UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

MARTA VINAGRE DE FREITAS

ARQUITETURA DA NEGLIGÊNCIA: A RESPONSABILIDADE DO ESTADO, DAS PLATAFORMAS DIGITAIS E DA SOCIEDADE FRENTE À VIOLÊNCIA CIBERNÉTICA NA INFÂNCIA

BRASÍLIA
2025

MARTA VINAGRE DE FREITAS

ARQUITETURA DA NEGLIGÊNCIA: A RESPONSABILIDADE DO ESTADO, DAS PLATAFORMAS DIGITAIS E DA SOCIEDADE FRENTE À VIOLÊNCIA CIBERNÉTICA NA INFÂNCIA

Monografia apresentada como requisito parcial para obtenção de título de Bacharela em Direito pela Universidade de Brasília (UnB).
Orientadora: Prof.ª. Dr.ª. Eneida Orbage de Britto Taquary

BRASÍLIA
2025

Ficha catalográfica elaborada automaticamente com os dados fornecidos pela autora

CIP - Catalogação na Publicação

Vinagre de Freitas, Marta.
VF866a / Marta Vinagre de Freitas;

Orientador: Eneida Orbage de Britto Taquary. Brasília, 2025.
122 f.

Trabalho de Conclusão de Curso (Graduação - Direito) Universidade de Brasília, 2025.

1. Direito da Criança e do Adolescente. 2. Direito Digital. 3. Responsabilidade Civil. 4. Proteção de Dados Pessoais. 5. Regulação de Plataformas Digitais. I. Orbage de Britto Taquary, Eneida, orient. II. Título.

MARTA VINAGRE DE FREITAS

ARQUITETURA DA NEGLIGÊNCIA: A RESPONSABILIDADE DO ESTADO, DAS PLATAFORMAS DIGITAIS E DA SOCIEDADE FRENTE À VIOLÊNCIA CIBERNÉTICA NA INFÂNCIA

Monografia apresentada como requisito parcial para obtenção de título de Bacharela em Direito pela Universidade de Brasília (UnB).

Brasília, 4 de dezembro de 2025.

BANCA EXAMINADORA

Eneida Orbage de Britto Taquary – Orientadora
Doutora em Direito
Professora da Faculdade de Direito da UnB

Othon de Azevedo Lopes — Membro da Banca
Doutor em Direito
Professor da Faculdade de Direito da UnB

Caroline Henriques Mota Balduíno Santos – Membro da Banca
Mestre em Direito

Dedico este trabalho à Martinha – a criança que fui, cuja voz tentaram silenciar, mas que hoje grita em cada página escrita. À minha criança interior, que sobreviveu à negligência do Estado e à cegueira da sociedade quando a justiça lhe foi negada. Esta obra é prova de que resistimos. E a todas as crianças vítimas de violência que ainda esperam por socorro: vocês não estão sozinhas. A minha luta agora é a nossa defesa.

AGRADECIMENTOS

Agradeço aos meus pais, Paulo e Maria. Aos autores da minha vida, minha gratidão eterna por me ensinarem, através das cobranças saudáveis, que o único caminho possível era a educação. Em mim, corre a simbiose que me trouxe até aqui: a força e a resistência da mulher nordestina entrelaçadas à disciplina e à resiliência de um homem negro, gaúcho e militar. Sou o fruto dessa mistura e deste sonho. Obrigada pela vida.

Ao meu irmão Marciano e à minha sobrinha Kalitta, pelo amor em ato. A presença de vocês nos cuidados com o nosso pai (e avô) foi o que me permitiu, de certa forma, ter a tranquilidade necessária para continuar na faculdade. O diploma que seguro hoje também pertence ao esforço de vocês.

À Giovanna, minha parceira de vida. Você chegou como na canção de Geraldo Azevedo, trazendo a certeza de um "dia branco" para os meus dias nublados. Obrigada por ser minha rocha inabalável e por dividir os sonhos comigo. "Se você vier, pro que der e vier, comigo...". E esse tanto que sinto? Esse tanto é de amor.

À espiritualidade, aos que me guiam e protegem, e a todos os irmãos da corrente. Em força uníssona, vocês sustentaram meu espírito e me mantiveram em pé. Sem essa proteção, eu não estaria aqui.

Aos amigos de longa data, que testemunharam todas as minhas versões e nunca soltaram a minha mão. A lista é longa, mas o carinho é único: Tauane, Juliana Veras, Suelma, Mariana, Laís, Anna, Domitila, Thiago, Rauena e Evandro. Vocês são a prova de que a lealdade é a forma mais bonita de amor.

À Mayra, pela parceria de uma vida. Você acompanhou todas as minhas metamorfoses acadêmicas — da Engenharia à Ciência Política, até finalmente me encontrar no Direito. Obrigada por ter estado ao meu lado em cada mudança de rota, apoiando e orientando meus passos.

Ao Lucas, meu amigo e irmão da vida, por ser essa presença atenta e sempre disponível. Obrigada pelo cuidado que transcendeu a amizade e alcançou minha família nos momentos em que mais precisamos. Você foi alicerce, amo-te.

Ao Arthur, meu melhor amigo, por ser presença. Obrigada por nunca me negar ajuda e por tornar o fardo mais leve com o seu carinho. Sua amizade é um presente.

À Cris, Ana Maria e Inácio. Vocês foram, sem dúvida alguma, os maiores incentivadores deste trabalho. Obrigada por ouvirem minhas lamentações e, principalmente, por me fazerem olhar para mim mesma como alguém capaz de realizar coisas grandiosas.

Ao meu ambiente de trabalho, um espaço de acolhimento. Aos meus gestores, Leonardo e Cecília, pela compreensão durante as dificuldades da minha caminhada. Ao Dr. Ricardo, pela liderança humana; sua postura reservada, mas profundamente cuidadosa com os seus, transformou o ambiente profissional em um espaço seguro nos momentos em que minha saúde fragilizou.

À Edileusa, pelo cuidado diário. O seu olhar sobre mim nunca foi apenas profissional, mas um zelo quase maternal que me curou em dias difíceis. Você é essencial.

À minha orientadora, Professora Eneida Orbage. Obrigada pela paciência, pela sensibilidade ímpar e, acima de tudo, por acreditar no meu potencial quando eu mesma duvidava. Sua crença de que este trabalho poderia ser grandioso foi o combustível para que ele existisse.

Aos membros da banca. Ao Professor Othon, pelo trabalho desenvolvido em sala de aula, pela compreensão e pela atenção dedicada aos alunos. À Caroline Balduíno, cuja obra foi de extrema importância para o meu pontapé inicial; o esforço do seu trabalho foi a inspiração direta para a escolha deste tema.

Enfim, à Martinha, minha criança interior, por ter sobrevivido para que a Marta pudesse escrever.

E desviando de pés inocentes

Porém mortais que cercam

Com fé no que sei e no que não sei

No que sou e no que serei

Sigo hoje forte, mais do que ontem

Minha resistência é voz

E se for preciso

Eu aprendo a ser feroz

“Minha Prece”, canção de Dandara Manoela.

RESUMO

O presente trabalho investiga a tutela jurídica da infância e adolescência no ciberespaço, partindo da seguinte problemática: diante da sofisticação da violência cibernética e da lógica algorítmica de exploração da atenção, como a persistência de uma negligência compartilhada entre Estado, plataformas digitais e sociedade compromete a efetividade da proteção integral prevista no ordenamento jurídico brasileiro? O estudo diagnostica a existência de uma "Arquitetura da Negligência" forjada pela tríplice falha desses agentes em proteger o sujeito em desenvolvimento. A pesquisa adota o método hipotético-dedutivo, mediante revisão bibliográfica e documental, para demonstrar que o arcabouço normativo brasileiro — composto pelo Marco Civil da Internet, pela Lei Geral de Proteção de Dados (LGPD) e pelo recente "ECA Digital" (Lei nº 15.211/2025) — ainda se revela fragmentado e insuficiente para conter fenômenos como a adultização, o *sharenting* e o *grooming* algorítmico. A análise comparada com o modelo estadunidense (COPPA), em contraste com o *Digital Services Act* (União Europeia) e o *Online Safety Act* (Reino Unido), evidencia a falência da autorregulação e a urgência de superação do modelo reativo de moderação de conteúdo. Como resultado, propõe-se a implementação da Governança Digital de Proteção Integral (GDPI), fundamentada na responsabilidade civil objetiva pelo risco do empreendimento, na inversão do ônus da prova e na imposição de deveres estruturais de *safety by design* e *duty of care*. Conclui-se que a efetivação da prioridade absoluta prevista no artigo 227 da Constituição Federal exige não apenas regulação estatal, mas o fim da passividade social diante da violência virtual, forçando as plataformas a internalizarem os custos sociais de seus modelos de negócio.

Palavras-chave: Direito da Criança e do Adolescente. Responsabilidade Civil. ECA Digital. Arquitetura da Negligência. Governança Digital.

ABSTRACT

This study investigates the legal protection of children and adolescents in cyberspace, addressing the following research problem: given the sophistication of cyber violence and the algorithmic logic of attention exploitation, how does the persistence of shared negligence among the State, digital platforms, and society compromise the effectiveness of integral protection foreseen in the Brazilian legal system? The study diagnoses the existence of an "Architecture of Negligence" forged by the triple failure of these agents to protect the developing subject. The research adopts the hypothetical-deductive method, through bibliographic and documentary review, to demonstrate that the Brazilian normative framework — composed of the Civil Rights Framework for the Internet (Marco Civil), the General Data Protection Law (LGPD), and the recent "Digital ECA" (Law No. 15,211/2025) — remains fragmented and insufficient to contain phenomena such as adultization, sharenting, and algorithmic grooming. The comparative analysis contrasts the United States model (COPPA), marked by the failure of self-regulation, with the Digital Services Act (European Union) and the Online Safety Act (United Kingdom), highlighting the urgency of overcoming reactive content moderation. As a result, the implementation of Integral Protection Digital Governance (GDPI) is proposed, grounded in strict civil liability based on business risk, the reversal of the burden of proof, and the imposition of structural duties of safety by design and duty of care. It is concluded that the effectuation of the absolute priority foreseen in Article 227 of the Federal Constitution demands not only state regulation but the end of social passivity regarding virtual violence, forcing platforms to internalize the social costs of their business models.

Keywords: Child and Adolescent Law. Civil Liability. Digital ECA. Architecture of Negligence. Digital Governance.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Agência Nacional de Proteção de Dados
CCPA	California Consumer Privacy Act
CDA	Communications Decency Act
CF	Constituição Federal
CJF	Conselho da Justiça Federal
COPPA	Children's Online Privacy Protection Act
COVID-19	Coronavirus Disease 2019
CP	Código Penal
CRAS	Centros de Referência de Assistência Social
CSAM	Child Sexual Abuse Material (Material de Abuso e Exploração Sexual Infantojuvenil)
DCAV-RJ	Delegacia da Criança e do Adolescente Vítima do Rio de Janeiro
DSA	Digital Services Act
ECA	Estatuto da Criança e do Adolescente
ESF	Estratégia Saúde da Família
FTC	Federal Trade Commission
GDPI	Governança Digital de Proteção Integral
GDPR	General Data Protection Regulation
IPqHC	Instituto de Psiquiatria do Hospital das Clínicas
IWF	Internet Watch Foundation
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MMFDH	Ministério da Mulher, da Família e dos Direitos Humanos
OFCOM	Office of Communications (Órgão regulador de comunicações do Reino Unido)
OSA	Online Safety Act
TCU	Tribunal de Contas da União
TIC	Tecnologias da Informação e Comunicação (referente à pesquisa TIC Kids Online)
VLOPs	Very Large Online Platforms (Plataformas Online de Grande Porte)

LISTA DE SÍMBOLOS

 Símbolo do ciclone usado em redes sociais

SUMÁRIO

INTRODUÇÃO

A contemporaneidade digital, marcada pela onipresença de dispositivos conectados e pela centralidade das plataformas digitais na estruturação das relações sociais, reconfigurou não apenas os modos de comunicação, mas também as dinâmicas de violência, perpetrando vulnerabilidades específicas que incidem com particular gravidade sobre o público infantojuvenil.

Em 2024, apenas no Brasil, foram registradas pela Central Nacional de Denúncias de Crimes Cibernéticos da SaferNet Brasil 53 mil novas denúncias de imagens de abuso e exploração sexual de crianças e adolescentes[1], evidenciando a escala industrial de uma violação sistêmica que opera sob lógica de rentabilização algorítmica. Esse cenário não se configura como externalidade negativa do ambiente digital, mas como consequência estrutural de uma arquitetura programada para maximizar engajamento a qualquer custo, capturando dados sensíveis e expondo menores de idade a conteúdos nocivos sem implementação de salvaguardas adequadas.

A pesquisa TIC Kids Online Brasil 2024 demonstrou que 93% da população entre 9 e 17 anos — cerca de 24,5 milhões de pessoas — é usuária regular da internet[2], sendo que o crescimento da conectividade infantil não foi acompanhado por políticas públicas protetivas proporcionais. Mais alarmante ainda: segundo estudo da ChildFund Brasil divulgado em 2025, 54% dos adolescentes brasileiros — equivalente a mais de 9 milhões de pessoas — relataram ter sofrido algum tipo de violência sexual online[3].

---

[1] SOCIEDADE BRASILEIRA DE PEDIATRIA. **SBP cobra do Congresso Nacional 'tolerância zero' a crimes virtuais contra crianças e adolescentes e exige aprovação de PL que aumenta rigor da lei**. Rio de Janeiro, 14 mar. 2024. Disponível em:https://www.sbp.com.br/imprensa/detalhe/news/sbp-cobra-do-congresso-nacional-tolerancia-zero-a-crimes-virtuais-contra-criancas-e-adolescentes-e-e/. Acesso em: 14 out. 2025.

[2] CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **TIC Kids Online Brasil 2024**: pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2025. p. 59

[3] CHILDFUND BRASIL. Mais da metade dos adolescentes brasileiros já sofreu violência sexual on-line. ChildFund Brasil, 2025. Disponível em: https://childfundbrasil.org.br/mais-da-metade-dos-adolescentes-brasileiros-ja-sofreu-violencia-sexual-on-line/ . Acesso em: 12 de out. 2025.

A violência digital dirigida a crianças é um fenômeno complexo, cuja compreensão exige múltiplas perspectivas, evitando explicações simplistas que atribuem a responsabilidade apenas à família ou a indivíduos específicos. Trata-se de negligência arquitetônica e sistêmica, estruturada em três níveis de omissão corresponsável: **(i) a negligência estatal**, manifestada pela ausência de política pública específica para prevenção e combate aos crimes sexuais contra crianças e adolescentes na internet, conforme constatado pelo Tribunal de Contas da União (TCU) no Acórdão 2515/2025, que identificou lacunas normativas, deficiências operacionais e desarticulação entre órgãos de segurança[4]; **(ii) a negligência corporativa das plataformas digitais**, que operam sob modelo de negócio baseado na captura de atenção infantojuvenil e na monetização de dados pessoais sensíveis, privilegiando lucro em detrimento da proteção integral[5]; e **(iii) a negligência social**, expressa tanto pela naturalização da sexualização precoce quanto pelo abandono digital parental, caracterizado pela ausência de mediação qualificada do uso de tecnologias por crianças e adolescentes.[6]

Em síntese, a presente pesquisa sustenta que essa tríade, Estado, plataformas e sociedade, configura uma **arquitetura da negligência**: sistema multidimensional no qual a omissão de cada agente potencializa e retroalimenta as demais omissões, cristalizando um ambiente estruturalmente hostil aos direitos fundamentais de crianças e adolescentes.

O conceito de "arquitetura" é aqui empregado em duplo sentido: **(i) no sentido técnico-informacional**, referindo-se ao *design* intencional das plataformas digitais[7]; e **(ii) no sentido sociojurídico**, designando a estrutura normativa, institucional e

[4] CHILDFUND BRASIL, *op. cit.*, p. 8.
[5] FERREIRA, Letícia Sthefane Santos. **Prática de crimes cibernéticos contra a criança e o adolescente:** mecanismos investigativos e combativos. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Lavras, Lavras, 2025, p. 9.
[6] MARTIN, Júlia Saes. **Abandono digital e dever de vigilância parental sob a ótica do princípio da proteção integral à criança**. Monografia (Bacharelado em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2024, p. 11.
[7] KOFFERMANN, Marcia; AGUADED, Ignacio. **A influência das redes sociais sobre os adolescentes**: ciberconsumo e educação crítica. Lumina, Juiz de Fora, v. 17, n. 1, p. 127-128, 2023

cultural que possibilita a perpetuação sistemática de violências contra menores de idade, mediante a produção deliberada de invisibilidades e indiferenças.

Nesse contexto, a violência cibernética contra a infância assume múltiplas manifestações: **(i) pornografia infantil e disseminação de material de abuso e exploração sexual infantojuvenil** (*Child Sexual Abuse Material — CSAM*), que circula em plataformas abertas, em redes sociais *mainstream* e na *dark web*;[8] **(ii) aliciamento sexual online** (*grooming*), mediante o qual adultos manipulam psicologicamente crianças e adolescentes para obtenção de conteúdo sexual ou encontros presenciais[9]; **(iii) extorsão sexual** (*sextortion*), caracterizada pela chantagem com divulgação de imagens íntimas caso a vítima não produza mais conteúdo ou não efetue pagamentos;[10] **(iv) cyberbullying**, incluindo ofensas sistemáticas, exposição vexatória e difamação em ambientes virtuais[11]; **(v) adultização precoce**, mediante exposição deliberada de crianças e adolescentes a conteúdos sexualizados, incentivada por algoritmos que premiam visualizações e engajamento[12]; e **(vi) produção de conteúdo sexual mediante uso de inteligência artificial generativa** *(deepfakes)*, que permite a criação de imagens e vídeos sintéticos explorando a imagem de menores de idade sem qualquer tipificação penal específica no ordenamento jurídico brasileiro[13].

