025 e a Lei nº 15.487/2026, a aplicação desses mecanismos enfrenta diversos entraves práticos e institucionais relativos ao anonimato, à jurisdição e à responsabilidade das plataformas.

O objetivo geral consiste em analisar de que forma o ambiente digital amplia a vulnerabilidade de crianças e adolescentes à prática de crimes contra a dignidade sexual, examinando os mecanismos jurídicos de proteção, as tipificações e os principais desafios para a responsabilização no ordenamento brasileiro. Os objetivos específicos desdobram-se em: a) Contextualizar a vulnerabilidade de crianças e adolescentes no ambiente digital, considerando as transformações da internet, o perfil de risco e o acompanhamento familiar; b) Identificar as principais formas de ocorrência de crimes sexuais contra crianças e adolescentes no ambiente virtual, especialmente o *grooming*, o aliciamento online e a exploração sexual digital; c) Examinar os mecanismos jurídicos e institucionais de prevenção e proteção de crianças e adolescentes no ambiente digital, com ênfase no ECA, no Marco Civil da Internet, na LGPD, na

Lei nº 15.211/2025 e na Lei nº 15.487/2026; d) Analisar os desafios à efetividade da proteção jurídica, considerando o anonimato digital, a jurisdição transnacional e a responsabilidade das plataformas.

A relevância social do presente estudo evidencia-se pelo alastramento da vitimização infantojuvenil no ciberespaço, corroborada por dados empíricos de órgãos como UNICEF e *SaferNet*. Sob o prisma jurídico, a investigação justifica-se pela necessidade de examinar o impacto sistêmico das leis nº 15.211/2025 e nº 15.487/2026 e da jurisprudência recente dos tribunais superiores ainda pouco sistematizadas pela dogmática. Por fim, a pertinência prática manifesta-se na utilidade de orientar famílias, escolas, plataformas de redes sociais e investigações policiais a lidarem melhor com o problema no dia a dia.

O presente estudo utiliza o método hipotético-dedutivo, adotando abordagem qualitativa e natureza exploratório-descritiva. Como técnicas de pesquisa, empregam-se a revisão bibliográfica doutrinária e a pesquisa documental. O corpus analisado compreende o ordenamento jurídico pátrio, acórdãos e precedentes do STF e STJ, além de relatórios institucionais da *SaferNet* e do UNICEF referentes ao período de referência da pesquisa.

O estudo estrutura-se em quatro seções de desenvolvimento, além da introdução e das considerações finais. A Seção 2 contextualiza a vulnerabilidade digital infantojuvenil e o perfil de risco; a Seção 3 examina a tipificação penal e a dinâmica do *grooming* e da exploração; a Seção 4 analisa os marcos normativos de proteção; a Seção 5 investiga os desafios operacionais do anonimato, jurisdição transnacional, responsabilidade das plataformas e retenção de

dados; por fim, a Seção 6 traz a síntese conclusiva retomando o problema e a hipótese à luz do que foi desenvolvido.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. A Vulnerabilidade de Crianças e Adolescentes no Ambiente Digital: Conceito, Perfil e Fatores de Risco

O mandamento primário do art.227 da Constituição Federal que impõe à família, à sociedade e ao Estado o dever de cuidar da infância e da juventude com absoluta prioridade, mantendo-as salvas de qualquer forma de violência ou exploração, encontra no ciberespaço seu desafio mais sensível, pois o ambiente virtual é um espaço que não tem fronteiras físicas e tem velocidade de milissegundos. A vulnerabilidade de crianças e adolescentes no ambiente digital deve ser interpretada de acordo com a doutrina da proteção integral, vigente no ordenamento jurídico brasileiro e materializada no Estatuto da Criança e do Adolescente (ECA). Essa vulnerabilidade decorre da visão de fragilidade em que essas crianças e adolescentes são seres dependentes e ainda em fase de desenvolvimento físico, psicológico e social, que se intensifica diante das dinâmicas próprias do ambiente virtual. Nesse sentido, Teresa Cristina Rebolho Rego aborda que crianças e adolescentes ainda não possuem maturidade suficiente para lidar com todas as situações que lhes são apresentadas, o que os torna mais suscetíveis à violação de direitos, principalmente em ambientes marcados pela ausência de controle direto e pela velocidade da informação, como ocorre na internet. (Rego, 2026)

O ambiente digital, por mais que forneça informação, educação e comunicação, também potencializa riscos, principalmente por sua

natureza difusa, descentralizada e muitas vezes anônima. Conforme Rosane Leal da Silva, a internet reconstitui as formas de interação social e expõe crianças e adolescentes a situações que ultrapassam os limites da convivência tradicional, exigindo uma releitura dos mecanismos de proteção jurídica. A autora salienta que a vulnerabilidade no meio digital não substitui a vulnerabilidade física, mas que é mais complexa e ampla, pois essas crianças e adolescentes estão inseridas em uma sociedade marcada pela violência e exposição, criando novos desafios para o Direito e para as políticas públicas. (Silva, 2022, p. 148)

De acordo com a UNICEF Brasil (2023), crianças e adolescentes estão cada vez mais inseridos no ambiente virtual desde cedo, em sua maioria sem a devida orientação ou acompanhamento. O uso precoce e intenso dessas plataformas digitais colabora para a formação de um cenário onde os riscos são constantes e diversificados, incluindo exposição a conteúdos impróprios, *cyberbullying*, exploração sexual online e coleta indevida de dados pessoais.

Observa-se que essas crianças e adolescentes já nascem inseridas no contexto tecnológico, desde cedo desenvolvem habilidades para uso de dispositivos eletrônicos e plataformas digitais. Apesar da familiaridade tecnológica, esse público ainda não possui maturidade emocional e cognitiva suficiente para compreender riscos envolvidos nas interações online. A busca por aceitação social é comum e evidente nesse cenário, ocorre especialmente nas redes sociais, onde as curtidas, comentários e compartilhamentos têm grande impacto na construção da identidade. Além disso, verifica-se uma predisposição à exposição excessiva de dados pessoais, imagens e rotinas, por conta da falta de maturidade e por essas crianças e

adolescentes não têm consciência das possíveis consequências. Segundo dados da UNICEF Brasil, esse uso excessivo sem a devida orientação e acompanhamento, pode intensificar mais essa condição de vulnerabilidade.

Diante disso, muitos fatores contribuem para o aumento de riscos no ambiente digital. A ausência e fragilidade de acompanhamento familiar é um dos principais elementos, a pesquisa TIC *Kids Online* Brasil (CGI.br, 2026, p. 141), realizada em 2025 e publicada em 2026, apontou que cerca de 58% dos adolescentes nunca receberam acompanhamento dos pais sobre o que fazem na internet e que 33% desses adolescentes não recebem nenhum acompanhamento sobre o que publicam nas redes sociais, o que dificulta a supervisão das atividades realizadas na internet e impedindo a identificação de situações perigosas, como tentativas de manipulação, golpes ou contatos mal-intencionados. A interação com desconhecidos também representa um fator relevante, podendo expor crianças e adolescentes a práticas como aliciamento e exploração. Outro aspecto importante é o acesso facilitado a conteúdos inadequados, como violência e discursos de ódio, que podem impactar negativamente o desenvolvimento psicológico. Cerca de um em cada dez adolescentes relataram se sentir frequentemente mal por algo que aconteceu online e, entre os usuários de 11 a 17 anos, 20% já receberam alguma mensagem ou solicitação de cunho sexual, de acordo com a pesquisa TIC *Kids Online* Brasil (2025, p. 24). Por fim, características próprias do ambiente virtual, como a rápida disseminação de informações e a dificuldade de controle sobre conteúdos compartilhados, fazem com que eventuais exposições indevidas tenham efeitos mais amplos e duradouros.

2.2. Crimes Sexuais Contra Crianças e Adolescentes no Ambiente Virtual: Tipificação Penal, Modalidades e Dinâmicas do *Grooming* e da Exploração Sexual

O cenário digital contemporâneo, embora catalisador de direitos e acessos, consolidou-se também como um local para o surgimento e o refinamento de graves violações aos direitos fundamentais de crianças e adolescentes. A transição da criminalidade sexual do ambiente físico para o virtual não representa apenas uma mudança de meio, mas uma alteração profunda nas dinâmicas de vitimização, que agora contam com o anonimato, a transnacionalidade e a perenidade dos dados na rede. Sob essa ótica, o ordenamento jurídico brasileiro passou por intensas atualizações, culminando em normas como a Lei nº 15.211/2025 e a Lei nº 15.487/2026.

Neste tópico, busca-se analisar a tipificação penal dessas condutas. A tutela penal da dignidade sexual infantojuvenil no ambiente digital estrutura-se, essencialmente, na conjugação entre o Estatuto da Criança e do Adolescente e o Código Penal (Decreto-Lei nº 2.848/1940). A tipificação específica das condutas praticadas em meio digital remonta à Lei nº 11.829/2008, que inseriu os arts. 241-A a 241-E no ECA, tendo o tratamento penal sido sucessivamente agravado pelas Leis nº 14.811/2024, Lei nº 15.280/2025 e a Lei nº 15.487/2026. As penas a seguir transcritas resultam do agravamento e da evolução promovidos pelas reformas mais recentes.

Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, conteúdo de violência sexual contra criança ou adolescente: Pena - reclusão, de 4 (quatro) a 10 (dez) anos, e multa. (BRASIL, 1990, art. 240, redação pela Lei nº15.487/2026).

Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha violência sexual contra criança ou adolescente: Pena - reclusão, de 4 (quatro) a 10 (dez) anos, e multa, além da perda de bens e valores recebidos em virtude da prática criminosa em favor do Fundo dos Direitos da Criança e do Adolescente da unidade da Federação em que foi cometido o crime, ressalvado o direito de terceiro de boa-fé. (BRASIL, 1990, art. 241, redação dada pela Lei nº15.487/2026).

Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha violência sexual contra criança ou adolescente: Pena - reclusão, de 4 (quatro) a 10 (dez) anos, e multa. (BRASIL, 1990, art. 241-A, redação dada pela Lei nº15.487/2026).

Art. 241-B. Adquirir, possuir, armazenar ou solicitar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha violência sexual contra criança ou adolescente: Pena - reclusão, de 3 (três) a 6 (seis) anos, e multa. (BRASIL, 1990, art. 241-B, redação dada pela Lei nº15.487/2026).

Art. 241-C. Simular a participação de criança ou adolescente em conteúdo de violência sexual por meio de adulteração, montagem ou modificação de fotografia, vídeo ou outra forma de representação visual, mediante qualquer recurso tecnológico que altere imagem ou voz da vítima, inclusive com uso de inteligência artificial: Pena - reclusão, de 3 (três) a 5 (cinco) anos, e multa. (BRASIL, 1990, art. 241-C, redação dada pela Lei nº 15.487/2026).

Art. 241-D. Aliciar, assediar, convidar, instigar ou constranger, por qualquer meio, menor de 14 (quatorze) anos, com o fim de praticar ato libidinoso: Pena - reclusão, de 3 (três) a 5 (cinco) anos, e multa, se o fato não constituir crime mais grave.

[...] § 2º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o agente pratica as condutas previstas no caput e no § 1º deste artigo:

I - utilizando recursos de inteligência artificial, deepfake, filtros ou qualquer outro recurso tecnológico que permita ao autor alterar sua imagem e voz, fazendo-se passar por criança ou adolescente, com o fim de induzir a vítima a se exhibir de forma lasciva ou sexualmente explícita ou a fornecer fotografias ou vídeos sexuais ou sensuais; (BRASIL, 1990, art. 241-D, redação dada pela Lei nº 15.487/2026).