O objetivo geral deste trabalho consiste em demonstrar que a violência cibernética contra a infância não resulta de falhas pontuais ou de condutas isoladas, mas de uma arquitetura estrutural de negligências interdependentes, cujo enfrentamento demanda a superação de abordagens fragmentadas e a construção de sistema integrado de proteção que articule regulação estatal efetiva,

---

[8] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025 – Plenário**. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 7.
[9] *Ibid*., p. 7.
[10] *Ibid*., pp. 7 – 8.
[11]PORFÍRIO, Francisco. **Cyberbullying**. Brasil Escola, [s.d.]. Disponível em: https://brasilescola.uol.com.br/sociologia/cyberbullying.htm . Acesso em: 12 nov. 2025.
[12] SAFERNET BRASIL. **Nota Técnica nº 02/2025**: em 2025, cerca de 64% das denúncias recebidas pela SaferNet Brasil envolveram conteúdos digitais de abuso e exploração sexual de criança e adolescentes. Salvador: SaferNet Brasil, 19 ago. 2025, p. 3-4.
[13] *Ibid*., pp. 11-13

responsabilização corporativa das plataformas digitais e fortalecimento das capacidades sociais de mediação e resistência.

A pesquisa adota uma abordagem qualitativa, crítico-normativa e interdisciplinar para enfrentar esse cenário. Seus objetivos específicos consistem em: **(i)** mapear as lacunas normativas e institucionais na proteção infantojuvenil; **(ii)** examinar os modelos de negócio das plataformas que potencializam riscos à integridade de menores; **(iii)** problematizar juridicamente o conceito de abandono digital parental; e **(iv)** avaliar a eficácia dos instrumentos vigentes, notadamente o ECA, o Marco Civil, a LGPD e a recente Lei nº 15.211/2025 (ECA Digital). Em caráter propositivo, busca-se formular diretrizes para uma cultura protetiva digital, alicerçada no direito comparado (COPPA, GDPR e Online Safety Act) e no dever de cuidado sistêmico.

Diante desse contexto, o presente trabalho busca responder à seguinte questão de pesquisa:

> Como a persistência de uma **arquitetura de negligência compartilhada entre Estado, plataformas digitais e sociedade** compromete a efetividade da proteção integral prevista no art. 227 da CF/88, no ECA, na LGPD e no novo ECA Digital (Lei 15.211/2025), **especialmente diante do aumento de crimes cibernéticos, da curadoria algorítmica nociva e do abandono digital infantil?**

A relevância do tema justifica-se pela convergência entre **urgência empírica** (milhões de crianças e adolescentes brasileiros expostos diariamente a riscos com consequências traumáticas duradouras) e **complexidade teórica**, que demanda abordagem multidisciplinar. Ademais, o recorte temporal abrange o período de 2015 a 2025, em que se intensificou o uso infantil de redes sociais e emergiram novas formas de violência digital.

O presente trabalho estrutura-se em quatro capítulos: o **1º** traça o diagnóstico fenomenológico da violência digital, abordando a hipervulnerabilidade e a tipologia dos riscos na infância conectada; o **2º** analisa o arcabouço normativo de proteção,

examinando a dogmática constitucional, civil e a regulação vigente até o recente ECA Digital; o **3º** desenvolve a tese da “Arquitetura da Negligência”, confrontando a norma com a realidade para expor as omissões sistêmicas do Estado, das plataformas e da sociedade; e por fim, o **4º** apresenta a proposta de Governança Protetiva (GDPI), sugerindo diretrizes de *safety by design* e responsabilização estrutural inspiradas no direito comparado.

Ao longo dos capítulos, busca-se demonstrar que a proteção integral da infância no ambiente digital somente será efetiva quando as respostas legais, institucionais e sociais forem articuladas de forma sistêmica, deslocando o foco do combate pontual ao conteúdo para a regulação estrutural dos mecanismos que geram, amplificam e lucram com a vulnerabilidade infantil.

CAPÍTULO 1 A INFÂNCIA NA ERA DIGITAL: FENOMENOLOGIA DA VIOLÊNCIA E VULNERABILIDADE

A maneira como entendemos a infância hoje exige reconhecer que o desenvolvimento das crianças ocorre em múltiplos ambientes, entre eles o digital, que deixou de ser complementar para assumir papel decisivo na formação social e identitária. Neste capítulo, examina-se como a crescente presença de crianças e adolescentes nas redes e plataformas online transformou o modo como se manifestam situações de vulnerabilidade, introduzindo desafios que ultrapassam os modelos tradicionais de proteção.

A dinâmica da violência no ambiente digital caracteriza-se por um funcionamento contínuo e difuso, sustentado por mecanismos algorítmicos que não apenas expõem os jovens a conteúdos inadequados, mas também tendem a amplificá-los.

Nesse contexto, discute-se como a hiperconexão frequentemente apresentada como oportunidade de acesso e inclusão, pode, ao mesmo tempo, abrir espaço para práticas abusivas e violações persistentes que se aproveitam do processo ainda em maturação das capacidades emocionais e cognitivas das crianças.

1.1 O contexto da infância hiperconectada e a "plataformização" da vida

Os dados apresentados na introdução revelam que cerca de três em cada dez crianças brasileiras já enfrentaram situações de risco online, com mais da metade exposta a alguma forma de violência sexual digital, evidenciam não apenas magnitude quantitativa, mas também natureza estrutural do fenômeno: trata-se de violência indissociável da reorganização contemporânea da socialidade infantojuvenil mediante processos de "plataformização" da vida[14].

[14] VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society:** public values in a connective world. Oxford: Oxford University Press, 2018, p. 4. Os autores definem "plataformização" como processo mediante o qual "*plataformas digitais penetram profundamente nas esferas da vida social, reorganizando práticas culturais, econômicas e políticas em torno de suas infraestruturas técnicas e modelos de negócio baseados em dados*".

Crianças e adolescentes não utilizam a internet meramente como ferramenta, eles habitam ambientes digitais arquitetados por corporações cujo modelo de negócio fundamenta-se na captura, retenção e monetização de atenção, sem implementação proporcional de salvaguardas protetivas.

Esse cenário agravou-se exponencialmente no contexto da pandemia de COVID-19, quando o isolamento social forçado e o deslocamento compulsório de atividades educativas, recreativas e sociais para o ambiente digital criaram aquilo que Lima e Viana denominam "terreno fértil para o incremento dessas violações"[15]. A análise dos autores demonstra que o período pandêmico não apenas ampliou o tempo de tela e a exposição digital de menores, mas também reduziu drasticamente a supervisão parental qualificada, aumentando a vulnerabilidade a crimes cibernéticos[16].

Segundo dados da SaferNet Brasil, a Central Nacional de Denúncias de Crimes Cibernéticos recebeu, somente em 2025, denúncias nas quais 64% dos conteúdos relacionavam-se ao abuso e à exploração sexual de crianças e adolescentes — quase sete em cada dez denúncias recebidas pela organização dizem respeito a essa modalidade específica de violência[17].

A magnitude desses dados não pode ser compreendida apenas mediante análise quantitativa; impõe-se reconhecer que a violência digital contra a infância opera sob lógica sistêmica, inscrita na própria arquitetura das plataformas digitais. Koffermann e Aguaded demonstram que as tecnologias digitais contemporâneas "são pensadas e desenhadas para impulsionar e fortalecer o consumo, o que muitas vezes ocorre de forma invisível e incompreensível para o usuário"[18]. Esse design intencional é baseado em captura de atenção, exploração de vieses cognitivos e maximização de engajamento no qual se transformam crianças e adolescentes em mercadorias cujos

[15] LIMA, Jamile Moreira; VIANA, Johnnatan Reges. **Crimes cibernéticos:** aumento de crimes virtuais contra crianças e adolescentes pós-pandemia no Brasil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, maio 2024, p. 2051,
[16] *Ibid*., p. 2051-2052.
[17] SAFERNET BRASIL. **Nota Técnica nº 02/2025**: aumento de denúncias e uso de inteligência artificial na produção de conteúdo de abuso sexual infantil. Salvador: SaferNet Brasil, 19 ago. 2025, p. 2.
[18] KOFFERMANN, Marcia; AGUADED, Ignacio. **A influência das redes sociais sobre os adolescentes**: ciberconsumo e educação crítica. **Lumina**, Juiz de Fora, v. 17, n. 1, p. 127, 2023

dados pessoais, padrões comportamentais e vulnerabilidades psicológicas são monetizados sem consentimento informado ou proteção adequada[19].

A "plataformização" da vida infantojuvenil representa reconfiguração estrutural das dinâmicas de socialização, aprendizagem e construção identitária, operada por corporações cujo modelo de negócio depende da captura e monetização de dados. Se a rua e a praça representavam, em contextos históricos anteriores, os principais espaços de convívio e experimentação social para crianças e adolescentes, as plataformas digitais assumem hoje essa função com a diferença fundamental de que não são espaços neutros ou desregulamentados, mas ambientes privados, opacos e geridos por corporações cujo modelo de negócio depende da extração sistemática de dados e da indução de comportamentos compulsivos[20].

A Sociedade Brasileira de Pediatria recomenda que crianças menores de 2 anos não sejam expostas a telas e que, entre 2 e 5 anos, o tempo de tela não ultrapasse uma hora diária[21]. Contudo, a realidade brasileira distancia-se drasticamente dessas diretrizes. Pesquisa realizada pela Fundação Maria Cecilia Souto Vidigal em parceria com o Datafolha revelou que crianças de 0 a 2 anos ficam em média duas horas por dia em frente a telas, o dobro do limite máximo recomendado para a faixa etária seguinte e infinitamente superior ao ideal de exposição zero[22]. O estudo evidenciou ainda que 78% das crianças de 0 a 3 anos e 94% das de 4 a 6 anos estão expostas diariamente a dispositivos digitais, configurando padrão de hiperconectividade precoce sem paralelo histórico.

Essa temporalidade digital não se distribui uniformemente na população: as assimetrias socioeconômicas que estruturam o acesso a recursos materiais, culturais e educacionais reproduzem-se e aprofundam-se no ambiente digital. A pesquisa TIC

---

[19] *Ibid*., p. 127-128.
[20] SANTOS, Caroline Henriques Mota Balduíno. **A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021, p. 32.
[21] BRASIL. Ministério dos Direitos Humanos e da Cidadania; Ministério da Saúde. **Guia sobre usos de dispositivos digitais por crianças e adolescentes**. Brasília: MDH/MS, 2025, p. 21.
[22] FUNDAÇÃO MARIA CECILIA SOUTO VIDIGAL; DATAFOLHA. **Panorama da Primeira Infância**: o que o Brasil sabe, vive e pensa sobre os primeiros seis anos de vida. São Paulo: FMCSV, 2025. Disponível em: https://fundacaomariacecilia.org.br/noticias/primeira-infancia-brincar-livre-exposicao-a-telas-alta/ . Acesso em: 2 nov. 2025.

Kids Online 2024 evidencia que o uso exclusivo de telefone celular para acesso à internet predomina entre crianças e adolescentes das classes D e E (32%), enquanto o acesso mediante múltiplos dispositivos, incluindo computadores e tablets, concentra-se nas classes A e B[23].

Nota-se que a diferença não é meramente técnica: o uso exclusivo de telefone celular limita as possibilidades de navegação qualificada, reduz a capacidade de identificação de conteúdo nocivos e dificulta a implementação de ferramentas de controle parental, ampliando a vulnerabilidade de crianças e adolescentes em situação de pobreza[24].

1.2 Tipologia das violências digitais: do *cyberbullying* à exploração algorítmica

A violência digital contra a infância constitui fenômeno multifacetado que demanda análise tipológica rigorosa. Para fins analíticos, propõe-se distinção entre duas modalidades fundamentais: **(i)** violências interpessoais mediadas por plataformas, perpetradas por indivíduos mediante interações diretas entre usuários, abrangendo *cyberbullying, grooming, sextortion* e divulgação não consensual de imagens íntimas; e **(ii)** violências estruturais ou algorítmicas, produzidas pela própria arquitetura das plataformas digitais mediante modelo de negócios baseado na economia da atenção e na maximização do engajamento, frequentemente em conflito com a segurança infantojuvenil[25].

Embora analiticamente distintas quanto aos agentes perpetradores, essas modalidades não operam de forma isolada. Conforme diagnosticado pelo Tribunal de Contas da União, "as plataformas digitais não são neutras — seu modelo de negócios, baseado na economia da atenção e na maximização do engajamento, muitas vezes

[23] CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **TIC Kids Online Brasil 2024:** pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Cetic.br, 2024, p. 6

[24] SANTOS, Caroline Henriques Mota Balduíno**. A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021, p. 172

[25] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 26.

conflita com a segurança infantojuvenil"[26], configurando estrutura que potencializa e facilita a perpetração de violências interpessoais. A ausência de moderação proativa e de mecanismos efetivos de detecção e remoção de conteúdos ilícitos transforma as plataformas em ambientes facilitadores da violência, não meramente em espaços neutros onde ela ocasionalmente ocorre[27].

Essa relação fundamenta-se em assimetrias de poder estruturantes: enquanto crianças e adolescentes navegam em ambientes sobre os quais não possuem compreensão plena, as plataformas detêm "conhecimento necessário para operar a tecnologia", conferindo-lhes "o poder para operá-la"[28].

1.2.1 Estupro virtual e constrangimento sexual mediante tecnologias

O estupro virtual constitui modalidade de crime sexual que, embora não envolva contato físico direto entre agressor e vítima, produz danos psicológicos equivalentes e, em muitos casos, superiores aos decorrentes de violência sexual presencial.

Lima, Fernandes e Pedrosa definem o estupro virtual como aquele no qual "o criminoso constranja sua vítima através de ameaça ou violência psicológica a praticar ato libidinoso sem sua vontade ou consentimento, sem que haja toque físico entre agressor e ofendido"[29]. A ausência de contato físico não descaracteriza a gravidade da conduta conforme sustentam os autores, "a doutrina penal contemporânea reconhece que a violação sexual mediante coação psicológica produz trauma

[26] *Ibid.*, p. 26.
[27] *Ibid.*, p. 44.
[28] SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016, p. 77. *apud* SANTOS, Caroline Henriques Mota Balduíno. **A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021, p. 31.
[29] LIMA, Francisco Zamourano Silva de; FERNANDES, Maria Allice Dantas; PEDROSA, Eduarda Shirley Fernandes de Oliveira Vale. **A prática dos crimes cibernéticos como violação dos direitos da criança e do adolescente**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Potiguar, Natal, 2023, p. 11.

equiparável ao decorrente de agressão física, especialmente quando a vítima é criança ou adolescente"[30].

A tipificação do estupro virtual no ordenamento jurídico brasileiro resultou de construção jurisprudencial progressiva, cristalizada no paradigmático caso julgado pelo Tribunal de Justiça do Rio Grande do Sul em 2017[31]. Nesse precedente, o acórdão reconheceu que a internet não é um universo sem lei e sustentou que "o assédio praticado pelo réu, por meio de sites de relacionamento e chat na internet, a fim de que a vítima se despisse e praticasse atos libidinosos, inclusive pedindo expressamente que o menor ligasse a câmera e tirasse a roupa, tratou-se de um estupro virtual."[32].

A decisão foi pioneira ao reconhecer que o ambiente digital não constitui espaço de exceção normativa, e que condutas praticadas mediante tecnologias digitais podem configurar crimes sexuais mesmo na ausência de proximidade física entre agressor e vítima.

1.2.2 Adultização algorítmica e a sexualização programada da infância

A adultização algorítmica configura fenômeno contemporâneo no qual plataformas digitais, mediante sistemas automatizados de recomendação de conteúdo, expõem crianças e adolescentes a representações sexualizadas de seus próprios corpos, induzindo-os a produzir e compartilhar conteúdos que mimetizam padrões estéticos e comportamentais adultos[33].

Lima demonstra que "a exposição precoce a conteúdos e comportamentos adultos, impulsionada por algoritmos que privilegiam a performance digital e a visibilidade, aumenta significativamente os riscos de exploração e violência

---

[30] *Ibid*. 11.
[31] AGÊNCIA BRASIL. Justiça do RS faz condenação inédita por "estupro virtual de vulnerável". Exame, São Paulo, 20 dez. 2018. Disponível em: https://exame.com/brasil/justica-do-rs-faz-condenacao-inedita-por-estupro-virtual-de-vulneravel/ . Acesso em: 25 nov. 2025.
[32] LIMA; FERNANDES; PEDROSA, *op. cit.*, p. 13.
[33] LIMA, Reginaldo Soares de Sousa. **Vulnerabilidade digital e riscos da adultização de menores em plataformas de mídia social**. Periódicos Brasil: Pesquisa Científica, [S.l.], v. 4, n. 2, p. 321-331, 2025.

simbólica"[34]. Essa dinâmica não resulta de escolhas individuais ou de "uso inadequado" das plataformas por parte de menores, mas de arquitetura intencional programada para maximizar tempo de tela mediante indução de comportamentos que geram alto engajamento, incluindo, especialmente, conteúdos sexualizados.

O caso emblemático denunciado pelo youtuber Felca (Felipe Bressanim), amplamente divulgado pela mídia brasileira em agosto de 2025, ilustra com clareza as dinâmicas predatórias da adultização algorítmica. Em vídeo viral com mais de 26 milhões de visualizações, Felca denunciou a exploração sistemática de menores pelo influenciador Hytalo Santos, que reunia crianças e adolescentes em sua residência e as expunha em vídeos sexualizados nas plataformas TikTok e Instagram[35]. Entre as vítimas está Kamylinha, que foi morar com o influenciador aos 12 anos, aparecia em vídeos dançando de forma sensualizada com pouca roupa, foi emancipada aos 16 anos e realizou cirurgia de implante de silicone aos 17 anos[36].

Conforme documentado pela SaferNet Brasil, "o vídeo sobre 'adultização infantil' envolvendo a criança gerou pico de denúncias à Central Nacional de Denúncias, evidenciando que o conteúdo expôs a menor a situação de exploração sexual comercial mediante monetização de visualizações"[37].

No vídeo do Felca, ele traz uma expressão que sintetiza a violência algorítmica: "ela foi ensinada a ser um produto para um público", ou seja, crianças transformadas em mercadorias cujo valor de troca reside na capacidade de gerar visualizações, likes e engajamento, independentemente dos danos psicológicos, morais e sociais produzidos. A adultização algorítmica não constitui, portanto, mero uso inadequado das plataformas por parte de crianças ou negligência parental isolada; configura estratégia deliberada de monetização da infância, na qual os algoritmos premiam e

---

[34] *Ibid*., p. 321.