Art. 241-E. Para efeito dos crimes previstos nesta Lei, considera-se material ou conteúdo de violência sexual contra criança ou adolescente qualquer representação,

por qualquer meio, inclusive fotografia, vídeo, imagem digital ou outro registro audiovisual, que envolva criança ou adolescente, real ou fictício, ainda que produzida, manipulada ou gerada mediante o uso de tecnologias digitais, inclusive inteligência artificial, quando:

I - retratar atividade sexual explícita, real ou simulada;

II - conter nudez total ou parcial com finalidade sexual ou libidinosa; ou

III - representar situação, contexto, enquadramento ou pose que evidencie conotação sexual ou libidinosa, ainda que não haja exposição de órgãos genitais ou que esses estejam cobertos. (BRASIL, 1990, art. 241-E, redação dada pela Lei nº 15.487/2026).

Registre-se, ainda, que o § 4º-A do art. 217-A do Código Penal incluído pela Lei nº 15.353/2026, consolidou o caráter absoluto da presunção de vulnerabilidade da vítima, tornando inadmissível sua relativização judicial e estabelecendo que as penas aplicam-se independentemente de eventual consentimento, experiência sexual anterior ou de gravidez resultante de conduta (§ 5º).

Paralelo a isso, a Lei de Crimes Hediondos (nº 8.072/1990), define:

Art. 1º [...]

Parágrafo único. Consideram-se também hediondos, tentados ou consumados:

[...]

VII - os crimes previstos no caput e nos § 1º e 2º do art. 240, no caput e no parágrafo único do art. 241, no caput e nos § 1º e 3º do art. 241-A, no caput do art. 241-B, no caput e nos §§ 1º e 2º do art. 241-D[...]da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). (BRASIL, 1990, redação dada pela Lei nº 15.487, 2026).

Com a consolidação legislativa, as condutas de produção (art. 240), venda (art. 241), compartilhamento (art. 241-A), armazenamento (art. 241-B) e aliciamento (art. 241-D) praticados no ambiente digital integram o rol de crimes hediondos, com os severos efeitos processuais e executórios daí decorrentes.

A análise conjunta desses dispositivos buscou cercar todas as etapas da cadeia criminosa, desde a produção e venda até a simples oferta ou compartilhamento de material ilícito. Essa estrutura rigorosa visa interromper o ciclo de disseminação que instiga a exploração sexual de crianças e adolescentes no cenário atual, de forma a agravar mais a pena como forma de repressão aos agressores.

Essa alteração legislativa reflete a percepção do Estado de que a lesividade desses crimes no ambiente virtual é equiparável às formas mais graves de violência física, dado o potencial de

replicação infinita das imagens e a perpetuação da violação à dignidade sexual da vítima.

Acerca dessa fragilidade desses vulneráveis à frente dos crimes cibernéticos, Guilherme de Souza Nucci (2026, p.23) leciona que “o respeito à dignidade humana conduz a orquestra e a sintonia das liberdades fundamentais, pois estas são os instrumentos essenciais para alicerçar a autoestima do indivíduo [...]”. No contexto da infância e juventude, essa dignidade e autoestima tornam-se ainda mais suscetíveis a violações no ambiente virtual, onde a assimetria entre a maturidade da vítima e a malícia do aliciador é amplificada. Sob esta perspectiva, a proteção da dignidade sexual infantojuvenil na rede transcende a mera repressão de atos físicos, alcançando a integridade psíquica e moral de crianças e adolescentes. Nessa lógica, a tutela da liberdade sexual em formação exige que o ordenamento jurídico atue não apenas após o dano consumado, mas também de forma preventiva em relação à manipulação digital.

É nesse contexto de preservação antecipada que se inserem as dinâmicas da exploração sexual e do *grooming*. O aliciamento digital, tipificado no art. 241-D do ECA, manifesta-se como um processo psicológico progressivo, onde o agressor se utiliza do anonimato e da quebra de barreiras geográficas para conquistar a confiança da vítima, isolá-la de seu círculo e, finalmente, proceder à exploração.

O *grooming*, ou aliciamento online, é uma prática que vem expandindo-se nos dias atuais. Doutrinariamente, não se caracteriza como ato impulsivo, mas como um processo psicodinâmico meticulosamente estruturado para fragilizar as barreiras de proteção da criança ou adolescente. Diferentemente de outros crimes

cibernéticos, esse aliciamento fundamenta-se na manipulação psicológica e na criação de um vínculo de confiança distorcido entre o agente e a vítima. Essa arquitetura de manipulação projeta reflexos nítidos e preocupantes nas estatísticas atuais e desafia os limites do ordenamento jurídico: embora o tipo penal específico do art. 241-D tutele primariamente a pessoa menor de 14 anos, os jovens de 14 a 17 anos permanecem expostos a essa mesma dinâmica de vulnerabilidade, revelando uma importante lacuna dogmática a ser enfrentada pela tutela penal e social. A gravidade do fenômeno deixa de ser uma hipótese teórica para se tornar um dado concreto na esfera social.

A relevância de compreender a mecânica do *grooming* reside no fato de que o aliciamento virtual raramente se esgota em si mesmo. Ele atua, em regra, como meio de execução para condutas de maior gravidade. À medida que as táticas de manipulação psicológica surtem efeito, o agente induz a vítima menor de 14 anos a praticar atos de conotação sexual diante da câmera ou a emitir registros íntimos de si mesma. Nesses cenários, a dinâmica ultrapassa a mera fase tipificada no art. 241-D do ECA, alcançando a efetiva violação da dignidade sexual do vulnerável. Sob essa ótica, o Superior Tribunal de Justiça (STJ) firmou que o entendimento de que a caracterização do crime de estupro de vulnerável (art. 217-A do Código Penal) prescinde de contato físico direto entre agressor e vítima. Para a Corte Superior, a exibição lasciva ou a indução à prática de atos libidinosos por meio virtual é suficiente para consumar o delito, visto que a tutela penal visa resguardar o desenvolvimento mental e integridade moral da criança. Nesse sentido, destaca-se o precedente RHC N° 70.976/MS (Rel. Min. Joel Ilan Paciornik), a sujeição do menor à contemplação lasciva mediante conduta

direcionada é suficiente para afrontar a sua integridade e consumir a violação a dignidade sexual da vítima.