[35] FELCA. **Adultização**. [S.l.]: YouTube, 6 ago. 2025. 1 vídeo. Disponível em: https://www.youtube.com/watch?v=FpsCzFGL1LE . Acesso em: 12 set. 2025.

[36] G1. **Pais de crianças e adolescentes que participam de vídeos de Hytalo Santos também são investigados na Paraíba**. G1 Paraíba, João Pessoa, 11 ago. 2025. Disponível em: https://g1.globo.com/pb/paraiba/noticia/2025/08/11/pais-de-criancas-e-adolescentes-que-participam-de-videos-de-hytalo-santos-tambem-sao-investigados-na-paraiba.ghtml . Acesso em: 25 out. 2025.

[37] SAFERNET BRASIL. **Nota Técnica nº 02/2025**: aumento de denúncias e uso de inteligência artificial na produção de conteúdo de abuso sexual infantil. Salvador: SaferNet Brasil, 19 ago. 2025, pp. 3-4

incentivam performances sexualizadas de menores mediante aumento de visibilidade e alcance[38].

O fenômeno não se restringe a casos isolados. Lima, Fernandes e Pedrosa demonstram que “na doutrina, entende-se o estupro virtual como aquele onde o criminoso constranja sua vítima através de ameaça a praticar ato libertino sem sua vontade/consentimento", reconhecendo que plataformas digitais "possuem inúmeros conteúdos de menores dançando de forma sensual", abrindo margem para crimes contra a dignidade sexual infantojuvenil[39].

Monteiro *et al*. argumentam que "a naturalização da sexualização precoce nas redes sociais contribui para uma cultura que normaliza a exposição do corpo infantil, tornando crianças e adolescentes vulneráveis a predadores sexuais e a práticas de exploração comercial"[40].

A omissão regulatória das plataformas digitais não é acidental. Frazão demonstra que, no caso do YouTube, a idade "depende de mera autodeclaração", sendo que "a ajuda do Google ainda estimula o usuário-criança a não fornecer sua idade verdadeira", configurando "quase um estímulo para que as crianças não revelem sua verdadeira idade[41]". A experiência internacional reforça essa constatação: nos Estados Unidos, "o COPPA não exige que os operadores investiguem a idade de seus usuários, o que abre a possibilidade para que as crianças mintam sobre a questão"[42].

---

[38] NEXO JORNAL. **Como é a violência sexual infantil nas redes sociais:** o caso Felca e a adultização nas plataformas digitais. Podcast Nexo Políticas Públicas, 20 ago. 2025. Disponível em: https://www.nexojornal.com.br/podcast/2025/08/20/adultizacao-nas-redes-violencia-sexual-online-adolescentes-brasil . Acesso em: 11 nov. 2025.

[39] LIMA, Francisco Zamourano Silva de; FERNANDES, Maria Allice Dantas; PEDROSA, Eduarda Shirley Fernandes de Oliveira Vale. **A prática dos crimes cibernéticos como violação dos direitos da criança e do adolescente**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Potiguar, Natal, 2023, pp. 11-12.

[40] MONTEIRO, Jarlene Aparecida Bandoli *et al*. **Fatores, espaços e autores da violência sexual contra crianças e adolescentes na sociedade brasileira**. Revista Caderno Pedagógico, v. 22, n. 9, p. 01-29, 2025, p. 9

[41] FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes**: parecer. São Paulo: Instituto Alana, 2020, p. 40.

[42] *Ibid*., p. 42 – 43.

Essa crítica aplica-se integralmente ao contexto brasileiro. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece, em seu artigo 14, que o tratamento de dados pessoais de crianças deve realizar-se mediante consentimento específico de ao menos um dos pais ou responsável legal, mas não especifica mecanismos técnicos de verificação, relegando às plataformas a definição de procedimentos que, na prática, resumem-se à ineficaz autodeclaração[43].

1.2.3 *Grooming*, criação de perfis falsos e aliciamento sexual online

O *grooming* designa o processo de aliciamento sexual de crianças e adolescentes mediante construção gradual de relação de confiança. Cavalcante et al. demonstram que:

> o predador sexual tem extrema facilidade de entrar em contato com vítimas potenciais **mediante a criação de perfis falsos nas redes sociais e a adoção de uma linguagem de fácil compreensão** que simula proximidade etária e afetiva (...) [44]

A arquitetura das plataformas facilita essas práticas ao permitir criação irrestrita de perfis sem verificação de identidade ou autenticidade das informações fornecidas.

O processo opera mediante etapas sequenciais: identificação da vítima em perfis públicos; aproximação inicial simulando perfil de mesma faixa etária; construção de vínculo afetivo mediante conversas regulares; normalização de temas sexuais; solicitação de imagens íntimas; e, finalmente, ameaça e extorsão[45].

Assim, esse processo, que pode durar semanas ou meses, explora sistematicamente a vulnerabilidade psicológica de crianças e adolescentes, que não

[43] BOTELHO, Marcos César. **A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes**. Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE), Bebedouro, v. 8, n. 2, p. 197-230, 2020, p. 215.
[44] CAVALCANTE, Laylana Araújo *et al*. Psicologia forense aplicada à perícia de crimes sexuais contra crianças em ambiente digital. **Research, Society and Development**, v. 9, n. 10, e7129109181, 2020, p. 8.
[45] LOUREIRO, Wilson *et al*. **Capturados na Rede:** um documentário para repensar os crimes sexuais online contra menores de idade no Brasil. **Retos XXI**, v. 9, p. 1-21, 2025, p. 7.

dispõem de maturidade cognitiva e emocional para identificar a manipulação ou resistir à coação.

1.2.4 *Sextortion, revenge porn* e disseminação não consensual de imagens

A *sextortion* configura modalidade específica de extorsão na qual o agressor obtém imagens íntimas da vítima e, mediante ameaça de divulgação pública, extorque dinheiro, favores sexuais ou produção de conteúdos adicionais. Soares e Morais caracterizam a prática como "situações em que o usuário que compartilha imagens sensuais é ameaçado e coagido com intimidações de que esse conteúdo será disponibilizado publicamente caso não atenda às exigências do criminoso"[46].

A gravidade da *sextortion* reside na perpetuação do ciclo de vitimização: uma vez obtidas as primeiras imagens, o agressor detém material que lhe permite coação contínua e progressiva. Cavalcante et al. demonstram que "as sequelas psicológicas no desenvolvimento da personalidade da criança são profundas e, muitas vezes, irreversíveis"[47], agravadas pela impossibilidade de apagamento definitivo do registro digital. Casos documentados pela Children's Crisis Center da República Tcheca evidenciam que adolescentes chantageadas e ameaçadas de exposição de intimidades, diante da pressão psicológica extrema, buscam como "única saída" o suicídio[48].

O *revenge porn*, por sua vez, caracteriza-se pela divulgação não consensual de imagens íntimas com objetivo de expor, humilhar ou prejudicar a vítima, frequentemente em contexto de término de relacionamento. Lima e Viana demonstram que, em muitos casos, a prática não visa "vingança" pessoal meramente emocional,

---

[46] SOARES, Rebeca Rodrigues; MORAIS, Rosângela Maria Rodrigues Medeiros Mitchell de. **Abandono digital:** a responsabilidade parental diante dos perigos das redes sociais. **Revista de Estudos Jurídicos do UNI-RN**, Natal, n. 6, p. 239-272, 2022, p. 246.

[47] CAVALCANTE, Laylana Araújo *et al*. **Psicologia forense aplicada à perícia de crimes sexuais contra crianças em ambiente digital.** Research, Society and Development, v. 9, n. 10, e7129109181, 2020, p. 4.

[48] LOUREIRO, Wilson; RODRIGUES, Gabriele; DUCATTI, Rafaela; SILVA, Marcella; DOS SANTOS, Thais. **Capturados na Rede:** um documentário para repensar os crimes sexuais online contra menores de idade no Brasil. **Retos XXI**, v. 9, p. 1-21, 2025, pp. 13-14.

mas monetização do material em plataformas especializadas ou redes de pedofilia, configurando exploração sexual comercial com fins lucrativos[49].

O Acórdão TCU 2515/2025 identificou que "criminosos utilizam a infraestrutura de monetização das próprias plataformas e sistemas de pagamento digitais para lucrar com a exploração sexual"[50], demonstrando que as plataformas tornam-se cúmplices estruturais ao fornecerem os meios econômicos para a perpetração do crime.

A ausência de obrigação legal de remoção proativa e a lentidão na moderação, mesmo após denúncias fundamentadas, permitem que imagens permaneçam circulando indefinidamente, agravando o dano e configurando negligência institucional sistemática.

1.2.5 *Cyberbullying* e violência psicológica sistemática

O *cyberbullying* designa ofensas, humilhações e constrangimentos sistemáticos perpetrados mediante tecnologias digitais, configurando crimes contra a honra praticados em meio virtual. Distingue-se do bullying tradicional por três características: alcance ilimitado, dado que conteúdos ofensivos podem ser visualizados por milhares de pessoas; permanência temporal, pois permanecem acessíveis indefinidamente; e anonimato relativo, que encoraja práticas mais violentas [51].

Ferreira sustenta que a vulnerabilidade digital pode ser descrita como "estado de predisposição a risco nos ciberespaços, que favorece a aparição de iniquidades, assimetrias de poder e violações à privacidade"[52]. Essas vítimas de violência

---

[49] LIMA, Jamile Moreira; VIANA, Johnnatan Reges. **Crimes cibernéticos**: aumento de crimes virtuais contra crianças e adolescentes pós-pandemia no Brasil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 5, p. 2051-2067, maio 2024, p. 2056.

[50] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 31.

[51] FERREIRA, Letícia Sthefane Santos. **Prática de crimes cibernéticos contra a criança e o adolescente:** mecanismos investigativos e combativos. 2025. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Lavras, Lavras, 2025, p. 9.

[52] LOPES, Juliano. Delimitando o conceito de vulnerabilidade digital. **Jota**, 2021. *apud* FERREIRA, Letícia Sthefane Santos. **Prática de crimes cibernéticos contra a criança e o adolescente:**

psicológica online apresentam quadros graves de ansiedade, depressão e ideação suicida, com consequências que podem se estender por anos após a cessação das agressões.

1.2.6 Desafios online e indução a práticas autolesivas

Os chamados "desafios online" (*challenges* ou *trends* viralizados em plataformas digitais) constituem fenômeno que ilustra a capacidade das redes sociais de induzir comportamentos de risco em crianças e adolescentes mediante dinâmicas de pressão social, busca por validação e mimetismo comportamental. Soares e Morais documentam casos emblemáticos, incluindo o "desafio Baleia Azul" (que induzia adolescentes a práticas progressivamente autolesivas, culminando em suicídio) e o "desafio do álcool em gel" (no qual crianças eram incentivadas a atear fogo em partes do próprio corpo).[53]

Em outubro de 2025, a Polícia Civil do Distrito Federal instaurou inquérito para investigar a morte de Sarah Raissa Pereira, de 8 anos, que participou do "desafio do desodorante", circulante nas redes sociais[54]. A criança inalou gás de desodorante aerossol, o que lhe provocou parada cardiorrespiratória, sendo posteriormente constatada morte cerebral. Os responsáveis pela publicação do desafio podem responder por homicídio duplamente qualificado (por emprego de meio capaz de causar perigo comum e por vítima menor de 14 anos), com pena de até 30 anos de reclusão.

A dinâmica dos desafios online opera mediante exploração de vulnerabilidades psicológicas específicas da infância e da adolescência: desejo de aceitação pelo

---

mecanismos investigativos e combativos. 2025. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Lavras, Lavras, 2025, p. 13.

[53] SOARES, Rebeca Rodrigues; MORAIS, Rosângela Maria Rodrigues Medeiros Mitchell de. **Abandono digital:** a responsabilidade parental diante dos perigos das redes sociais. **Revista de Estudos Jurídicos do UNI-RN,** Natal, n. 6, p. 239-272, 2022, p. 247.

[54] CNN BRASIL. **Polícia instaura inquérito após morte de criança em desafio pela internet.** CNN Brasil, 13 out. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/centro-oeste/df/policia-instaura-inquerito-apos-morte-de-crianca-em-desafio-pela-internet/ . Acesso em: 25 nov. 2025.

grupo de pares, busca por reconhecimento e visibilidade, dificuldade em avaliar adequadamente riscos futuros, e crença na invulnerabilidade pessoal.

1.2.7 Deepfakes sexuais e a violência sintética produzida por inteligência artificial

A inteligência artificial generativa introduziu modalidade inédita de violência digital: a produção de conteúdo sexual sintético mediante manipulação algorítmica de imagens ou vídeos reais, resultando em representações falsas, mas visualmente indistinguíveis de registros autênticos, de crianças e adolescentes em situações sexuais explícitas. Entre janeiro e julho de 2025, a SaferNet Brasil recebeu 76.997 denúncias de crimes digitais, sendo 49.336 (64%) relacionadas a abuso e exploração sexual infantil[55].

Quatro casos de *deepfakes* sexuais envolvendo estudantes foram registrados em escolas de São Paulo, com ocorrências identificadas em 10 estados brasileiros, incluindo Minas Gerais, Rio de Janeiro e Paraná. O levantamento aponta que aplicativos permitem gerar imagens hiper-realistas, incluindo fotos manipuladas e animações (deepfakes) com vozes e rostos de menores, circulando rapidamente em redes sociais, aplicativos de mensagens e sites de pornografia com pouca moderação[56].

Estudos internacionais demonstram a magnitude global do problema. A *Internet Watch Foundation* (Reino Unido) identificou, em um único mês, 20.254 imagens de abuso infantil geradas por IA postadas em fórum darknet[57]. O *Australian Institute of Criminology* alerta que "aumentos no volume de material de abuso infantil online

[55] CNN BRASIL. **Deepfakes e IA geram quase 50 mil denúncias de abuso infantil no Brasil.** CNN Brasil, ago. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/brasil/deepfakes-e-ia-geram-quase-50-mil-denuncias-de-abuso-infantil-no-brasil/ . Acesso em: 25 out. 2025.
[56] CNN BRASIL, **Deepfakes e IA geram quase 50 mil denúncias de abuso infantil no Brasil**, *op. cit.*
[57] WOLBERS, Heather; CUBITT, Timothy; CAHILL, Michael John. Artificial intelligence and child sexual abuse: a rapid evidence assessment. **Trends & issues in crime and criminal justice**, Canberra, n. 711, jan. 2025, p. 2.

podem influenciar a capacidade de investigar crimes sexuais contra crianças, dado que conteúdos gerados por IA podem ser indistinguíveis de material real"[58].

A produção de *deepfakes* sexuais envolvendo menores não encontra tipificação penal específica no ordenamento jurídico brasileiro. Embora o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) criminalize a produção, reprodução e divulgação de material pornográfico envolvendo criança ou adolescente (artigo 241), a legislação foi elaborada em contexto tecnológico anterior ao desenvolvimento de inteligência artificial generativa, não contemplando explicitamente a produção de imagens sintéticas. Essa lacuna normativa foi identificada pelo Tribunal de Contas da União no Acórdão 2515/2025, que recomendou ao Congresso Nacional a elaboração de proposta legislativa específica para criminalizar a produção e disseminação de deepfakes sexuais envolvendo menores de idade[59].

1.3 Hipervulnerabilidade digital e o conceito de abandono digital

As violências descritas na seção anterior não ocorrem em vácuo normativo ou social; prosperam precisamente porque encontram terreno fértil na tríplice omissão de Estado, plataformas digitais e sociedade**.**

A transição da fenomenologia das violências (seção 1.2) para o conceito de abandono digital (presente seção) não constitui mera sequência expositiva: revela relação de causalidade estrutural. O abandono digital, entendido como negligência parental na supervisão das atividades virtuais de crianças e adolescentes, não é causa isolada das violências, mas componente de uma arquitetura mais ampla de negligências interdependentes que torna possível, facilita e, em muitos casos, incentiva a perpetração de crimes contra menores no ambiente digital**[60].**

---

[58] *Ibid.*, p. 2.
[59] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 18.
[60] MARTIN, Júlia Saes. **Abandono digital e dever de vigilância parental sob a ótica do princípio da proteção integral à criança**. 2024. Monografia (Bacharelado em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2024, p. 4.

A expressão "abandono digital" foi cunhada pela advogada especialista em Direito Digital Patricia Peck Pinheiro mediante provocação retórica que expõe, com clareza incômoda, a contradição estrutural da parentalidade contemporânea:

> Você deixaria seu filho sozinho o dia todo, sentado na calçada de sua casa, sem saber com quem ele está falando, o que está conversando ou para onde poderia ir? Então por que será que hoje há tantos jovens assim, abandonados na calçada digital?[61]

A metáfora da "calçada digital" materializa a percepção social de que o ambiente virtual, embora fisicamente confinado ao espaço doméstico, constitui território de risco equivalente ou superior aos espaços públicos tradicionais.

A vulnerabilidade de crianças e adolescentes no ambiente digital não decorre apenas de desconhecimento técnico, mas de características inerentes ao seu desenvolvimento psicossocial. O Delegado Cristiano Maia, titular da Delegacia da Criança e do Adolescente Vítima do Rio de Janeiro (DCAV-RJ), referência nacional no combate a crimes virtuais contra menores, explica que "crianças e adolescentes são mais vulneráveis porque ainda estão em formação emocional, cognitiva e social. O desejo de pertencimento, a busca por aceitação e a exposição intensa nas redes os tornam alvos fáceis de manipulação"[62].

Essa vulnerabilidade cognitiva é sistematicamente explorada por predadores sexuais mediante estratégias de *grooming*, mas também pelas próprias plataformas digitais, cujos algoritmos são programados para capturar atenção mediante exploração de circuitos de recompensa dopaminérgica.

---

[61] PINHEIRO, Patricia Peck. apud DIAS, Camila dos Reis. **O abandono digital:** análise jurídica da responsabilidade civil dos pais frente à desídia na supervisão da atividade online dos filhos. 2019. Monografia (Bacharelado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2019, p. 6.

[62] BRASIL. Agência Nacional de Telecomunicações. **Polícia Civil do Rio de Janeiro faz alerta sobre novos crimes virtuais praticados contra crianças e adolescentes**. Entrevista com Cristiano Vale Maia, Delegado Titular da DCAV-RJ. Portal Anatel, out. 2025. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/policia-civil-do-rio-de-janeiro-faz-alerta-sobre-novos-crimes-virtuais-praticados-contra-contra-criancas-e-adolescentes . Acesso em: 3 nov. 2025.

Martin define o abandono digital como "negligência parental em relação à supervisão das atividades virtuais de crianças e adolescentes, expondo-as a diversos riscos sem orientação adequada quanto aos perigos do ambiente digital"[63]. A autora sustenta que o abandono digital não se limita à ausência física dos pais; configura-se pela "omissão no dever constitucional e legal de vigilância, assistência e educação dos filhos menores no ambiente digital, em violação aos artigos 227 da Constituição Federal, 22 do Estatuto da Criança e do Adolescente, e 1.634, inciso I, do Código Civil"[64].

Nesse contexto, a omissão parental na mediação do uso de tecnologias digitais por crianças e adolescentes não pode, contudo, ser compreendida exclusivamente como falha individual ou negligência voluntária. Três assimetrias estruturais configuram obstáculos materiais à mediação protetiva:

1. primeira assimetria (letramento digital): enquanto crianças e adolescentes desenvolvem, desde a primeira infância, habilidades técnicas para navegação em plataformas digitais, constituindo a chamada "geração de nativos digitais", seus pais e responsáveis, em sua maioria, não foram formados em ambiente digital e carecem de conhecimento técnico sobre funcionamento de algoritmos, mecanismos de privacidade, ferramentas de controle parental e estratégias de predadores sexuais online[65].

O Delegado Maia reconhece essa assimetria ao afirmar que "é fundamental que os adultos entendam o universo digital das crianças. Saber quais aplicativos utilizam, com quem conversam e que tipo de conteúdo consomem não é invasão, mas ato de cuidado e proteção”[66].

---

[63] MARTIN, Júlia Saes. **Abandono digital e dever de vigilância parental sob a ótica do princípio da proteção integral à criança**. 2024. Monografia (Bacharelado em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2024, p. 4.
[64] *Ibid*., p. 4.
[65] SANTOS, Caroline Henriques Mota Balduíno. **A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados.** 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021, p. 170
[66] BRASIL. Agência Nacional de Telecomunicações, 2025, *op. cit*.

2. segunda assimetria (acesso a recursos protetivos): ferramentas de controle parental, aplicativos de monitoramento, cursos de alfabetização digital e serviços de apoio psicológico especializado em violência digital encontram-se, em sua maioria, disponíveis apenas mediante pagamento ou requerem dispositivos tecnológicos avançados, excluindo famílias em situação de vulnerabilidade socioeconômica[67]. A pesquisa TIC Kids Online 2024 demonstra que apenas 42% dos pais brasileiros utilizam ferramentas técnicas de controle parental, sendo que esse percentual é significativamente inferior entre famílias de baixa renda[68].

3. terceira assimetria (disponibilidade temporal): a mediação parental qualificada do uso de tecnologias por crianças e adolescentes demanda tempo, dedicação e presença constante, recursos escassos em contextos familiares nos quais os responsáveis submetem-se a jornadas de trabalho extensas, múltiplos vínculos empregatícios ou trabalho informal precarizado[69].

Essas três assimetrias configuram aquilo que se pode denominar hipervulnerabilidade digital: condição estrutural na qual crianças e adolescentes encontram-se duplamente expostos a riscos, tanto pela insuficiência das políticas públicas estatais e pela omissão corporativa das plataformas digitais, quanto pela impossibilidade material de suas famílias exercerem mediação protetiva efetiva.

Um caso emblemático dessa hipervulnerabilidade é o fenômeno dos "influenciadores mirins", documentado em reportagem investigativa da Repórter Brasil. A matéria revela que 93% da população brasileira entre 9 e 17 anos usam a internet e três a cada quatro jovens sonham em produzir conteúdo. Crianças de 5 e 6 anos atuam como influenciadores digitais, promovendo produtos comerciais e

[67] SANTOS, 2021, *op. cit*., p. 172.
[68] CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **TIC Kids Online Brasil 2024:** pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Cetic.br, 2024, p. 4
[69] MARTIN, 2024, *op. cit*., p. 27.

produzindo conteúdo diariamente, sem alvará judicial exigido pelo Estatuto da Criança e do Adolescente para trabalho artístico infantil[70].

A hipervulnerabilidade digital infantojuvenil não decorre de falhas isoladas ou de negligências individuais**, mas de uma arquitetura sistêmica de omissões corresponsáveis: Estado que não regula, plataformas que não protegem, e sociedade que não intervém**.

O capítulo seguinte examinará criticamente cada um desses agentes, demonstrando como suas omissões articuladas configuram aquilo que esta pesquisa denomina arquitetura da negligência.

[70] REPÓRTER BRASIL. **Influencers mirins atuam em Big Techs sem alvará judicial**; TV pede. Repórter Brasil, 11 abr. 2025. Disponível em: https://reporterbrasil.org.br/2025/04/influencers-mirins-big-techs-alvara-judicial/ . Acesso em: 2 nov. 2025.

CAPÍTULO 2 O DEVER DE PROTEÇÃO: O IDEAL NORMATIVO E SUAS PROMESSAS

O capítulo anterior demonstrou que a hipervulnerabilidade digital infantojuvenil decorre de arquitetura sistêmica de omissões corresponsáveis. Nessa senda, este capítulo examinará criticamente cada dimensão dessa tríade, revelando como a promessa constitucional de proteção integral, embora densamente inscrita no ordenamento jurídico brasileiro, enfrenta entraves estruturais que esvaziam, na prática, a efetividade dos direitos fundamentais.

A compreensão jurídica da infância no Brasil sofreu uma transformação copernicana com a promulgação da Constituição Federal de 1988 e, posteriormente, do Estatuto da Criança e do Adolescente (ECA). Superou-se o antigo Código de Menores (1979), fundamentado na "Doutrina da Situação Irregular", que via a criança pobre ou infratora como objeto de intervenção estatal repressiva-assistencialista, para adotar a "Doutrina da Proteção Integral".

Nesse novo paradigma, crianças e adolescentes deixam de ser objetos de tutela para se tornarem sujeitos de direitos, dotados de absoluta prioridade. A promessa constitucional de proteção integral à infância e adolescência encontra-se densamente inscrita no ordenamento jurídico brasileiro. O artigo 227 da Constituição Federal estabelece que:

> 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 dignidade e ao desenvolvimento pleno, devendo colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.[71]

Essa mudança de eixo não é apenas semântica, mas impõe um novo dever de agir.

[71] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988.

A arquitetura normativa erigida a partir desse fundamento — o Estatuto da Criança e do Adolescente (ECA), a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet (MCI) e, mais recentemente, a Lei nº 15.211/2025 (ECA Digital) — materializa um sistema de garantias que, em tese, deveria blindar crianças e adolescentes contra toda forma de violência, inclusive aquelas perpetradas no ambiente digital.

Contudo, entre a letra da lei e sua concretização há um abismo estrutural. Monteiro et al. diagnosticam com precisão essa contradição ao afirmarem que, apesar da existência de um arcabouço legislativo internacional e nacional robusto, os números alarmantes de casos no Brasil e no mundo demonstram existir uma lacuna significativa entre a legislação e seu efetivo cumprimento[72]. Essa lacuna não é acidental: decorre de escolhas políticas, omissões institucionais e da subordinação de direitos fundamentais de crianças e adolescentes à lógica de mercado das plataformas digitais. Como será demonstrado ao longo deste capítulo, o Brasil não padece de falta de leis; padece de falta de efetividade.

2.1 Proteção Integral: a hermenêutica do melhor interesse e sua adaptação ao ambiente digital

O princípio da proteção integral, consagrado no artigo 227 da Constituição Federal e no artigo 3º do ECA, constitui o epicentro hermenêutico de toda legislação protetiva infantojuvenil no Brasil. Diferentemente de doutrinas anteriores, como a da "situação irregular" que reduzia criança e adolescente a objetos de intervenção estatal, a doutrina da proteção integral os reconhece como sujeitos de direitos fundamentais em condição peculiar de desenvolvimento, exigindo prioridade absoluta na concretização de seus interesses.

[72] MONTEIRO, Jarlene Aparecida Bandoli *et al*. **Fatores, espaços e autores da violência sexual contra crianças e adolescentes na sociedade brasileira**. Revista Caderno Pedagógico, Curitiba, v. 22, n. 9, p. 01-29, 2025, p. 25.

Botelho esclarece que o princípio da proteção integral não constitui categoria estática ou de conteúdo semântico fixo; ao contrário, seu significado depende da cultura, da sociedade e das posições axiológicas vigentes, de modo que os elementos e circunstâncias do caso concreto devem servir como balizas, cujo resultado sempre deverá se traduzir em uma melhora concreta na situação da criança ou do adolescente[73]. Essa formulação dinâmica impõe ao intérprete, seja o juiz, o controlador de dados, a plataforma digital ou o agente estatal, uma obrigação de fundamentação contextual e orientada a resultados protetivos mensuráveis.

No campo do tratamento de dados pessoais, essa hermenêutica ganha contornos específicos. O artigo 14 da LGPD estabelece que o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse, exigindo que os elementos do caso concreto sejam balizas para a aplicação do princípio[74]. Botelho sustenta que o nível de desenvolvimento físico e intelectual em que se encontram crianças e adolescentes não lhes permite ter uma visão clara das consequências que poderão advir do tratamento de seus dados pessoais[75]. Essa vulnerabilidade cognitiva, portanto, não é contingente ou superável mediante educação digital; é estrutural e inerente à condição de pessoa em desenvolvimento.

Não obstante, a aplicação dessa hermenêutica protetiva colide frontalmente com a arquitetura opaca das plataformas. Koffermann e Aguaded alertam que as tecnologias digitais contemporâneas são desenhadas intencionalmente para impulsionar o consumo de forma "invisível e incompreensível para o usuário", criando um ambiente onde a autonomia da vontade é suplantada por mecanismos de indução comportamental[76]. Nesse cenário, a assimetria não é apenas informacional, mas arquitetônica: a criança navega em um espaço projetado para explorar suas fragilidades cognitivas, tornando inócua a mera exigência formal de transparência.

---

[73] BOTELHO, Marcos César. **A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes**. Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE), Bebedouro, v. 8, n. 2, p. 197-230, 2020, p. 216

[74] *Ibid*., p. 215.

[75] *Ibid*., p. 217.

[76] KOFFERMANN, Marcia; AGUADED, Ignacio. **A influência das redes sociais sobre os adolescentes:** ciberconsumo e educação crítica. Revista Lumina, v. 17, n. 1, p. 127, 2023.

A vulnerabilidade da criança no ciberespaço é, portanto, absoluta e presumida, independente de eventual consentimento — ainda que mediado pelos pais — prestado em meio a políticas de privacidade ininteligíveis. Botelho reforça essa premissa ao sustentar que, em razão da condição vulnerável natural de crianças e adolescentes, “a sua compreensão acerca das consequências do tratamento de seus dados pessoais é mitigada”, uma vez que o nível de desenvolvimento físico e intelectual não lhes permite ter uma “visão clara das consequências que poderão advir do tratamento”[77]. Essa hipossuficiência cognitiva torna irrelevante a mera formalidade do 'clique no aceite', exigindo do Estado e das plataformas uma postura ativa de proteção que independa da manifestação de vontade da vítima ou de seus responsáveis.

O ordenamento jurídico brasileiro atribui aos pais, no âmbito do poder familiar, a responsabilidade de assegurar que seus filhos estejam protegidos de qualquer forma de negligência, conforme previsto no art. 227 da Constituição Federal e no art. 22 do Estatuto da Criança e do Adolescente. Contudo, como será demonstrado na próxima seção, a mera imposição desse dever aos pais, sem que o Estado forneça os meios materiais, cognitivos e institucionais para seu exercício, configura criminalização da pobreza e transferência indevida de responsabilidades que deveriam recair sobre o poder público e as corporações.

Nesse cenário, o Tribunal de Contas da União diagnosticou que o País não possui, até o presente momento, política pública específica para tratar da prevenção e do combate a crimes sexuais contra crianças e adolescentes na internet[78]. Esse diagnóstico evidencia que o cenário de negligência não decorre simplesmente do avanço tecnológico, mas resulta de decisões intencionais das empresas na forma como estruturam suas plataformas, somadas à insuficiência de atuação regulatória por parte do Estado.

Posto isso, a ausência de política pública específica evidencia que, embora o ordenamento jurídico reconheça formalmente a proteção integral como princípio

[77] BOTELHO, *op. cit*., p. 216-217.
[78] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 14.

orientador, o Estado brasileiro tem falhado sistematicamente em traduzi-lo em ações concretas, coordenadas e efetivas.

2.2 O poder familiar e os deveres de supervisão no Código Civil

O papel tradicional dos pais, antes centrado sobretudo na supervisão presencial dos filhos, passa por uma transformação profunda no contexto da sociedade da informação, adquirindo novos sentidos e exigências práticas. O Código Civil de 2002, em seu artigo 1.634, incisos I e II, impõe aos pais o dever-poder de dirigir a criação e a educação dos filhos, bem como de exigir-lhes respeito e obediência, e de tê-los em seu poder e guarda.

Nesse contexto, a doutrina civilista contemporânea, atenta a essa mutação social, compreende que o conceito de criação e educação no século XXI é indissociável da mediação e da supervisão das interações digitais, estendendo ao ambiente virtual a proteção integral e a prioridade absoluta consagradas pelo artigo 227 da Constituição Federal.

Dessa forma, a simples disponibilização de um equipamento conectado à internet a uma criança ou adolescente implica, para os pais, a assunção dos riscos inerentes ao seu uso, tornando-os corresponsáveis pelo ambiente digital acessado por seus filhos.

A falta de supervisão adequada não se limita a uma falha educativa, podendo configurar responsabilidade civil. Tal conduta, frequentemente descrita na literatura como uma forma de negligência digital, corresponde à ausência de cuidado dos responsáveis quanto à proteção online dos filhos e, quando se mostra grave e reiterada, pode justificar medidas como a suspensão ou mesmo a perda do poder familiar, conforme prevê o art. 1.638 do Código Civil.

A falha no cumprimento desse dever de vigilância, longe de ser uma mera opção educacional, configura, em sua face mais grave, um ato de negligência digital. Este fenômeno, conceituado na doutrina como "abandono digital", caracteriza-se pela

delegação às redes sociais e plataformas digitais da criação e do entretenimento dos filhos, associada à falta de fiscalização e orientação quanto aos conteúdos acessados.

Conforme analisado por Ana Paula Gimenez, "o abandono digital é delegar às redes sociais, a criação dos filhos. É uma forma de negligenciar a própria prole"[79] . Trata-se de uma conduta omissiva que, para além de uma falha educativa, pode gerar consequências jurídicas diretas, incluindo a responsabilização civil por atos praticados pelos filhos no ambiente virtual com base na culpa in vigilando.

Quando a conduta negligente se mostra grave e reiterada, configurando um descumprimento deliberado e persistente dos deveres inerentes ao poder familiar, o próprio Código Civil prevê medidas drásticas para a proteção do menor. O artigo 1.638 estabelece como causa de perda do poder familiar o fato de os pais incorrerem em “falta grave" em relação aos deveres que lhes competem.

Em uma interpretação sistemática e atualizada, a "falta grave" pode hoje, perfeitamente, englobar o abandono digital extremado, em que a ausência total de supervisão parental exponha a criança ou adolescente aos crimes cibernéticos, com sérios danos ao seu desenvolvimento físico e mental. Nesses casos, o Estado, na condição de garantidor da doutrina da proteção integral (art. 227 da CF/88), pode e deve intervir, suspendendo ou destituindo o poder familiar para salvaguardar o superior interesse da criança.

A complexidade jurídica atinge seu ápice quando a omissão parental no ambiente digital resulta em danos concretos a terceiros. O ordenamento brasileiro, na esteira de sistemas jurídicos comparados, adotou um regime de responsabilidade civil objetiva para os genitores, consagrado nos artigos 932, inciso I, e 933 do Código Civil. Este último dispositivo é peremptório ao estabelecer que, nestes casos específicos, "independe de culpa o dever de indenizar"[80].

---

[79] GIMENEZ, Ana Paula. **Parentalidade e a Era Digital:** Abandono Digital, Oversharenting e Feed Zero. Instituto Brasileiro de Direito de Família (IBDFAM), Belo Horizonte, [s.d.]. Disponível em:https://ibdfam.org.br/artigos/2303/Parentalidade+e+a+Era+Digital%3A+Abandono+Digital%2C+Oversharenting+e+Feed+Zero . Acesso em: 25 nov. 2025.

[80] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil. Brasília: Presidência da República, 2002. Art. 933.

Trata-se de uma opção legislativa que impõe uma obrigação de garantia ou de resultado: se o filho menor, sob sua guarda, causa um dano através da prática de algum tipo de crime cibernético, por exemplo, o patrimônio dos pais é o garantidor da reparação, independentemente de sua ciência ou capacidade técnica para impedir o ato ilícito. A doutrina civilista clássica, representada por autores como Caio Mário da Silva Pereira, sustenta que a responsabilidade dos pais pelos atos ilícitos praticados pelos filhos menores sob sua autoridade possui natureza objetiva, não dependendo da comprovação de culpa.

A dinâmica da responsabilização torna-se ainda mais complexa diante da regra do art. 928 do Código Civil, que admite, em caráter subsidiário e excepcional, a responsabilidade do próprio incapaz. Trata-se de um mecanismo que busca evitar que a vítima permaneça sem reparação quando inexistirem outros responsáveis aptos a indenizar.

Caso os pais não disponham de recursos suficientes, ou se o menor estiver de fato emancipado pela via econômica, fenômeno cada vez mais comum com os influenciadores mirins que geram renda própria, o próprio incapaz responderá com seu patrimônio. Apesar disso, como bem destacam Facchini Neto e Andrade, a corrente doutrinária atual ressalva que essa responsabilização deve ser equitativa (parágrafo único do art. 928), impedindo que a reparação do dano prive o menor dos recursos mínimos para sua subsistência e desenvolvimento, diretriz consolidada no Enunciado nº 449 da V Jornada de Direito Civil do CJF[81].