Dessa forma, resta evidenciado que o ordenamento jurídico e a interpretação dos Tribunais Superiores buscam reprimir a manipulação digital em suas diversas fases, coibindo os abalos ao desenvolvimento saudável das crianças e adolescentes.

Conforme Zanatta e Castro apontam:

Apesar das conseqüências, a vítima mantém segredo por medo do que pode acontecer após a revelação. Temem a punição ou medo do adulto ser incapaz de protegê-la da violência de seu agressor, e além disso, sentem que correm o risco de não serem credibilizadas no que dizem, por isso, guardam segredos sobre o abuso. (Zanatta e Castro, 2020, p.1099)

Este silêncio compulsório é o que permite a continuação da violência no ambiente digital. O medo da falta de credibilidade mencionado pelas autoras é, muitas vezes, reforçado pela própria estrutura da rede, onde o agressor se utiliza do anonimato para convencer a criança ou adolescente de que a culpa pelo ocorrido é dela e de que não haverá suporte externo caso haja a denúncia.

Em suma, a transição do aliciamento psicológico para a exploração sexual efetiva encontra no ambiente digital um panorama de extrema vulnerabilidade. Entende-se que a legislação atual é um passo essencial para combater a sensação de impunidade que alimenta o agente desses crimes sexuais. O rigor penal deve ser

compreendido à luz da dificuldade de denúncia por parte da vítima, ou seja, o sistema de justiça deve estar preparado para identificar que o segredo e o medo são ferramentas presentes nesses crimes contra a dignidade sexual. Garantindo assim, que resulte em uma proteção mais real e efetiva nesse meio infantojuvenil.

2.3. Marcos normativos Como Mecanismos Jurídicos de Proteção: ECA, Marco Civil da Internet, LGPD e Estatuto Digital da Criança e do Adolescente

A transição da sociedade para uma era conectada trouxe inúmeros desafios sem precedentes ao ordenamento jurídico brasileiro, exigindo que o Direito se adaptasse para garantir a proteção da dignidade humana no ciberespaço. Para poder compreender como esse sistema jurídico responde aos riscos inerentes à rede, é importante analisar marcos normativos que atuam diariamente como mecanismos de defesa, especialmente no que tange às crianças e adolescentes, sendo estes um dos mais vulneráveis.

No topo desta pirâmide de proteção, a Constituição Federal traz em seu artigo 227 que consagra a doutrina da proteção e o princípio da absoluta prioridade de crianças e adolescentes. Ao impor à família, à sociedade e ao Estado o dever de assegurar a esses vulneráveis os seus direitos fundamentais e os resguardando contra qualquer forma de violência ou exploração. No contexto contemporâneo, esse comando constitucional expande-se para o ciberespaço, exigindo que as garantias de proteção à dignidade humana e à integridade psíquica e sexual sejam rigorosamente observadas, vinculando com os órgãos estatais quanto com a sociedade civil no combate aos ilícitos virtuais.

Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (BRASIL, 1988)

Paralelamente, o ECA também estabelece uma doutrina mais ampla, que serve de bússola para a interpretação de qualquer tecnologia. No contexto digital, ele atua como a base ética que veda qualquer forma de violência ou exploração de crianças e adolescentes. Conforme o ECA elenca:

Art. 18. É dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor. (BRASIL, 1990.)

A referida norma impõe a toda sociedade o dever de zelar pela dignidade de crianças e adolescentes independente de qual espaço ele esteja inserido, o que impõe no ambiente digital, um dever de cuidado que alcança o Estado, a sociedade e os provedores de aplicações, sem que disso decorra, todavia, um dever geral de monitoramento prévio.

Nesse panorama de responsabilidade e mitigação de danos, destaca-se a relevância do artigo 21 do Marco Civil da Internet, Lei nº 12.965/2014. O dispositivo estabelece uma importante exceção à regra geral da necessidade de ordem judicial prévia, permitindo a responsabilização do provedor de aplicações que deixe de remover, após simples notificação da vítima ou de seu representante legal, conteúdos contendo cenas de nudez ou de atos sexuais de caráter privado. Essa previsão consolida, desde a origem do diploma legal, um mecanismo específico de remoção extrajudicial, reforçando a proteção imediata à intimidade e à dignidade no ambiente virtual.

Paralelo a isso, a Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet, estabeleceu os princípios fundamentais para o uso da rede no Brasil. Sua relevância para que haja a proteção desses direitos reside na garantia da privacidade e na preservação de dados pessoais assegurando que o ambiente virtual seja regido pelo respeito à vida privada. Além disso, a norma define mecanismos para a retirada de conteúdos ilícitos, equilibrando o direito à informação com a necessidade de proteção de imagem do usuário. A Lei nº 12.965/2014 traz em sua redação:

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente. (BRASIL, 2014.)

Diante disso, o Marco Civil rege como uma cláusula de integração normativa ao referenciar expressamente o ECA, consolidando o ambiente digital como uma extensão da vida civil sujeita aos mesmos deveres de cuidado para com essas crianças e adolescentes. Ao prever a utilização de ferramentas de controle parental, o legislador não apenas delega aos pais ou responsáveis a vigilância ativa, mas reafirma a doutrina de proteção no ciberespaço, impondo que a liberdade de navegação seja sempre ponderada pelo melhor interesse do menor.

A integração entre o Marco Civil da Internet e do ECA atinge seu ápice de eficácia com o advento da LGPD (Lei Geral de Proteção de Dados). Enquanto o artigo 29 da Lei nº 12.965/2014 assegura o direito ao controle parental sobre o que é utilizado digitalmente, a LGPD, através de seu artigo 14 aponta que:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (BRASIL, 2018.)