Nada obstante, a aplicação rígida desta dogmática civilista, concebida em um contexto analógico, colide frontalmente com a realidade sociotécnica do século XXI, gerando uma tensão crítica que a lei pura é incapaz de resolver. A premissa de um guardião onisciente e onipresente desaba ante a evidência empírica. Sousa et al. (2025) denunciam a lacuna de competência digital parental, demonstrando uma

[81] FACCHINI NETO, Eugênio; ANDRADE, Fábio Siebeneichler de. **Notas sobre a indenização equitativa por danos causados por incapazes**. Revista Brasileira de Direito Civil, v. 13, n. 3, p. 93-118, 2018, p. 101.

"discrepância significativa entre o conhecimento percebido e o conhecimento real dos pais" para gerir riscos digitais[82].

A exigência legal de um controle parental eficiente desconsidera os profundos níveis de desigualdade em alfabetização digital, convertendo a responsabilidade objetiva em uma verdadeira *probatio diabolica*[83]. Para muitas famílias afetadas pela exclusão digital, faltam tanto os recursos tecnológicos quanto o conhecimento necessário para realizar a supervisão que o ordenamento jurídico presume ser possível.

Este regime de responsabilidade enfrenta, ademais, um paradoxo normativo intrínseco. Guterres et al. (2022) apontam a antinomia entre a incapacidade absoluta presumida pelo Código Civil e o princípio da autonomia progressiva conferido pelo Estatuto da Criança e do Adolescente (ECA) e, notadamente, pela Lei Geral de Proteção de Dados (LGPD), que reconhece a capacidade de consentimento do adolescente[84]. Enquanto o Código Civil impõe vigilância irrestrita, o ECA Digital (Lei 15.211/2025), em seu artigo 5º, ao tratar dos direitos da criança e do adolescente no ambiente digital, reforça o direito à participação e ao desenvolvimento, criando um campo de tensão inevitável: **até onde se estende o dever de vigilância dos pais sem macular o direito à privacidade e à construção da autonomia do adolescente?** Este descompasso gera uma insegurança jurídica palpável, deixando pais e operadores do direito em um limbo interpretativo.

Por fim, a própria premissa fundante do sistema – a de que a família é, por excelência, o *locus* seguro de proteção – é desafiada por dados cruéis. Monteiro et al. (2025) alertam que "o tabu e o fato da grande maioria dos agressores ser constituída

[82] SOUSA, Mykaele F. A. et al. **Avaliação da Competência Parental na Gestão da Privacidade dos Filhos em Ambientes Digitais**. Programa de Pós-Graduação em Informática (PPGIa), Pontifícia Universidade Católica do Paraná, 2025, p. 2

[83] Nota explicativa: *Probatio diabolica* é a expressão utilizada para designar prova excessivamente difícil ou praticamente impossível de ser produzida por uma das partes.

[84] GUTERRES, Isadora Balestrin; DUARTE, Hendrisy Araujo; CHAVES, Elisa Viana Dias. **Limites entre autoridade parental e autonomia digital de crianças e adolescentes**. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 6., 2022. Anais [...]. [S.l.: s.n.], 2022, p. 7.

por figuras paternas ou parentes induz à manutenção da cultura do silêncio"[85]. Este dado revela que o dever de vigilância, em contextos de violência intrafamiliar, falha não por uma mera omissão, mas por uma ação direta e predatória do próprio guardião.

A arquitetura da negligência, portanto, é complexa e multifacetada. O descompasso entre o dever civil de vigilância e as condições materiais e sociais para seu exercício será retomado criticamente no próximo capítulo, que investigará a corresponsabilidade do Estado e das plataformas digitais na proteção da infância online, completando o desenho desta arquitetura sistêmica da negligência.

2.3 A regulação atual das plataformas: do Marco Civil à LGPD

A resposta jurídica brasileira aos desafios da sociedade da informação consolidou-se através de um arcabouço normativo que buscou equilibrar a liberdade de expressão, a inovação tecnológica e a proteção de direitos fundamentais. A análise da regulação vigente exige, portanto, um exame crítico da transição de um modelo de mínima intervenção estatal para um paradigma de proteção de dados e privacidade, consubstanciado na interação entre o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD).

Contudo, é imperativo questionar se os mecanismos de responsabilização desenhados por essas legislações permanecem suficientes diante da complexidade dos danos algorítmicos atuais. Este tópico examina a estrutura jurídica que rege a atuação das plataformas no Brasil, identificando como a arquitetura normativa, embora robusta em princípios, apresenta lacunas operacionais que dificultam a tutela efetiva da criança e do adolescente no ambiente digital.

2.3.1 O Marco Civil da Internet e o Regime de Responsabilidade das Plataformas

[85] MONTEIRO, Jarlene Aparecida Bandoli et al. **Fatores, espaços e autores da violência sexual contra crianças e adolescentes na sociedade brasileira**. Revista Caderno Pedagógico, Curitiba, v. 22, n. 9, 2025, p. 12.

O Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu a base do ordenamento jurídico brasileiro para a internet, e seu Artigo 19 consagrou um regime de responsabilidade civil para os provedores de aplicações de internet que tem sido central para a governança das plataformas. Em sua redação original, o dispositivo estabelece que tais provedores somente poderão ser responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomarem as providências para, no âmbito de seu serviço, tornar indisponível o conteúdo apontado como ilícito[86].

Este modelo, conhecido como *notice-and-take-down*, foi concebido para equilibrar a liberdade de expressão, a inovação e a responsabilização, partindo da premissa de que a rede é, por essência, uma estrutura de interlocução de terceiros. No entanto, sua aplicação prática revela uma tensão crítica: ao condicionar a atuação do provedor a uma intervenção judicial prévia, o sistema pode se mostrar excessivamente lento e burocrático para conter danos de propagação instantânea e impacto devastador, como aqueles associados à divulgação não consensual de imagens íntimas (*revenge porn*), *cyberbullying* e *deepfakes* de natureza difamatória contra crianças e adolescentes[87].

A análise do conflito entre normas do MCI e da LGPD evidencia que, embora o MCI tenha sido a primeira lei a elevar a proteção de dados à condição de princípio fundamental do uso da internet no Brasil (art. 3º, III), sua estrutura de responsabilidade pode, em certos casos, criar um descompasso temporal que agrava a violação de direitos[88].

2.3.2 LGPD e o mito do consentimento parental informado: o abismo da verificação de idade

[86] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Art. 19.
[87] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2022, p. 307-308.
[88] BIONI, Bruno. **Proteção de Dados Pessoais**. 3. ed. São Paulo: Revista dos Tribunais, 2023, p. 298.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), no artigo 14, §1º, estabelece que o tratamento de dados pessoais de criança (menor de 12 anos) deve ocorrer com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal[89]. O dispositivo, inspirado no GDPR europeu e no COPPA estadunidense, baseia-se na premissa de que pais possuem capacidade técnica e jurídica para compreender políticas de privacidade e avaliar riscos associados ao tratamento de dados de seus filhos. Contudo, essa premissa é empiricamente falsa e normativamente vazia.

Mais grave ainda: no direito brasileiro, não há nenhuma lei regulando expressamente como deverá ser feita a identificação de crianças e adolescentes. A LGPD exige o melhor interesse, mas não explicita como o controlador irá identificar esses usuários menores de idade.

Ana Frazão denuncia que essa lacuna regulatória é um abismo normativo que permite às plataformas digitais alegarem cumprimento formal da LGPD mediante mecanismos de autodeclaração de idade, sabidamente ineficazes e facilmente burlados por crianças, sem implementar qualquer tecnologia robusta de verificação. A jurista argumenta que essa omissão legislativa não é acidental: reflete a subordinação do interesse público à pressão corporativa, uma vez que exigir verificação de idade mediante documentos ou biometria implicaria custos operacionais e redução de base de usuários — fatores que afetam diretamente o modelo de negócio das plataformas[90].

Paralelamente, Botelho aprofunda sua crítica ao evidenciar o caráter circular do art. 14 da LGPD. O dispositivo exige que o controlador adote medidas razoáveis para confirmar que o consentimento foi realmente concedido pelo responsável legal da criança. Entretanto, essa verificação depende, em muitos casos, do acesso a informações pessoais que o próprio controlador não pode coletar antes da obtenção do consentimento. Assim, cria-se um impasse: a lei veda o tratamento prévio dos

[89] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Art. 14.
[90] FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes:** parecer. São Paulo: Instituto Alana, 2020, p. 42-43.

dados, mas simultaneamente impõe ao controlador o dever de comprová-lo, resultando em uma dinâmica operacional praticamente inviável.[91]

Essa circularidade de que é preciso coletar dados para pedir autorização para coletar dados, expõe a inviabilidade prática do art. 14 da LGPD quando aplicado a plataformas de grande escala. Diante desse impasse, as empresas passaram a utilizar sistemas de autodeclaração de idade, nos quais o próprio usuário informa sua data de nascimento.

Frazão identifica esse mecanismo como uma ficção jurídica que permite às plataformas sustentar uma forma de ignorância deliberada. Ela observa que o COPPA, nos Estados Unidos, dispensa os operadores de investigar a idade real de seus usuários, o que facilita que crianças omitam sua verdadeira idade. Assim, enquanto não houver conhecimento efetivo de que se trata de criança, o operador não é responsabilizado.[92]

Esse mesmo modelo que tolera a ignorância como estratégia de conformidade tem sido replicado no Brasil em razão da falta de regulamentação específica por parte da Autoridade Nacional de Proteção de Dados (ANPD).

Nesse contexto, a lógica econômica do modelo de negócios baseado em dados agrava a vulnerabilidade. Quando os pais, especialmente aqueles em situação de vulnerabilidade socioeconômica, acreditam estar oferecendo entretenimento gratuito aos filhos, estão, na verdade, inserindo-os em um complexo sistema de coleta e monetização de dados, que opera por meio de publicidade direcionada e perfilamento comportamental.

2.3.3 Síntese crítica: a antinomia prática no interior do sistema normativo

De um lado, o Art. 19 do MCI, em sua redação original, instituía um regime de responsabilidade civil que, ao condicionar a indisponibilidade de conteúdo à ordem

[91] BOTELHO, 2020, *op. cit*., p. 225.
[92] FRAZÃO, 2020, *op. cit*., p. 42-43.

judicial específica, conferia às plataformas um status de relativa imunidade em relação aos ilícitos praticados por terceiros.

Apesar disso, o Supremo Tribunal Federal, em junho de 2025, declarou a inconstitucionalidade parcial deste dispositivo, reconhecendo que a regra geral do art. 19 não confere proteção suficiente a bens jurídicos constitucionais de alta relevância[93]. O Tribunal estabeleceu que, até que nova lei seja editada, os provedores poderão ser responsabilizados civilmente por danos decorrentes de conteúdos de terceiros em casos de crimes ou atos ilícitos se, após receber um pedido de retirada, deixar de remover o conteúdo, afastando-se a exigência de ordem judicial para todas as hipóteses[94].

Do outro, o Art. 14 da LGPD, ao erigir o consentimento parental como pilar para o tratamento de dados de crianças, impõe uma obrigação que é estruturalmente esvaziada pela ausência de um mecanismo eficaz de verificação de idade e pela complexidade das políticas de privacidade[95].

O descompasso normativo produz um vácuo de responsabilização, no qual a hipervulnerabilidade da criança é paradoxalmente ampliada pela própria arquitetura do sistema que deveria protegê-la. A transferência da tutela aos pais, por meio do consentimento, revela-se insuficiente diante da profunda assimetria informacional e técnica; ao mesmo tempo, o modelo emergente de responsabilidade das plataformas pelo conteúdo (ainda em fase de consolidação) tenta corrigir a morosidade de mecanismos tradicionais, incapazes de responder à velocidade dos danos digitais.

A antinomia, portanto, não é externa ao ordenamento, mas integrante de sua própria estrutura. Ela expõe a divergência entre a promessa constitucional de proteção integral da criança e os instrumentos normativos concebidos para concretizá-la. É

---

[93] BRASIL. SUPREMO TRIBUNAL FEDERAL. **STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros**. Brasília: STF, 26 jun. 2025. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/ . Acesso em: 4 nov. 2025.

[94] LEITE, Thiago de Paula. **Responsabilização de plataformas por conteúdos de terceiros.** Estratégia Carreira Jurídica, [S.l.], 2 jul. 2025. Disponível em: https://cj.estrategia.com/portal/responsabilidade-plataformas-conteudos-de-terceiros/ . Acesso em: 3 nov. 2025.

[95] BRASIL. **Lei nº 13.709/2018**. Art. 14.

nesse ponto que se delineia a arquitetura normativa da negligência: na incapacidade do sistema de oferecer respostas coerentes e eficazes, mantendo a criança em uma zona de sombra em que seus direitos são reconhecidos em tese, mas pouco resguardados na prática.

2.4 O ECA Digital (Lei 15.211/2025): a nova esperança regulatória e seus desafios

A sanção da Lei nº 15.211, de 17 de setembro de 2025[96], popularmente denominada por ECA Digital, representa o esforço legislativo mais ambicioso do Brasil para enfrentar os riscos digitais à infância. No entanto, uma leitura meramente descritiva não basta. É necessário submeter o diploma legal a um exame crítico que confronte suas inovações normativas com os obstáculos concretos de implementação.

2.4.1 Fundamentação e âmbito: resposta a lacunas históricas

O ECA Digital surge como resposta direta à insuficiência reconhecida do Marco Civil da Internet e da LGPD em proteger integralmente a infância online[97]. Seu Art. 1º e parágrafo único definem um âmbito amplíssimo pelo conceito de "acesso provável", estratégia crucial para coibir a evasão regulatória das plataformas[98]. Conforme análise do TCU, tal conceito visa obstruir a estratégia, até então comum, de plataformas como TikTok e Instagram alegarem não serem direcionadas a crianças para se furtarem às obrigações mais rigorosas[99].

A fundamentação do ECA Digital alinha-se com estudos internacionais que destacam a hipervulnerabilidade digital infantojuvenil. Como aponta Reginaldo Lima em pesquisa sobre vulnerabilidade digital, "crianças submetidas à adultização digital

---

[96] BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Diário Oficial da União, Brasília, DF, 17 set. 2025.
[97] SANTOS, Caroline Henriques Mota Balduíno. **A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021, p. 116.
[98] BRASIL. Lei nº 15.211/2025, art. 1º.
[99] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 18.

estão mais suscetíveis a práticas de mercantilização, objetificação e cyberbullying"[100]. Esta percepção da vulnerabilidade específica no ambiente digital fundamenta a necessidade de legislação especializada.

2.4.2 Inovações e princípios: avanços à luz da doutrina

O princípio do safety by design (Art. 3º) opera uma inversão paradigmática na regulação digital brasileira[101]. Conforme análise de Patrícia Klunck sobre regulação e infância, "a proteção de crianças no ambiente digital exige abordagem preventiva, não meramente reparatória"[102]. O TCU já recomendara que "a segurança da criança deve ser um requisito de engenharia de software desde a fase de concepção do produto"[103], fundamentando tecnicamente a opção legislativa.

O dever de cuidado (*duty of care*) expresso no Art. 6º representa outro avanço conceitual significativo. Frazão aborda sobre o dever de cuidado das plataformas e argumenta que "Por essa razão, discute-se a necessidade de algum tipo de regulação para conter o alto grau de externalidades negativas que as plataformas digitais vêm apresentando"[104]. Essa interpretação evidencia que a própria lógica de autorregulação das plataformas enfrenta limitações concretas, já que o consentimento parental, embora previsto em lei, não se ajusta às dinâmicas operacionais dos ambientes digitais.

2.4.3 Tensões e desafios: crítica sobre efetividade

[100] LIMA, Reginaldo Soares de Sousa. **Vulnerabilidade digital e riscos da adultização de menores em plataformas de mídia social**. Periódicos Brasil: Pesquisa Científica, [S.l.], v. 4, n. 2, 2025, p. 324.
[101] BRASIL. Lei nº 15.211/2025, art. 3º.
[102] KLUNCK, Patrícia. **A Regulação da Inteligência Artificial e a Proteção de Crianças e Adolescentes**. Porto Alegre: PUCRS, 2020, p. 8
[103] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 22.
[104] FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes: parecer**. São Paulo: Instituto Alana, 2020, p. 77.

O regime sancionatório do Art. 35, que prevê multas de até 10% do faturamento, é potente em tese. Entretanto, sanções mais drásticas mantêm-se dependentes de ordem judicial, reintroduzindo morosidade que a lei pretende superar.

Assim, esta crítica alinha-se com análise de Gomes *et al.* sobre crimes cibernéticos: “além disso, é fundamental que o sistema de justiça esteja preparado para lidar com a natureza técnica e transnacional dos crimes cibernéticos, adotando medidas preventivas e reativas que sejam eficazes e ágeis"[105]. Observa-se, portanto, que a lei enfrenta o desafio da assimetria regulatória. Como aponta estudo sobre a relação do ECA Digital com inteligência artificial, "integrar direito, engenharia e design de produto sob uma mesma bússola: o melhor interesse da criança como critério técnico, jurídico e ético de desenvolvimento digital"[106]. O Art. 36-A, que vincula multas ao Fundo da Criança, é passo na direção certa, mas insuficiente sem investimento massivo em capacidade estatal.

Nos últimos anos, observa-se que o predomínio de mecanismos de autorregulação vem gradualmente cedendo espaço a modelos de regulação estatal mais rígidos. Essa mudança de paradigma tende a desencadear disputas jurídicas relevantes, especialmente quanto à constitucionalidade de medidas mais invasivas previstas nas novas normas.

A distância entre robustez formal e efetividade prática será preenchida pela capacidade fiscalizatória do Estado, superação de resistências jurídicas e investimento em educação digital. O diploma é, sem dúvida, marco legislativo esperançoso, mas sua consolidação como ferramenta efetiva de proteção constitui desafio que será analisado, sob ótica da responsabilidade dos atores, no próximo capítulo.

---

[105] GOMES, J. C. L. da C.; MEDRADO, L. C.; GAMA, G. B. A. C. R. N. **Crimes cibernéticos**: desafios jurídicos no processo e julgamento de infrações penais virtuais cometidas por agentes estrangeiros contra vítimas brasileiras. **Revista JRG de Estudos Acadêmicos**, São Paulo, v. 7, n. 15, p. e151563, 2024. DOI: 10.55892/jrg.v7i15.1563. p. 15.

[106] ECA Digital e IA: **Limites jurídicos para a infância conectada**. Migalhas, [S.l.], 2025. Disponível em: https://www.migalhas.com.br/depeso/443309/eca-digital-e-ia-limites-juridicos-para-a-infancia-conectada . Acesso em: 1 nov. 2025.

CAPÍTULO 3 A ARQUITETURA DA NEGLIGÊNCIA: O COLAPSO SISTÊMICO DA PROTEÇÃO

A violência sexual digital contra crianças e adolescentes não pode ser compreendida como uma sucessão de episódios isolados ou como simples falhas tecnológicas. Ela emerge de condições estruturais que permitem sua reprodução contínua no ambiente online, revelando um cenário em que fatores técnicos, sociais e institucionais se combinam para manter o risco sempre presente.

Trata-se de um arranjo estrutural em que cada agente – pela omissão ou pela ação – alimenta a negligência do outro, criando um ciclo no qual o abuso, a exploração e a adultização infantil se tornam fenômenos previsíveis, não excepcionais. A negligência estatal em relação às denúncias realizadas contra abuso sexual infantil revela que o ciclo não consiste em erros procedimentais corrigíveis, mas em vácuos sistêmicos que se reforçam mutuamente.

3.1 O conceito de arquitetura da negligência

A noção de “arquitetura da negligência” parte de uma premissa crítica: negligência não é simples ausência de ação, mas estrutura relacional na qual cada ponto de falha depende e alimenta os demais. Essa arquitetura não advém com o fenômeno das plataformas digitais, é algo enraizado. E nesse momento, crianças precisam conviver com os crimes que já existiam e agora os cibernéticos. Analisando o contexto da arquitetura da negligencia fora do espectro digital, o caso paradigmático de Eva Luana exemplifica essa dinâmica: aos 13 anos, ela formalizou denúncia contra seu padrasto em delegacia, mas “houve uma falha por parte do Estado em não prosseguir com as investigações, tanto que o Ministério Público não tomou conhecimento do caso, e após sofrer muitas ameaças de seu agressor, ela se viu

obrigada a retirar a queixa”[107]. Esse processo perdurou oito anos de abuso contínuo, não pelos méritos do crime, mas pela desarticulação pura da rede de proteção.

A revelação é, conforme Faleiros sistematiza, “o primeiro e decisivo passo, no qual a vítima conta para alguém sobre a violência que sofria ou que vem sofrendo”[108]. Mas a simples revelação não garante proteção. A informação pode ficar “restrita à família ou se tornar pública por meio da notificação, que se refere ao momento no qual a vítima, ou a pessoa para quem o abuso foi revelado, a qual poderá se dirigir ao Conselho Tutelar ou à delegacia para fazer a comunicação da violência ou o boletim de ocorrência”[109]. Nesse intervalo entre a revelação, a notificação e a resposta institucional, reside o espaço de negligência.

As autoras ainda trazem que a comunicação da violência deveria gerar intervenções de diferentes instituições e de diferentes profissionais, cujo objetivo deve – ou deveria - ser proteger a vítima e responsabilizar o abusador[110]. Todavia, tal finalidade esbarra na fragmentação operacional da rede de apoio. Quando não há fluxos de trabalho definidos, a capacidade de resposta do Estado se dilui, tornando a proteção insuficiente diante da complexidade das situações de abuso. Essa falha de articulação não é contingente; é estrutural. O Estado não investiu em protocolos internacionais, em capacitação de profissionais, em sistema de informação integrado.

Nesse cenário marcado pela revitimização contínua, a violência digital contra crianças e adolescentes se articula a novas modalidades de abuso, revelando aquilo que se pode denominar de “arquitetura da negligência” sistêmica.

Trata-se de um arranjo em que a omissão não resulta de falhas pontuais, mas da atuação simultaneamente insuficiente do Estado, das plataformas digitais e da

---

[107] PEREIRA, Débora Thais dos Santos *et al*. Negligência do Estado em relação às denúncias realizadas contra abuso sexual infantil. **Revista REASE**, v. 8, n. 10, p. 1344, 2022. Caso referenciado em: UNIVERSA. **Ela foi abusada e torturada pelo padrasto por 9 anos**. UOL, 21 fev. 2019. Disponível em: https://www.uol.com.br/universa/noticias/redacao/2019/02/21/ela-foi-abusada-e-torturada-pelo-padrasto-por-9-anos-nao-vivi-sobrevivi.htm. Acesso em: out. 2025.

[108] FALEIROS, Eva. **Abuso sexual contra crianças e adolescentes:** os (des)caminhos da denúncia. Brasília: Presidência da República, Secretaria Especial dos Direitos Humanos, 2003.

[109] PEREIRA, Débora Thais dos Santos; SANTOS, Jessica Lara dos Santos; MACENA, Cláudia Waléria Carvalho Mendes. Negligência do Estado em relação às denúncias realizadas contra abuso sexual infantil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 10, 2022, p. 1350.

[110] *Ibid.,* p. 1350.

própria dinâmica social, que acabam por reforçar, em conjunto, a vulnerabilidade estrutural infantil. Compreender essa lógica é essencial: a negligência não é um acidente do sistema, mas parte de seu próprio funcionamento, no qual cada brecha legitima a seguinte e sustenta um ambiente fértil para a exploração e a violação de direitos.

Segundo o Tribunal de Contas da União, no Acórdão 2515/2025, a atual ausência de políticas integradas e preventivas na proteção digital se traduz em omissão institucional que beira a cumplicidade com o agressor, uma vez que as instituições estatais permanecem fragmentadas e preferem atuar reativamente, apenas após o dano já ter ocorrido. Esse padrão revela um projeto institucional que não reconhece a plenitude do dano digital, generalizando as práticas jurídicas e preventivas do mundo *offline* de forma inadequada ao contexto tecnológico[111].

Paralelamente, as plataformas digitais operam sob a lógica da economia da atenção, cuja meta é "gerar desejo e fidelizar consumidores desde cedo", utilizando estratégias que exploram os vieses cognitivos da infância e adolescência[112]. O algoritmo, configurado para maximizar engajamento, selecione conteúdos de maior potencial viral, incluídos material sexual exploratório e discursos que naturalizam a violência.

O que se vislumbra é o lucro e na ótica do "Capitalismo da Vigilância" trazido por Shoshana Zuboff, entende-se que:

> Apesar disso, cada geração pisa em falso na areia movediça do esquecimento de que a tecnologia é uma expressão de outros interesses. Nos tempos modernos, isso significa os interesses do capital, e na nossa

[111] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, pp. 22-27.
[112] BRASIL. Presidência da República. Secretaria de Comunicação Social. **Guia de uso de telas, dispositivos digitais e internet por crianças e adolescentes**. Brasília: SECOM, 2024, p. 35. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Acesso em: 01 nov. 2025.

> época é capital de vigilância que comanda o meio digital e dirige nossa trajetória rumo ao futuro. [113]

Isto é, sustentadas pela venda de tempo e exposição, as plataformas operam sob uma lógica onde o risco é calculado e assumido em nome do lucro, enquanto o passivo social decorrente dessa arquitetura predatória é transferido para o Estado e para as famílias. A opacidade algorítmica dificulta a responsabilização e transforma o abuso em uma externalidade estrutural normalizada.

Na esfera familiar e social, a negligência assume formas distintas, mas igualmente graves. A parentalidade digital distraída, em que pais e responsáveis estão exaustos, sem letramento digital, ou envolvidos no fenômeno do *sharenting*, expõe as crianças a um abandono afetivo e tecnológico que reforça o ciclo da exploração digital. Pesquisa recente apresenta que o mito do “nativo digital” ignora o fato de que crianças, mesmo nascidas na era digital, não possuem ferramentas cognitivas maduras para navegar de forma crítica e segura no ambiente online[114].

Essa tríade, ao operar de forma concatenada, cria uma arquitetura perversa: o Estado não atua preventivamente, as plataformas desenham risco para maximizar lucro, e a família não dispõe dos recursos ou conhecimento para fazer a mediação necessária, fazendo da infância digital um território vulnerável e explorável. Esse sistema não é acidental; é um projeto funcional cuja prioridade do lucro e da inércia institucional prioriza a ilusão da proteção enquanto perpetua o dano.

3.2 Negligência Estatal: lei sem *enforcement* e políticas sem orçamento

A atuação do Estado na proteção de crianças e adolescentes no ambiente digital revela fragilidades que não decorrem da inexistência de normas, mas da

[113] ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021, p. 28.
[114] COELHO, Gabi. **Nativos digitais ou crianças desprotegidas na internet?** Lunetas, São Paulo, 28 jul. 2025. Disponível em: https://lunetas.com.br/nativos-digitais-ou-criancas-desprotegidas-na-internet/. Acesso em: 10 set. 2025.

incapacidade de torná-las operacionais no cotidiano. Este trecho da pesquisa examina o descompasso entre o discurso institucional que coloca a infância como prioridade e a prática governamental, marcada por limitações administrativas e financeiras que comprometem a execução de políticas de segurança digital.

Defende-se que a insuficiência estatal se expressa tanto na baixa capacidade de fiscalização quanto na interrupção recorrente de iniciativas preventivas. Assim, embora o marco jurídico brasileiro apresente avanços relevantes, sua aplicação concreta permanece limitada. A análise demonstra que a falta de equipes especializadas e de recursos destinados exclusivamente à proteção online transforma o compromisso constitucional em uma diretriz que raramente se materializa, deixando crianças e adolescentes expostos à crescente complexidade das ameaças digitais.

3.2.1 O paradoxo normativo: consolidação jurídica e inércia prática

O Brasil dispõe de arcabouço normativo robusto: Constituição Federal (art. 227), Estatuto da Criança e do Adolescente (Lei 8.069/1990), Marco Civil da Internet (Lei 12.965/2014), LGPD (Lei 13.709/2018) e Lei 14.811/2024. Apesar dessa consolidação, os dados revelam o oposto: a epidemia de crimes sexuais contra crianças.

A materialidade da negligência estatal revela-se de forma brutal nas estatísticas criminais, confirmando que a violência sexual não é um desvio esporádico, mas opera com uma centralidade simbólica na lógica de dominação e controle dos corpos. Dados do Anuário Brasileiro de Segurança Pública (2025) apontam que o ano de 2024 atingiu o maior volume de registros desde o início da série histórica em 2011, totalizando 87.545 vítimas de estupro no país. Deste montante, a absoluta fragilidade das vítimas é o vetor predominante: foram 67.204 casos tipificados especificamente como estupro de vulnerável — um número três vezes superior ao estupro comum (art. 213 do CP)

—, evidenciando uma epidemia que cresce continuamente e que já atinge a taxa de 41,2 casos por grupo de 100 mil habitantes[115].

O abuso sexual infantil é “todo envolvimento de uma criança em uma atividade sexual na qual não compreende completamente, já que não está preparada em termos de seu desenvolvimento”[116]. Apesar dessa definição clara, o índice de abuso sexual infantil, no Brasil, ainda é altíssimo, e as estruturas de resposta permanecem fragmentadas e subfinanciadas.

A investigação de crimes contra crianças na internet enfrenta obstáculo crucial: a preservação de logs e metadados digitais. Quando denúncias envolvem crimes cibernéticos (*grooming, sextortion*, compartilhamento de CSAM), a investigação depende de capacidade técnica que delegacias brasileiras raramente possuem. A falta de especialização é crítica: profissionais policiais frequentemente não possuem treinamento contínuo em perícia digital; protocolos de preservação de provas são inexistentes ou desconhecidos. O resultado: evidências digitais se perdem antes de qualquer diligência; investigações são paralisadas pela falta de expertise.

Essa inércia técnica não é remediável por treinamento episódico. Exige investimento estrutural em infraestrutura: núcleos de perícia digital, laboratórios forenses, equipes especializadas.

3.2.2 Revitimização institucional: o segundo abuso

A criança que teve coragem de denunciar é obrigada a: **(1)** relatar o abuso múltiplas vezes (para delegacia, psicólogo, juiz); **(2)** enfrentar contraditório processual que questiona sua credibilidade; **(3)** testemunhar em juízo diante do agressor; **(4)** lidar com morosidade processual que estende o trauma por anos.

---

[115] FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2025**. São Paulo: FBSP, 2025, p. 178-179. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025.pdf. Acesso em: 19 nov. 2025.

[116] MOURA, Andreina. **Alguns aspectos sobre o abuso sexual contra crianças**. Curitiba: Ministério Público do Estado do Paraná, [20--?]. Disponível em: https://site.mppr.mp.br/crianca/Pagina/Alguns-aspectos-sobre-o-abuso-sexual-contra-criancas. Acesso em: 01 nov. 2025.

A inércia social diante da violência é reforçada por barreiras culturais que minimizam o sofrimento infantil. Conforme destaca Rangel (2001) *apud* Cardoso e Santos (2021), as concepções sobre a infância ainda são impregnadas pela falsa percepção de que a "criança não sabe de nada" e não carregará lembranças do ocorrido. A autora denuncia que o esquecer torna-se a palavra-chave de uma reação defensiva dos adultos, que preferem negar a gravidade do abuso a enfrentar suas consequências traumáticas, perpetuando a desproteção sob o manto da ignorância fingida[117].

A revitimização institucional representa uma das dinâmicas mais perversas da violência contra crianças e adolescentes, especialmente quando estas são vítimas de abusos digitais. Segundo Pereira *et al*., "há, no Brasil, um processo de revitimização das crianças e adolescentes vítimas de abusos, especialmente em virtude da incapacitação profissional"[118]. Tal incapacitação acontece não apenas pela ausência de protocolos formativos, mas fundamentalmente pela falta de preparo dos profissionais para lidar com as especificidades do ambiente digital, onde o abuso ocorre em redes sociais, aplicativos de mensagem ou plataformas de jogos, muitas vezes, sem marcas físicas, o que dificulta o reconhecimento do sofrimento.

O processo de proteção deveria operar em regime integrado e multidisciplinar. Entretanto, as autoras são enfáticas: "ainda que exista essas previsões legais e se trate de garantias profissionais, está longe de ser a realidade" [119]. Os encaminhamentos previstos pela rede (Conselho Tutelar, Ministério Público, Delegacia Especializada, Escola, Saúde) são seriamente prejudicados pela carência de rotinas e fluxos de trabalho coerentes.

Esse ciclo fragmentado impõe à vítima sucessivos testemunhos do mesmo fato, em ambientes muitas vezes hostis, com profissionais sem treinamento específico para

---

[117] RANGEL, Patrícia Calmon. **Abuso sexual intrafamiliar recorrente**. Curitiba: Juruá, 2001. apud CARDOSO, Fernanda Costa; SANTOS, Kátia Paulino dos. Violência sexual infantil e os mecanismos de inibição adotados por escola pública da comunidade Ribeirinha da Ilha de Santana - Amapá. **Brazilian Journal of Development**, Curitiba, v. 7, n. 2, p. 15829, 2021.

[118] PEREIRA, Débora Thais dos Santos; SANTOS, Jessica Lara dos Santos; MACENA, Cláudia Waléria Carvalho Mendes. Negligência do Estado em relação às denúncias realizadas contra abuso sexual infantil. **Revista REASE**, v. 8, n. 10, out. 2022, p. 1351.

[119] *Ibid*., p. 1355.

abordagem digital ou para tecnologias de prova, e frequentemente exposta ao contraditório processual. A demora na resposta estatal e a exigência da produção de provas digitais que requerem expertise técnica ainda rara, agravam o sofrimento inicial e transformam o sistema de justiça em palco do segundo abuso.

A subnotificação também é consequência direta desse contexto. Conforme indicam as autoras, “a maioria dos casos envolvendo crianças e adolescentes dificilmente é relatada devido a vergonha, ignorância, sentimento de culpa, além desses fatores, alguns profissionais relutam em reconhecer e relatar o abuso sexual”[120]. No espectro da violência digital, esse quadro se intensifica: crianças e adolescentes raramente possuem vocabulário ou referência para nomear experiências online abusivas (grooming, sextorsão, linchamento virtual) como crimes, sentem vergonha ou medo de retaliações dos pais, e enfrentam um sistema que desconfia do depoimento infantil.

Em síntese, a revitimização é produzida e reproduzida por mecanismos institucionais e culturais: desde o despreparo para acolher e escutar até a incapacidade para preservar provas digitais e romper o ciclo do silêncio e da subnotificação. Esta lógica faz do ambiente digital não um espaço de emancipação, mas de vulnerabilização institucionalizada, onde a vítima é obrigada a narrar repetidamente sua dor, sem que a rede produza, de fato, proteção e responsabilização eficientes.

3.3 Negligência corporativa: o lucro pelo risco e a violação do dever de cuidado

O segundo pilar da arquitetura da negligência reside na esfera corporativa, onde o modelo de negócio das plataformas digitais é intrinsicamente fundado na assunção calculada de risco. Esta seção demonstra como a opção por maximizar o

[120] FALEIROS, Vicente de Paula. **A violência sexual contra crianças e adolescentes: a proteção social como missão.** São Paulo: Cortez, 2001. apud NEVES NETO, Wilmar Ferreira et al. Violência sexual infantil: estratégias extensionistas de prevenção e enfrentamento no contexto escolar. In: COLÓQUIO ESTADUAL DE PESQUISA MULTIDISCIPLINAR, 5., 2021, Mineiros. Anais [...]. Mineiros: Unifimes, 2021, pp. 7-8.

engajamento e o lucro, em detrimento da segurança do usuário, configura uma violação flagrante do dever de cuidado – um princípio jurídico basilar que impõe a obrigação de agir com a diligência de uma pessoa prudente para evitar danos previsíveis.

A dignidade da pessoa humana, pedra basilar constitucional (art. 1º, III, CF), exige que o ser humano jamais seja tratado como meio para fins alheios. Nesse sentido, Taquary (2007) adverte que a coisificação do ser humano, especialmente dos grupos vulneráveis, representa a violação máxima dessa dignidade. Ao analisar a proteção internacional e interna, a autora destaca que "a dignidade da pessoa humana é o valor que dá unidade e coerência ao sistema jurídico", sendo inadmissível qualquer prática que reduza a criança a objeto de comércio ou exploração[121].

Quando plataformas tratam a atenção infantil como *commodity* e seus dados como insumo para publicidade comportamental, viola-se a dignidade desse sujeito em formação. A vulnerabilidade digital não é apenas técnica (não saber usar a ferramenta), mas cognitiva e emocional. Algoritmos desenhados para viciar exploram a imaturidade do córtex pré-frontal, incapaz de frear impulsos ou avaliar consequências de longo prazo da exposição de dados.