Nesse sentido, ao exigir que o tratamento de dados de crianças e adolescentes seja pautado estritamente pelo seu melhor interesse, a LGPD impõe importantes limites à exploração de informações desse público vulnerável. A norma estabelece balizas rigorosas que

buscam mitigar a exposição indevida de hábitos e preferências infantojuvenis. Juntamente, os marcos normativos garantem que a identidade da criança e do adolescente não seja uma mercadoria digital, assegurando que o desenvolvimento da personalidade ocorra em um ambiente resguardado da lei.

Sob esta perspectiva, embora o ordenamento jurídico brasileiro tenha consolidado barreiras preventivas e estruturais, a realidade das redes sociais para o acúmulo de crimes sexuais com crianças e adolescentes passou a ser mais propícia, exigindo uma resposta estatal mais contundente e imediata. Nesse contexto, a Lei nº 15.211/2025 surge como um marco normativo, transcendendo a esfera da recomendação ética para instituir uma política mais supervisora, para conferir máxima efetividade à prevenção integral no ambiente virtual. Esse regramento estabelece obrigações diretas às plataformas digitais, entre as quais a verificação confiável de idade para o acesso a conteúdos restritos, vedando-se a autodeclaração; a vinculação das contas de usuários menores de 16 anos ao perfil de um responsável legal; a adoção de configurações protetivas por padrão e de ferramentas de supervisão parental; e a vedação da publicidade direcionada baseada em perfilamento. No âmbito repressivo e preventivo, fixa o dever de remoção imediata e de comunicação aos órgãos competentes quanto aos conteúdos de abuso e exploração sexual, aliciamento e correlatos. Para assegurar o cumprimento dessas obrigações, a fiscalização resta incumbida à Autoridade Nacional de Proteção de Dados (ANPD), que dispõe do poder de aplicar as sanções administrativas previstas no art. 35 da referida lei, variando desde advertências e multas de até 10% do faturamento do grupo econômico no Brasil, limitadas a R\$ 50 milhões por infração, até a suspensão temporária ou a proibição definitiva das atividades da empresa no país. Trata-se de um

arcabouço rigoroso cujos efeitos práticos e exigibilidade já se impõem ao mercado, visto que a norma situa-se em pleno vigor desde 17 de março de 2026.

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 ofertado ou direcionado a crianças ou a adolescentes no território nacional ou cujos dados sejam coletados no País, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). (BRASIL, 2025).

Portanto, ao estabelecer sanções, o legislador reconhece que a proteção de crianças e adolescentes no ambiente digital exige uma postura que acompanha a velocidade das redes e seu crescimento cada dia mais atual no cenário brasileiro.

Em síntese, enquanto os diplomas de regulação e proteção digital voltam-se à tutela preventiva do ambiente cibernético e à vedação de exploração comercial, o efetivo recrudescimento repressivo no campo penal advém da Lei nº 15.487/2026. A referida norma endureceu significativamente o tratamento punitivo atribuído aos delitos cibernéticos sexuais infantojuvenis, majorando as penas e garantindo maior rigorosidade na repressão. Desse modo, o ordenamento jurídico pátrio consolida uma tutela de dupla face: de um lado, a prevenção administrativa e tecnológica da exposição de fatos e de outro, o rigor penal e processual viabilizado pela Lei nº 15.487/2026 que buscar reprimir a cooptação de crianças e adolescentes.

Conclusivamente, o estudo dos marcos normativos brasileiros revela que a tutela de crianças e adolescentes no espaço virtual se sustenta em diálogo sistêmico entre normas atuando conjuntamente. Enquanto o ECA e o Marco Civil da Internet estabelecem os alicerces éticos e as garantias de navegação, a LGPD atua na raiz tecnológica ao resguardar os dados pessoais. No entanto, é a modernização da Lei nº 15.211/2025 (Lei Felca) e a severidade da Lei nº 15.487/2026 que enfrenta o aparecimento de novos riscos de violência virtual e confere a rigorosidade do sistema, demonstrando o compromisso de assegurar que o progresso tecnológico não ocorra em detrimento da dignidade humana de crianças e adolescentes. Dessa forma, garantindo que o ciberespaço deixe de ser um espaço de vulnerabilidade para se tornar um ambiente de desenvolvimento seguro e juridicamente amparado.

2.4. Desafios à Efetividade da Proteção Jurídica: Anonimato Digital, Jurisdição Transnacional, Responsabilidade das Plataformas e Políticas Públicas de Prevenção

A proteção jurídica de crianças e adolescentes enfrenta grandes dificuldades em razão da própria arquitetura da rede, decorrentes da estrutura e de características próprias da internet. Embora o ordenamento jurídico tenha avançado na criação de novas leis visando à proteção desses menores vulneráveis, a dinâmica da tecnologia ainda impõe muitas dificuldades para a aplicação dessas normas, especialmente quando se trata da responsabilização dos agentes e da prevenção de danos.

Um dos principais obstáculos está relacionado ao anonimato digital. A possibilidade de criação de perfis falsos e sua atuação através desses perfis dificultam a identificação desses autores e

compromete a responsabilização civil e penal. Para fazer frente a esse desafio, o ordenamento jurídico brasileiro desenvolveu importantes instrumentos de investigação probatória: a infiltração virtual de agentes policiais, disciplinada nos arts. 190-A a 190-E do ECA, incluídos pela Lei nº 13.441/2017, e alterados pela Lei nº 15.487/2026. Essas medidas permitem que os órgãos de persecução penal atuem preventivamente e proativamente nos ambientes digitais públicos para a coleta de indícios de autoria e materialidade, mitigando os efeitos do anonimato sem prescindir do devido processo legal. Conforme analisam Chiara Spadaccini de Teffé e Maria Celina Bodin de Moraes (2017, p. 138-141), as redes sociais ampliam os riscos à privacidade e à dignidade dos usuários, ao mesmo tempo em que criam barreiras práticas para a identificação desses usuários responsáveis por eventuais violações.