3.3.1 A economia da atenção e o design para engajamento

As plataformas digitais estruturam tecnicamente a experiência do usuário para maximizar tempo de permanência, captura de dados e receita publicitária – indiferente aos custos sociais. A “economia da atenção” segundo Nogaro, Anzolin e Provenzi, funciona assim:

> O mercado está alerta e já possui estratégias de como gerar desejo, vender e obter lucros com a economia da atenção, isto é, com vigoroso apelo ao

[121] TAQUARY, Eneida Orbage de Britto; TAQUARY, Catharina Orbage de Britto. **Comércio de seres humanos:** a influência da Convenção de Palermo sobre o novo modelo de Lei Penal brasileira. **Revista Jurídica**, Brasília, v. 9, n. 88, 2007, p. 4-5.

> visual e ao desejo, em um ambiente no qual crianças e jovens estão navegando. A lógica é atrair consumidores e fidelizá-los desde cedo.[122]

Percebe-se que não é uma mera estratégia de mercado, mas a base operacional de um modelo de negócio que instrumentaliza a psicologia humana. As plataformas estruturam tecnicamente a experiência do usuário para maximizar o tempo de permanência, a captura de dados e a receita publicitária, sendo indiferentes aos custos sociais externalizados[123].

Essa estratégia é incorporada em cada decisão de *design*: *feeds* infinitos que criam compulsão por *scroll* (deslize de tela); algoritmos de recomendação que promovem conteúdo sensacionalista (incluindo conteúdo sexual); notificações intermitentes que funcionam como reforço operante; mecanismos de gamificação que estimulam performance narcísica. Para adolescentes cujos cérebros ainda estão em desenvolvimento (particularmente a região pré-frontal, responsável por avaliação de risco), essas estratégias são especialmente predatórias[124].

3.3.2 Safety by Design: o padrão que não é implementado

Em contraposição ao modelo predatório, o paradigma do *Safety by Design* (Segurança desde a Concepção) emerge como um padrão técnico-jurídico necessário, porém sistematicamente negligenciado. Este princípio exige que a segurança e o interesse do usuário sejam incorporados na própria arquitetura do produto, e não tratados como uma medida reativa ou opcional. Isso se traduziria em configurações de privacidade e segurança ativadas por padrão no nível mais forte,

---

[122] NOGARO, A.; ANZOLIN, M. G.; PROVENZI, N. A. A economia da atenção e a fidelização de consumidores na era digital. **Revista Pedagógica**, [S. l.], v. 27, p. e8027, 2025. DOI: 10.22196/rp.v27i1.8027. Disponível em: https://bell.unochapeco.edu.br/revistas/index.php/pedagogica/article/view/8027. Acesso em: 12 nov. 2025.

[123] FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes:** parecer. São Paulo: Instituto Alana, 2020, p. 30.

[124] COSTELLO, Nancy et al. Algorithms, addiction, and adolescent mental health: an interdisciplinary study to inform state-level policy action to protect youth from the dangers of social media. **American Journal of Law & Medicine**, [S. l.], v. 49, n. 2-3, p. 135–172, 2023. DOI: 10.1017/amj.2023.25. p. 146.

transparência sobre o funcionamento dos algoritmos de recomendação e controle efetivo do usuário sobre suas próprias experiências.

A *Brookings Institution* argumenta que as plataformas notoriamente aplicaram esse conceito ao design de seus produtos para criar aplicativos que mantêm os usuários engajados, independentemente dos benefícios ou malefícios de sua experiência. Os mecanismos são conhecidos como "*dark patterns*" – designs que exploram vieses cognitivos humanos. Exemplos incluem *autoplay* de vídeos (que não permite pausa deliberada), notificações obsessivas, feeds algoritmicamente personalizados[125]. As plataformas oferecem proteções opcionais (frequentemente enterradas em configurações desconhecidas) e mantém algoritmos proprietários que continuam a recomendar conteúdo prejudicial.

A omissão em implementar o *Safety by Design* como política padrão não é uma falha técnica, mas uma escolha estratégica de negócio. Oferecer proteções opcionais e soterradas em menus complexos é a materialização da negligência, transferindo para o usuário – muitas vezes uma criança – o ônus de sua própria proteção em um ambiente hostil arquitetado pela própria plataforma.

3.3.3 Opacidade algorítmica e recomendação de CSAM (Material de Abuso Sexual Infantil)

Um indicador crucial da negligência corporativa é o volume crescente de denúncias de material de abuso sexual infantil (CSAM). A SaferNet Brasil registrou em 2025 aumento significativo: denúncias de abuso e exploração sexual representam 64% dos casos reportados, com crescimento de 102% em relação ao período anterior[126]. Esse crescimento não indica mero aumento em crimes; indica que

[125] PERRINO, John. **Using 'safety by design' to address online harms**. Brookings Institution, 26 jul. 2022. Disponível em: https://www.brookings.edu/articles/using-safety-by-design-to-address-online-harms/. Acesso em: 13 nov. 2025.
[126] SAFERNET BRASIL. **Nota Técnica 02/2025:** Aumento de denúncias e uso de inteligência artificial. Salvador: SaferNet Brasil, 2025, p.2

plataformas falharam em implementar sistemas robustos de detecção e não priorizaram remoção antes de alcançar escala de distribuição massiva.

De janeiro a junho de 2024, a SaferNet Brasil recebeu 874 denúncias de URLs relacionadas a crimes de abuso e exploração sexual infantil no Telegram, das quais 149 estavam ativas. Esse número não representa uma amostra isolada, mas evidencia um padrão: das 149 URLs ativas analisadas, 41 (27,5%) continham palavras-chave, termos, acrônimos, hashtags, emojis e informações relevantes na indexação, compartilhamento e comercialização de CSAM. Das 40 URLs adicionalmente verificadas, 30 (75%) continham material explícito[127].

A arquitetura permissiva e a negligência corporativa estrutural são evidenciadas, principalmente, em plataformas como *Telegram,* que opera como uma plataforma híbrida, que reúne mensagens privadas, comunicação em grandes grupos e mecanismos de difusão massiva. Seus grupos comportam até 200 mil membros, enquanto os canais admitem inscritos ilimitados e funcionam como fluxos unidirecionais de conteúdo, nos quais apenas administradores publicam e o público, em regra, apenas visualiza ou reage às postagens.

Essas características técnicas, embora legítimas em contextos de proteção de dissidentes e minorias, criaram um ecossistema ideal para circulação de CSAM. A maioria dos grupos e canais denunciados à SaferNet estava em idiomas além do português, como inglês e espanhol, o que reflete a globalização e a interconexão da internet, que permitem a disseminação de conteúdo em diferentes idiomas.[128]

A distribuição linguística revela algo crucial, a criminalização não é localizada, mas sistêmica:

> Entre 41 URLs que continham palavras-chave e outros termos associados à distribuição e comercialização de material de exploração sexual infantil, 26 tiveram seu número de membros (no caso de grupos) ou inscritos (no caso de canais) mapeados. A média total de participantes após essa coleta de

[127] SAFERNET BRASIL. **Relatório:** On Their Own Words - How Telegram has been used in Brazil as a marketplace for sexual abuse offenders. Salvador: SaferNet Brasil, 2024, p. 7.
[128] *Ibid*., p. 7.

> dados foi de 32.478, com a maior comunidade tendo mais de 200 mil participantes e a menor 23.[129]

Para além disso, um dos elementos mais graves da negligência das plataformas é a forma como seus sistemas de pagamento acabam permitindo — direta ou indiretamente — a comercialização de material de abuso sexual infantil (CSAM). No caso do Telegram, há amplo registro de uso da plataforma para esse tipo de atividade ilícita, viabilizada por diferentes mecanismos de transação, como criptomoedas, transferências instantâneas realizadas pelos próprios usuários e ferramentas automatizadas de pagamento integradas ao serviço.

Um desenvolvimento especialmente inquietante é o uso de inteligência artificial para gerar CSAM sinteticamente:

> O mapeamento de palavras-chave identificou três termos, entre 190, que se referem ao uso da inteligência artificial na geração de conteúdo sexual infantil: 'deepnudes', 'deepcum' e 'deepaudio'. A SaferNet não testou a criação de materiais ilegais, mas ao iniciar a interação com robôs que produzem e vendem conteúdo desse tipo, foi possível observar que eles afirmam ser capazes de 'nudificar' imagens, ou seja, remover as roupas com inteligência artificial.[130]

O *Internet Watch Foundation* (IWF), em relatório de julho de 2024, documenta uma escalada alarmante: o volume de imagens e vídeos de abuso infantil gerados artificialmente e disseminados na *dark web* cresceu 17% em relação ao semestre anterior, com conteúdos cada vez mais explícitos e realistas. Nesse período, foram identificadas mais de 2,5 mil pseudo-fotografias com potencial enquadramento criminal, além de outras quatro centenas classificadas como material proibido[131].

---

[129] *Ibid*., p. 7.
[130] *Ibid*., p. 12.
[131] INTERNET WATCH FOUNDATION. **How AI is being abused to create child sexual abuse imagery**. July 2024 Report. Disponível em: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/. Acesso em: 2 nov. 2025.

A gravidade do problema é ainda maior do que aparenta. Relatórios internacionais já indicam que vídeos sintéticos de abuso sexual infantil, produzidos por inteligência artificial, tendem a tornar-se comuns, com níveis crescentes de realismo e disseminação[132]. Esse cenário implica não apenas a expansão exponencial do volume de material disponível, mas também a transformação qualitativa da própria violência: vítimas reais podem ter sua imagem digitalmente reproduzida de forma indefinida, inseridas em novos contextos de abuso sem qualquer participação ou consentimento, perpetuando e ampliando sua vitimização.

A análise desenvolvida ao longo deste tópico evidencia que a opacidade algorítmica e determinadas práticas de governança corporativa não representam meras falhas contingenciais, mas integram um modelo estrutural que dificulta a responsabilização e fragiliza a proteção de crianças e adolescentes no ambiente digital.

No caso do *Telegram*, esse quadro torna-se particularmente visível na ausência de mecanismos eficazes de detecção e remoção proativa de material de abuso sexual infantil, no uso combinado de anonimato e criptografia que limita a rastreabilidade de agentes ilícitos, na integração de sistemas de pagamento suscetíveis à instrumentalização criminosa e na disponibilização de ferramentas automatizadas e de inteligência artificial sem salvaguardas adequadas para impedir usos abusivos. A falta de relatórios públicos de transparência e a resistência à cooperação institucional reforçam esse cenário, acentuado pela inexistência de políticas específicas de enfrentamento a CSAM comparáveis às adotadas por outras plataformas de grande escala.

Sob a perspectiva jurídica, embora o arcabouço normativo brasileiro contenha previsões relevantes, sua efetividade é limitada por dificuldades de fiscalização, pela falta de coordenação entre órgãos competentes e pela incapacidade de acomodar adequadamente práticas associadas a tecnologias emergentes, como *deepfakes*, agentes automatizados e meios de pagamento digitais. Soma-se a isso a insuficiência

[132] INTERNET WATCH FOUNDATION, op. cit.

de mecanismos sancionatórios capazes de produzir incentivos econômicos reais para o cumprimento das normas pelas plataformas.

Essa combinação de fatores revela um descompasso persistente entre o desenho legal e a responsabilização prática, resultando na manutenção de um ambiente em que crianças e adolescentes permanecem expostos a riscos significativos, inclusive à perpetuação digital de abusos por meio de conteúdos sintéticos que prolongam sua vitimização no tempo.

3.4 Negligência social e familiar: entre a omissão e a incapacidade estrutural

A terceira dimensão da arquitetura da negligência transcende a esfera individual da culpa parental e revela uma patologia social mais profunda: a incapacidade coletiva de mediar a relação entre infância e tecnologia. Não se trata apenas de "pais que não vigiam", mas de uma sociedade que normalizou o abandono digital como subproduto inevitável da modernidade, ignorando que o vácuo de autoridade deixado pela família e pela escola é imediatamente preenchido por algoritmos de radicalização e predadores sexuais.

Sobre o regime jurídico de proteção à infância, observa-se que:

> A Doutrina da Proteção Integral, estabelecida pelo artigo 227 da Constituição Federal de 1988 e pelos artigos 3º e 4º do Estatuto da Criança e do Adolescente (ECA), determina que, por estarem em condição peculiar de desenvolvimento, crianças e adolescentes devem ter seus direitos garantidos com absoluta prioridade em todas as áreas e que a proteção dessa população e o zelo pela efetivação de seus direitos é uma responsabilidade compartilhada e um dever de todos: famílias, Estado e sociedade.
>
> A proteção integral assegura não só os direitos fundamentais conferidos a todas as pessoas, mas também aqueles que atentam às especificidades da infância e da adolescência. Hoje, tanto crianças quanto adolescentes, têm

> poder de voz, são cidadãs e têm o direito de serem respeitadas como os adultos e protegidas por eles.[133]

A negligência social e familiar no contexto da violência digital contra crianças não é fenômeno caótico ou marginal, mas estrutura funcional de um arranjo em que responsabilidades se dissolvem entre múltiplos agentes através de mecanismos de dispersão de culpa. O Estado cria vácuos regulatórios; as plataformas exploram esses vácuos para lucro; a sociedade consome conteúdo exploratório sem questionar cumplicidade; e, finalmente, responsabiliza-se apenas os pais, frequentemente, os únicos atores sem poder real de transformação sistêmica. Essa estrutura de negligência é, portanto, não acidental, mas arquitetada.

3.4.1 O abandono digital e a negligência invisível: crítica às assimetrias estruturais

O termo “abandono digital” foi cunhado juridicamente e configura-se “pela omissão e desatenção dos pais quanto à segurança dos filhos no ambiente virtual. Há um descaso quanto ao monitoramento do conteúdo, uma falta de interesse em saber com quem interagem e, também desatenção quanto ao uso excessivo”[134]. Crucialmente, não se refere apenas a mera permissão de acesso a telas, mas de delegação ativa das funções de cuidado e proteção para dispositivos eletrônicos, transformando a tecnologia em substituto do afeto parental e da mediação responsável.

Sob perspectiva jurídica estruturada, Lima, Fernandes e Pedrosa (2023) documentam que:

---

[133] INSTITUTO ALANA. **Proteção integral.** São Paulo, 2025. Disponível em: https://alana.org.br/glossario/protecao-integral/. Acesso: 3 nov. 2025.

[134] KLUNCK, Patrícia; AZAMBUJA, Maria Regina Fay de. **O abandono digital de crianças e adolescentes e suas implicações jurídicas**. Porto Alegre: PUCRS, p. 2. Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2020/04/patricia_klunck.pdf. Acesso em: 12 nov. 2025.

> Com essa facilitação a internet, muitos não tem filtro do que podem assistir ou postar. Por falta de instrução muitas vezes, o celular é como qualquer outro aparelho e deve ser ensinado ao menor como usar, não de maneira literal, mas sim quais aplicativos ele ou ela pode acessar, que filmes pode assistir, com quem se deve falar ou quais fotos, vídeos se pode postar.[135]

Para além disso, observa-se que a rotina exaustiva enfrentada por grande parte dos pais e cuidadores, marcada por longas jornadas de trabalho e deslocamentos demorados, frequentemente, limita sua capacidade de acompanhar de perto o uso que crianças e adolescentes fazem das redes sociais, o que ajuda a explicar, em certa medida, a dificuldade de exercer uma supervisão contínua no ambiente digital.

A questão de classe social é central. Conforme explicitam Klunck e Azambuja (2019):

> muitos delegam à internet a função de entreter e acalmar seus filhos, sendo esta, inclusive, chamada por alguns estudiosos do assunto como ‘chupeta digital’ ou ‘babá digital’. As crianças e adolescentes passam horas tendo como melhor companhia um tablet, um computador ou um smartphone. [136]

Nesse sentido, essa prática tem-se pelo fenômeno denominado "parentalidade distraída" (*phubbing parental*) que afeta transversalmente todas as classes sociais, porém com consequências distintamente assimétricas. O discurso hegemônico sobre negligência parental frequentemente opera uma seletividade perversa ao criminalizar padrões de cuidado das famílias periféricas enquanto naturaliza modalidades equivalentes de omissão nas classes economicamente privilegiadas[137].

---

[135] LIMA, Francisco Zamourano Silva de; FERNANDES, Maria Allice Dantas; PEDROSA, Eduarda Shirley Fernandes de Oliveira Vale. **A prática dos crimes cibernéticos como violação dos direitos da criança e do adolescente**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Potiguar, Natal, 2023, p. 3.

[136] KLUNCK, Patrícia; AZAMBUJA, Maria Regina Fay de. **O abandono digital de crianças e adolescentes e suas implicações jurídicas**. Âmbito Jurídico, Rio Grande, 2019, p. 5.

[137] MARUCO, Fábia de Oliveira Rodrigues; RAMPAZZO, Lino. O abandono digital de incapaz e os impactos nocivos pela falta do dever de vigilância parental. **Revista de Direito de Família e Sucessão**, v. 6, n. 1, pp. 10-11, 2020.

O problema, porém, revela desigualdades ainda mais profundas. A distinção central manifesta-se nos recursos disponíveis para a reparação dos danos: enquanto famílias com maior poder aquisitivo conseguem acessar psicólogos, psicopedagogos e acompanhamento especializado, aquelas em situação de vulnerabilidade acumulam o peso da responsabilização social e a limitação material que as impede de enfrentar adequadamente as consequências desenvolvimentais decorrentes da negligência.

Importa esclarecer que a presente análise não busca esvaziar a responsabilidade dos pais e cuidadores na proteção digital de crianças e adolescentes, mas evitar que essa responsabilização seja aplicada de forma acrítica, homogênea e revitimizadora. Famílias que não dispõem de alfabetização digital adequada, nem dos meios materiais para exercer plenamente a vigilância exigida pelo ordenamento, não podem ser tratadas como igualmente culpáveis frente a um sistema que falha em prover mecanismos acessíveis de prevenção e apoio.

3.4.2 O mito do "nativo digital" e analfabetismo digital parental

A raiz profunda da negligência não é culpa moral, mas incapacidade estrutural decorrente de analfabetismo digital massivo que atravessa a sociedade brasileira.