Art. 226-A. Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se o agente comete crime previsto neste Capítulo mediante utilização de modulador de proxy ou técnica de mascaramento, ocultação, falsificação, alteração ou anonimização de endereço IP ou de qualquer outro identificador digital, por meio de software, programa, ferramenta, navegador ou qualquer outro meio, com o objetivo de impedir ou dificultar sua identificação. (BRASIL, 1990, Art.226-A ,redação dada pela Lei nº 15.487, de 2026)

Paralelamente ao reforço na supervisão das plataformas, o legislador buscou fechar o cerco contra a impunidade digital ao tipificar a utilização de artifícios tecnológicos de ocultação por parte dos infratores. Essa qualificadora visa punir com maior severidade a

conduta deliberada do agente que emprega meios digitais complexos com o objetivo de dificultar sua identificação e fraudar a investigação criminal.

Outro desafio significativo diz respeito à jurisdição transnacional. A internet não se limita a fronteiras geográficas, ela conecta pessoas de todos os lugares do mundo, ou seja, muitas condutas praticadas por esses agentes podem ocorrer em plataformas e servidores localizados em diferentes países. Nesse cenário, destaca-se a adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético, promulgada pelo Decreto nº 11.491/2023, instrumento fundamental para simplificar a obtenção de provas eletrônicas e fortalecer a cooperação jurídica internacional no combate aos crimes cibernéticos.

No que se refere à responsabilidade de plataformas digitais, há uma discussão relevante acerca dos limites de sua atuação e do dever de vigilância diante de conteúdos publicados por terceiros. Nesse cenário, discute-se a necessidade de proatividade das plataformas no controle de conteúdos e na adoção de mecanismos preventivos. Sobre essa questão, ressaltam Chiara Spadaccini de Teffé e Maria Celina Bodin de Moraes:

Afirma-se que a justificativa pela escolha desse regime de responsabilidade reside no fato de que a responsabilidade civil objetiva incentivaria o monitoramento privado e a exclusão de conteúdos potencialmente controvertidos, o que representaria uma indevida restrição à liberdade de expressão. Além disso, o regime objetivo criaria uma imprevisibilidade quanto à responsabilidade do provedor, o que constituiria uma possível barreira para a inovação tecnológica, científica, cultural e social, bem como obrigaria o provedor a realizar um controle prévio de tudo aquilo que fosse postado, o que poderia ser compreendido como uma forma de censura e aumentaria os custos do serviço. Entretanto, é necessário observar que a disposição presente no caput do art. 19 não impede que os provedores possam determinar requisitos para a remoção direta de conteúdo em seus termos de uso e atendam possíveis notificações extrajudiciais enviadas. (Teffé; Moraes, 2017, p. 132)

Diante dessas considerações, verifica-se que o regime de responsabilidade civil adotado pelo Marco Civil da Internet buscava equilibrar a proteção aos direitos da personalidade com a preservação da liberdade de expressão e o incentivo à inovação no ambiente digital. Contudo, essa opção legislativa passou por uma profunda redefinição com a jurisprudência recente do Supremo Tribunal Federal (STF), expressa nos julgamentos do Tema 987 e 533 (RE 1.037.396/SP e RE 1.057.258/MG), concluídos em 26 de junho de 2025. Ao redimensionar o alcance da imunidade prévia dos provedores, a Corte assentou que a proteção jurídica efetiva requer uma postura mais diligente dos provedores, que passam a ter

deveres de cuidado, autorregulação e moderação ativa de conteúdo. Nesse sentido, evidencia-se que a efetividade da proteção jurídica não depende apenas do modelo de responsabilização adotado, mas também da postura ativa dos provedores e da utilização adequada dos mecanismos já existentes, para assim reduzir os danos à privacidade e à dignidade dos usuários no ambiente digital.

Diante disso, o Supremo Tribunal Federal (STF) declarou inconstitucionalidade parcial do art. 19 do Marco Civil da Internet. Com o reconhecimento dessa inconstitucionalidade no dispositivo, a regra geral passou a ser a responsabilização mediante notificação extrajudicial para ilícitos em geral, abrangendo condutas lesivas praticadas contra crianças e adolescentes. Fixou-se um dever de atuar com a remoção imediata e moderação ativa diante de conteúdos ilícitos de gravidade extrema, tais como crimes sexuais contra vulneráveis, pornografia infantil e atrocidades análogas. A exigência rígida de ordem judicial prévia para a caracterização da responsabilidade civil ficou restrita aos ilícitos civis contra honra, hipótese em que se busca resguardar a liberdade de expressão e afastar a moderação privada desarrazoada em disputas de cunho relativo à reputação.

Além disso, as políticas de preservação de dados constituem outro ponto crítico para a efetividade da proteção jurídica. É de suma importância a guarda de registros de acesso e de dados de usuários, que servirão para a identificação de autores ilícitos e também para a produção de provas em processos judiciais. No entanto, diante dessa necessidade deve haver um equilíbrio entre a proteção à privacidade e aos dados pessoais dos usuários.

Nesse contexto, o Marco Civil da Internet (Lei nº 12.965/2014) disciplina expressamente os deveres e prazos de conservação de registros por parte dos provedores:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

[...]

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (BRASIL. 2014)

Dessa forma, a legislação estabelece um marco temporal objetivo para assegurar que a retenção de dados cumpra sua função persecutória sem sujeitar os usuários a uma vigilância permanente ou desproporcional.

Sob essa perspectiva, observa-se que a proteção jurídica no ambiente digital não depende apenas da existência de normas, mas também da capacidade de adaptação do Direito às transformações tecnológicas. Para vencer esses obstáculos exige-se a atuação conjunta do Estado, das plataformas e da sociedade, bem como aprimoramento de instrumentos jurídicos e tecnológicos que

garantam maior efetividade na prevenção e repressão de violação de direitos no ambiente virtual.

3. METODOLOGIA

A pesquisa caracteriza-se como um estudo de natureza qualitativa e exploratória, desenvolvido por meio de procedimento estritamente bibliográfico e documental. O objetivo do percurso metodológico foi analisar a ampliação da vulnerabilidade de crianças e adolescentes no ambiente digital e avaliar a efetividade dos mecanismos jurídicos de proteção e responsabilização previstos no ordenamento jurídico brasileiro.

O universo da pesquisa compreendeu o levantamento da legislação nacional pertinente à matéria, com destaque para o Estatuto da Criança e do Adolescente (ECA), o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), a Lei nº 15.211/2025 (Lei Felca) e a Lei nº 15.487/2026. A fundamentação teórica baseou-se na análise doutrinária acerca da Doutrina da Proteção Integral, da vulnerabilidade infantojuvenil no espaço virtual, dos direitos fundamentais à privacidade e liberdade de expressão e da responsabilidade das plataformas digitais.

A coleta e a seleção de dados deram-se partir da triagem e catalogação de diplomas normativos e referências bibliográficas especializadas em Direito Digital, Direito Penal e Direitos Humanos Infantojuvenis. Os dados e conteúdos coletados foram submetidos à análise dogmático-jurídica e qualitativo-descritiva, correlacionando os preceitos legais vigentes aos desafios práticos impostos pelas transformações tecnológicas, tais como a velocidade de

disseminação de conteúdos ilícitos, o anonimato, a perpetuação das violações e os limites da cooperação institucional.

Por fim, o método adotado reconhece limitações decorrentes de sua abordagem exclusivamente bibliográfica e documental, bem como do reduzido intervalo temporal para a consolidação jurisprudencial das Leis nº 15.211/2025 e nº 15.487/2026, indicando a necessidade de acompanhamento empírico e contínuo da aplicação prática desses diplomas em investigações futuras.

4. CONSIDERAÇÕES FINAIS

O presente artigo teve como finalidade responder ao seu problema central: como o ambiente digital amplia a vulnerabilidade de crianças e adolescentes à prática de crimes contra a dignidade sexual, e quais os desafios para a efetividade dos mecanismos jurídicos de proteção e responsabilização previstos no ordenamento brasileiro? A investigação partiu do pressuposto de que a expansão das tecnologias de informação e comunicação, embora tenha proporcionado relevantes benefícios sociais e educacionais, produziu novas formas de exposição e potencializou riscos à integridade de diversas crianças e adolescentes.

A análise desenvolvida ao longo deste estudo permitiu constatar que a vulnerabilidade de criança e adolescentes na internet decorre, em medida significativa, de sua condição peculiar de pessoas em desenvolvimento, conforme reconhecido pela doutrina de proteção integral. A familiaridade cada vez mais precoce com dispositivos eletrônicos, redes sociais, plataformas de comunicação e jogos on-line não implica necessariamente a capacidade de compreender os riscos decorrentes das interações virtuais. Nesse

contexto, fatores como a imaturidade emocional e cognitiva, a busca por aceitação social, a exposição excessiva de informações pessoais, a interação com desconhecidos, a insuficiência do acompanhamento familiar e a ausência de adequada educação digital podem ampliar a exposição desse público a práticas ilícitas.

No âmbito da criminalidade sexual, verificou-se que a utilização das tecnologias digitais não representa mera alteração do espaço em que a conduta criminosa é praticada, mas modifica substancialmente suas formas de execução, ampliando o alcance e a complexidade das violações. O anonimato, a facilidade de criação de perfis falsos, a ausência de barreiras geográficas e a velocidade de circulação das informações favorecem a aproximação entre agressores e vítimas e dificultam a identificação dos responsáveis, simultaneamente.

A pesquisa também evidenciou que a proteção da dignidade sexual infantojuvenil não pode se restringir à repressão de atos físicos de violência. A produção, o armazenamento, a disponibilização e a disseminação de materiais relacionados ao abuso sexual infantil prolongam a violação da dignidade da vítima, na medida em que o conteúdo pode permanecer acessível e ser continuamente reproduzido digitalmente. Dessa maneira, a tutela jurídica deve considerar não apenas a ocorrência inicial da violência, mas também os mecanismos tecnológicos que permitem sua perpetuação e amplificação.

A pesquisa permitiu identificar que a existência de normas jurídicas não é suficiente para garantir, por si só, uma tutela efetiva. Permanecem desafios relacionados à identificação dos autores, à preservação e obtenção de provas, à rápida disseminação de

conteúdos ilícitos, à atuação de agentes em diferentes países e à necessidade de cooperação entre autoridades nacionais. Esses fatores demonstram a dificuldade de acompanhar juridicamente a velocidade dessas transformações tecnológicas.

Diante disso, o enfrentamento dos crimes sexuais contra crianças e adolescentes no ambiente digital exige uma atuação conjunta de setores da sociedade. A atuação estatal deve estar associada à participação das famílias, instituições de ensino, plataformas digitais e órgãos responsáveis pela proteção infantojuvenil. A educação digital, a orientação adequada, o fortalecimento dos canais de denúncia e a capacitação dos profissionais responsáveis pelo atendimento das vítimas são medidas fundamentais para tornar efetiva a proteção de crianças e adolescentes.

Dessa forma, a hipótese apresentada na pesquisa encontra respaldo na constatação de que o ambiente digital ampliou as possibilidades de exposição de crianças e adolescentes aos crimes sexuais e criou novos obstáculos para sua prevenção e repressão. Embora o ordenamento jurídico brasileiro tenha avançado na origem de mecanismos de proteção, sua efetividade depende da capacidade das instituições de acompanhar as transformações tecnológicas e de aplicar concretamente os instrumentos previstos na legislação.

Conclui-se que a proteção jurídica de crianças e adolescentes no ambiente digital deve constituir um processo permanente de adaptação do Direito às transformações tecnológicas. A doutrina da proteção integral deve ser aplicada também às relações desenvolvidas no espaço virtual, garantindo que a dignidade, a integridade, a privacidade e os demais direitos fundamentais desse público sejam preservados independentemente do ambiente em

que se encontrem. Apesar dos achados, cumpre ressaltar que o presente estudo possui limitações decorrentes de sua natureza estritamente bibliográfica e documental, bem como do escasso interregno temporal para a consolidação jurisprudencial acerca das Leis nº 15.211/2025 e nº 15.487/2026. Diante dessas lacunas e da rápida evolução do tema, indica-se uma agenda de pesquisas futuras voltadas ao acompanhamento das primeiras decisões judiciais fundamentadas pela Lei nº 15.487/2026, bem como ao escrutínio da atuação fiscalizadora da Autoridade Nacional de Proteção de Dados (ANPD) na tutela dos direitos desse público vulnerável.

Por fim, o enfrentamento dos crimes sexuais praticados ou facilitados pelas tecnologias digitais exige a integração entre prevenção, educação, proteção de dados, investigação, responsabilização e cooperação institucional. A existência de normas é indispensável, mas sua efetividade depende de mecanismos concretos e continuamente atualizados, a fim de garantir que crianças e adolescentes possam utilizar de um ambiente digital seguro e apropriado.

REFERÊNCIAS BIBLIOGRÁFICAS

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

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro: Presidência da República, 1940.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília: Presidência da República, 2014.

BRASIL. Lei nº 13.441, de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Brasília, DF: Presidência da República, 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018.

BRASIL. Lei nº 14.811, de 15 de janeiro de 2024. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a política nacional de prevenção e combate à violência escolar e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), e a Lei nº 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos). Brasília, DF: Presidência da República, 2024.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília, DF: Presidência da República, 2025.

BRASIL. Lei nº 15.280, de 5 de dezembro de 2025. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para agravar a pena dos crimes contra a dignidade sexual de pessoa vulnerável; o Código de Processo Penal; a Lei de Execução Penal; a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente); e a Lei nº

13.146, de 6 de julho de 2015 (Estatuto da Pessoa com Deficiência). Brasília, DF: Presidência da República, 2025.

BRASIL. Lei nº 15.353, de 8 de março de 2026. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever a presunção absoluta de vulnerabilidade da vítima do crime de estupro de vulnerável e para estabelecer a aplicação das penas desse crime independentemente da experiência sexual da vítima ou da ocorrência de gravidez resultante do estupro. Brasília, DF: Presidência da República, 2026.

BRASIL. Lei nº 15.487, de 6 de agosto de 2026. Institui medidas de enfrentamento e repressão ao crime de violência sexual contra criança ou adolescente, inclusive no ambiente digital e com uso de inteligência artificial. Brasília, DF: Presidência da República, 2026.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente. Brasília: Presidência da República, 1990.

BRASIL. Lei nº 8.072, de 25 de julho de 1990. Dispõe sobre os crimes hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências. Brasília, DF: Presidência da República, 1990.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 70.976/MS (2016/0121838-5). Relator: Ministro Joel Ilan Paciornik. Quinta Turma. Julgado em 18/08/2016, *DJe* 31 ago. 2016.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.037.396/SP. Tema 987 da Repercussão Geral. Responsabilização civil de provedores de internet por conteúdo ilícito gerado por terceiros. Relator: Min. Dias Toffoli, Julgado em 26 de jun. 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.057.258/MG. Tema 533 da Repercussão Geral. Dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário. Relator: Min. Luiz Fux. Julgado em 26 de jun. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. 1. ed. São Paulo: CGI.br, 2026. *E-book*. Disponível em: <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2025/>.

NUCCI, Guilherme de Souza. Manual de direito penal. 22. ed. Rio de Janeiro: Forense, 2026.

REGO, Teresa Cristina Rebolho. “Crianças não têm maturidade suficiente para enfrentar os desafios do ambiente digital”. Jornal da USP, 2026. Disponível em: <https://jornal.usp.br/radio-usp/criancas-nao-tem-maturidade-suficiente-para-enfrentar-os-desafios-do-ambiente-digital/>. Acesso em: 22 set, 2026.

SAFERNET BRASIL. Relatório anual de denúncias. Disponível em: <https://new.safernet.org.br>. Acesso em: 23 set, 2026.

SAFERNET BRASIL. SaferNet Brasil alerta que 64% das denúncias recebidas em 2025 são de abuso e exploração. Acesso em: <https://new.safernet.org.br/content/safernet-brasil-alerta-que-64-das-denuncias-recebidas-em-2025-sao-de-abuso-e-exploracao>. Acesso em: 25 set, 2026.

SILVA, Rosane Leal da (org). Direitos da criança e do adolescente em tempos de internet: diálogos e reflexões no âmbito do Programa de

Mestrado em Direito da Universidade Federal de Santa Maria. Cachoeirinha: Editora Fi, 2022.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Pensar — Revista de Ciências Jurídicas, Fortaleza, v. 22, n. 1, 2017.

UNICEF Brasil. Crianças e adolescentes em ambiente digital: riscos e oportunidades. Brasília: UNICEF, 2023.

UNICEF; INTERPOL; ECPAT INTERNATIONAL; SAFE ONLINE. **DisruptingHarm in Brazil: enfrentando a violência sexual contra crianças facilitada pela tecnologia.** Brasília: UNICEF, 2026. Acesso em: <https://www.unicef.org/brazil/relatorios/disrupting-harm-brazil-2026> /. Acesso em: 20 jun.2026

ZANATTA, Alice; CASTRO, Amanda. Pesquisa sobre Impactos Psicossociais para o Adulto do Abuso Sexual na Infância. Revista de Psicologia, v.14, n.51, 2020.

¹ Discente do Curso Superior de Direito do Centro Universitário Santo Agostinho – UNIFSA. E-mail: [acesse o artigo original para visualizar o e-mail](#)

² Discente do Curso Superior de Direito do Centro Universitário Santo Agostinho – UNIFSA. E-mail: [acesse o artigo original para visualizar o e-mail](#)

³ Orientador. Mestre em Criminologia pela Universidade Fernando Pessoa e Docente do Curso Superior de Direito do Centro

Universitário Santo Agostinho – UNIFSA, E-mail: [acesse o artigo original para visualizar o e-mail](#)