O debate público costuma tratar a negligência digital como resultado apenas da vontade ou do descuido dos responsáveis, desconsiderando que, para milhões de famílias, as próprias condições materiais tornam a supervisão efetiva no ambiente digital praticamente inviável.

A pesquisa de Sousa *et al*. demonstra empiricamente que a maioria dos pais brasileiros não possui competência técnica mínima (analfabetismo digital) para exercer mediação qualificada no ambiente virtual, desconhecendo ferramentas de controle parental, configurações de privacidade e mecanismos de denúncia. Os autores concluem que "nossas descobertas revelam uma lacuna significativa entre o conhecimento autodeclarado e o real, indicando que muitos responsáveis podem não

estar totalmente preparados para cumprir as responsabilidades de privacidade previstas pela legislação".[138]

Esta incapacidade técnica intersecta-se com a exaustão laboral proveniente de jornadas extensas e precarizadas, que consomem o tempo e a energia psíquica necessários para um acompanhamento consistente.

Um dos mitos mais danosos é que crianças nascidas em contexto de onipresença digital ("nativos digitais") possuem competência inata para navegar ambientes online de forma segura e crítica. Essa crença é contraditada por evidência robusta. A pesquisa documentada pelo Senado Notícias descreve:

> Supõe-se que as crianças se movem no mundo digital de forma saudável, segura e crítica porque nasceram na era da internet e usam o computador, o celular e o tablet com desenvoltura. Pesquisas mostram que isso não é verdade. Como crianças, é natural que ainda não tenham maturidade e discernimento para perceber, entender e evitar ameaças[139].

O desenvolvimento cerebral, particularmente em regiões responsáveis por avaliação de risco (córtex pré-frontal), não se completa até o final da adolescência. Crianças são, portanto, neurobiologicamente desprovidas de ferramentas cognitivas para: **(a)** compreender estratégias de persuasão algorítmica; **(b)** avaliar risco de contato com adultos predadores; **(c)** resistir a pressão para compartilhamento de imagens sensíveis; **(d)** reconhecer manipulação emocional[140].

Concomitantemente, famílias enfrentam analfabetismo digital profundo. Pais que trabalham duplas ou triplas jornadas para sobreviver, frequentemente sem acesso à educação continuada sobre tecnologia, não dispõem de tempo, energia ou

---

[138] SOUSA, Mykaele F. A. et al. **Avaliação da Competência Parental na Gestão da Privacidade dos Filhos em Ambientes Digitais**. In: SIMPÓSIO BRASILEIRO DE CIBERSEGURANÇA (SBSEG), 25., 2025, Foz do Iguaçu. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025, pp. 12-14.
[139] SENADO NOTÍCIAS. Mundo digital esconde perigos para as crianças: saiba como protegê-las. Brasília, 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/09/mundo-digital-esconde-perigos-para-as-criancas-saiba-como-protege-las. Acesso em: 2 nov. 2025.
[140]BBC NEWS BRASIL. **Por que o cérebro dos adolescentes é particularmente vulnerável ao uso excessivo de redes sociais e jogos digitais**. 24 mar. 2022. Disponível em: https://www.bbc.com/portuguese/geral-60853962. Acesso em: 5 nov. 2025.

conhecimento para monitorar cada movimento digital de seus filhos. Essa incapacidade não é falha moral, mas estrutural: resultado de um Estado que não educou, não capacitou, não supervisionou.

Frazão articula com precisão que:

> Crianças e adolescentes são ainda mais vulneráveis nessas relações marcadas pela enorme assimetria de poder por serem pessoas em formação, que vivenciam um estágio peculiar de desenvolvimento físico, cognitivo e psicossocial. Necessitam de apoio para se desenvolver de forma sadia e a salvo de todo tipo de violência[141].

Ao mesmo tempo, espera-se que os pais, muitas vezes tão pouco familiarizados com o ambiente digital quanto os próprios filhos, e ainda mais sobrecarregados pelas demandas cotidianas, assumam isoladamente a tarefa de fornecer suporte e vigilância contínua. Trata-se de uma expectativa estruturalmente incompatível com as condições reais enfrentadas pela maioria das famílias.

3.4.3 Negligência intrafamiliar: quando a família é o locus do risco

Estatísticas revelam que a maior parte dos crimes sexuais contra crianças são cometidos por familiares ou conhecidos. De acordo com o MMFDH, em análise de 18.681 registros, “dentre os suspeitos, em 2.617 dos casos estavam o padrasto e a madrasta, 2.443 o pai e em 2.044 denúncias, a mãe era acusada”[142]. A família, longe de ser espaço irrestritamente seguro, é frequentemente o *locus* da violência.

Em contexto digital, essa dinâmica se replica. Pais exploram imagem de filhos para monetização (*sharenting*); parentes compartilham material abusivo em grupos fechados; cuidadores negligenciam supervisão deliberadamente para permitir abuso;

---

[141] FRAZÃO, Ana. **Dever geral de cuidado das plataformas diante de crianças e adolescentes**: parecer. São Paulo: Instituto Alana, 2021, p. 6.

[142] BRASIL. Ministério da Mulher, da Família e dos Direitos Humanos. **Levantamento sobre violência sexual contra crianças e adolescentes**. Disque 100, 2021. Cf. PEREIRA, Débora Thais dos Santos et al. Negligência do Estado em relação às denúncias realizadas contra abuso sexual infantil. **Revista REASE**, v. 8, n. 10, out. 2022, p. 1352-1353.

adolescentes são recrutados por familiares para criação de conteúdo sexualizado[143]. Concomitantemente, “é incontestável que a violência sexual é o delito menos denunciado pelas famílias, sobretudo porque há o medo da dissolução dos núcleos familiares caso o fato seja descoberto”[144].

Pesquisas mostram prevalência massiva: estudo realizado pela OFCOM em 2017 concluiu que “mais de 42% dos pais compartilham imagens dos filhos e, destes, 15% não tomam nenhum cuidado ou consideram os interesses dos filhos“[145]. Outra pesquisa, a “Sensible Sharing” demonstrou que, de modo geral, os pais compartilham aproximadamente cerca de 1.500 imagens dos filhos antes deles alcançarem 5 anos de idade[146].

Porém, conforme documenta Alencar, essa prática evoluiu:

> A exposição de menores em mídias sociais por seus pais pode trazer benefícios a eles, inclusive financeiros. Pois, quando esses perfis ganham popularidade, eles começam a receber propostas para promover determinado serviço ou produto, normalmente por meio de uma publicação em suas redes sociais, mediante uma contrapartida financeira. Dessa forma, a imagem do menor passa a ser comercializada[147].

A autora ainda esclarece que: “as crianças e adolescentes não devem ser consideradas como influenciadoras digitais, pois não são elas que manipulam as suas imagens e as suas presenças digitais. Em verdade, elas têm sua imagem utilizada por seus pais para fins publicitários”[148].

Essa transformação da criança em produto comercial ocorre através do que Alencar identifica como “amadorismo calibrado”, conceito desenvolvido por Abidin que descreve “a criação intencional de uma aparência de autenticidade ou causalidade

---

[143] ALENCAR, Carolina Cavalcante de. **Sharenting Comercial:** A Exposição de Menores em Redes Sociais por seus Pais como Fonte de Renda. Monografia (Bacharelado em Direito) – Universidade do Estado da Bahia, Juazeiro, 2021, p. 11.
[144] PEREIRA *et al.*, *op. cit*., p. 1352.
[145] OFCOM. **Children’s media literacy report**. 2017. *Apud* ALENCAR, *op. cit*., p. 13.
[146] NOMINET. **Sensible Sharing**. 2016. *Apud* ALENCAR, *op. cit.*, p. 13.
[147] ALENCAR, *op. cit*., p. 18.
[148] ALENCAR, *op. cit.*, p. 18

para que um conteúdo voltado e planejado pensando em sua contrapartida financeira seja visto como amador"[149].

Um ponto central nesse debate é a contradição vivenciada por muitos responsáveis, que acabam ocupando posições conflitantes: ao mesmo tempo em que têm o dever de resguardar a identidade digital de seus filhos e agir em seu melhor interesse, também podem ser os principais incentivadores da exposição dessas crianças nas redes, sobretudo quando essa visibilidade se converte em vantagens econômicas.

Ademais, a família não é apenas omissa; em muitos casos, é coautora direta da violência, dados revelam que apesar do ambiente familiar ser considerado um lugar seguro, em 38,9% dos casos de violência sexual, o agressor foi um familiar ou um amigo/conhecido da vítima[150].

Ao contrário do que sugerem as campanhas focadas em ameaças externas, as evidências apontam que o perigo é também doméstico e intrafamiliar. Tal constatação agrava-se quando o próprio lar se torna estúdio de exploração: o *sharenting* comercial, ao converter a intimidade dos filhos em ativo financeiro, subverte o poder familiar e configura abuso de direito, despindo a criança de sua proteção jurídica para vesti-la como objeto de lucro.

Soares e Morais chamam atenção para as implicações jurídicas dessa prática, ao sustentar que a invocação da liberdade de expressão pelos pais para divulgar informações pessoais de seus filhos pode configurar abuso de direito. Nesses casos, a atuação do Ministério Público é legítima e, em situações mais graves, a conduta pode inclusive fundamentar pedido de perda do poder familiar[151].

---

[149] ABIDIN, C. #familygoals: family influencers, calibrated amateurism, and justifying young digital labor. **Social Media + Society**, v. 3, n. 2, p. 1-15, abr. 2017. *Apud* ALENCAR, op. cit., p. 17.

[150] BRASIL. Ministério da Saúde. **Boletim Epidemiológico**, v. 54, n. 8, 2023, p. 4. Disponível em:https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/boletins/epidemiologicos/edicoes/2023/boletim-epidemiologico-volume-54-no-08. Acesso em: 12 nov. de 2025.

[151] SOARES, Rebeca dos Santos; MORAIS, Rosângela Pimentel de. **Abandono digital:** a responsabilidade parental no ambiente virtual. **Revista de Estudos Jurídicos do UNI-RN**, Natal, n. 6, jan./dez. 2022, p. 20

Mariana Mandelli coordenadora da EducaMídia articula a questão essencial sobre perpetuidade:

> Quais os efeitos que esses vídeos terão na socialização dessas crianças e também na vida adulta delas, uma vez que sabemos dos obstáculos infindáveis que as redes impõem ao chamado 'direito ao esquecimento', fazendo com que tais conteúdos estejam sempre atrelados à reputação delas?[152]

A resposta é perturbadora: conteúdo de crianças publicado por pais é frequentemente "apropriado por estranhos e, posteriormente, divulgado em outros locais como sites de pornografia"[153]. Não se trata de pânico moral, mas de fato documentado: a apropriação indesejada de imagens infantis é uma realidade sistêmica. O conteúdo compartilhado pelos pais é frequentemente coletado e redistribuído em ambientes de exploração sexual, convertendo memórias afetivas em insumos para o mercado da pedofilia digital.

Ilustra-se através caso do canal "Bel para Meninas" que destaca de forma paradigmática a metamorfose do registro familiar em exploração laboral. Conforme analisa Teixeira, o que se iniciou como uma atividade lúdica de "penteados" quando a criança tinha apenas seis anos, converteu-se, ao longo de uma década, em um empreendimento comercial onde a intimidade da menor era espetacularizada para milhões de seguidores.

A autora destaca que essa "profissionalização" da infância ocorreu à revelia da capacidade de consentimento da criança, criando um cenário de *sharenting* comercial onde a vida privada foi transformada em ativo financeiro sob a gestão exclusiva dos

---

[152] MANDELLI, Mariana. Caso 'Bel para meninas' e a exposição infantil nas redes. **EducaMídia**, [s.d.]. Disponível em: https://educamidia.org.br/caso-bel-para-meninas-e-a-exposicao-infantil-nas-redes/. Acesso em: 27 out. 2025.

[153] MARUM, Lorena Rodrigues. **Exposição infantil na internet**. In: Direito Digital e seus múltiplos aspectos. *Apud* ALENCAR, *op. cit.*, p. 15.

pais, que utilizavam a narrativa de "brincadeira em família" para mascarar a natureza trabalhista e exaustiva da exposição contínua[154].

A violação de direitos tornou-se palpável no episódio de 2020, que culminou na campanha popular #SalvemBelParaMeninas. Ao examinar o vídeo em que a mãe ridiculariza a escolha de uma mochila pela filha, coagindo-a a aceitar a preferência da audiência, Teixeira identifica uma flagrante violação da dignidade e da autonomia da adolescente em desenvolvimento. Para a autora, tal conduta configura uma "desapropriação de si mesma", na qual a personalidade e os desejos da criança são anulados em favor da "opinião da massa" e da manutenção do engajamento[155].

O caso evidencia, portanto, que no *sharenting* abusivo, o poder familiar é desvirtuado: em vez de proteger, ele instrumentaliza a criança para sustentar um personagem lucrativo.

A exposição massiva promovida pelo caso Bel para Meninas' elucida a vulnerabilidade de crianças entregues à lógica do algoritmo. O risco, contudo, transcende a audiência visível: predadores valem-se de estratégias semióticas discretas para catalogar esse material. Estudos recentes demonstram o uso de “criptolinguagens”, como o emoji do ciclone (🌀), para sinalizar e conectar comunidades que compartilham imagens de crianças com conotação sexual dentro de plataformas da Meta. Assim, o conteúdo produzido pelos pais para entretenimento é rapidamente etiquetado e migrado para bancos de dados na *deep web*, onde a moderação das plataformas, que atua de forma reativa bloqueando hashtags específicas, torna-se inócua diante da velocidade de mutação desses símbolos[156].

Em última análise, a consequência mais insidiosa do *sharenting* não é apenas a exposição imediata, mas a hipoteca da privacidade futura da criança. Minkus, Liu e Ross advertem que o compartilhamento indiscriminado alimenta uma indústria

---

[154] TEIXEIRA, Beatriz Quintas de Melo. **Sharenting e o uso indevido da imagem da criança para fins econômicos**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Presbiteriana Mackenzie, São Paulo, 2023, p. 7-8.
[155] *Ibid*., p. 9.
[156] CÔRTES, T. da S.; MUNARO, L. F. As estratégias dos "novíssimos aliciadores" para difundir material digital pornográfico. **Brazilian Journal of Business**, v. 6, n. 3, 2024, p. 3.

invisível de corretores de dados (*data brokers*), capazes de compilar fragmentos de informações para construir 'mini-perfis' detalhados dos infantes. A gravidade reside na natureza cumulativa desse processo: tais perfis não são estáticos, mas aprimorados continuamente à medida que a criança cresce e sua pegada digital se expande[157].

Assim, a negligência parental converte-se em uma sentença de rastreamento vitalício, entregando à lógica de mercado a autonomia informativa de uma geração que, antes mesmo de aprender a falar, já foi catalogada, perfilada e vendida.

3.4.4 Crimes cibernéticos praticados por menores: quando crianças e adolescentes assumem a posição de agentes da violência

A discussão sobre a tríade da negligência na esfera digital (Estado, sociedade e plataformas digitais) estaria incompleta se ignorasse sua consequência mais alarmante: a formação de agressores. O abandono não produz apenas vítimas passivas; ele forja perpetradores.

A negligência social e Estatal se manifesta na incapacidade de lidar com o adolescente como sujeito de direitos, oscilando entre omissão e punitivismo excessivo. Dados do 2º Boletim Técnico "Escola que Protege" revelam que, em 2024, o Brasil registrou 2.935 ocorrências de bullying e cyberbullying envolvendo vítimas de 0 a 19 anos, sendo 15,7% (460 casos) classificados como cyberbullying — um aumento de 67% em relação a 2023[158].

A resposta estatal, materializada na Lei nº 14.811/2024[159], tipifica o bullying e o cyberbullying como crimes autônomos no Código Penal (art. 146-A). No entanto, a lei estabelece penas distintas: a intimidação sistemática (bullying) é punida com multa,

---

[157] MINKUS, Tehila; LIU, Kelvin; ROSS, Keith W. Children seen but not heard: When parents compromise children's online privacy. In: **Proceedings of the 24th International Conference on World Wide Web.** Florence: ACM, 2015, p. 777.

[158] BRASIL. Ministério da Educação. **2º Boletim Técnico "Escola que Protege":** Dados sobre Bullying e Cyberbullying. Brasília: MEC, 2025, p. 17. Disponível em: https://www.gov.br/mec/pt-br/escola-que-protege/segundo-boletim-tecnico-escola-que-protege.pdf. Acesso em: 9 nov. 2025.

[159] BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência. Diário Oficial da União, Brasília, DF, 15 jan. 2024.

enquanto a intimidação sistemática virtual (cyberbullying) possui pena de reclusão de 1 a 4 anos. É crucial notar que o agravante de pena em dobro para líder de grupo virtual, mencionado no art. 122, § 5º, do CP, refere-se especificamente ao crime de indução ao suicídio, não se aplicando ao crime de cyberbullying.

Paralelamente, a norma atualiza o ECA, impondo medidas socioeducativas para adolescentes autores de atos infracionais análogos e prevendo a responsabilização civil dos pais por omissão. Apesar do avanço, a lei revela limitações críticas, como a técnica legislativa considerada vaga e o questionamento sobre sua efetividade, dado que a maior parte dos casos envolve adolescentes inimputáveis, para os quais a resposta penal tradicional é inaplicável, sugerindo que a prevenção por meio de políticas educativas seria mais eficaz.

Inspirando-se na análise de Jessica Cristina Ferracioli em sua tese sobre neurociência e Direito Penal, é possível reconhecer que a imaturidade biopsicológica característica da adolescência é marcada pela maior reatividade do sistema límbico e pela ainda incompleta maturação do córtex pré-frontal até aproximadamente os 25 anos, o que afeta de modo significativo a capacidade de avaliação de riscos e o controle de impulsos[160]. A autora reúne estudos com neuroimagens que demonstram como adolescentes processam tomada de decisão e autorregulação de maneira distinta dos adultos, apresentando menor ativação frontal em contextos que exigem reflexão e cálculo de consequências [161].

Ao transpor essas conclusões para a seara digital, observa-se que esses mesmos mecanismos ajudam a explicar por que adolescentes tendem a subestimar riscos on-line, agir impulsivamente nas redes sociais e engajar-se em condutas potencialmente danosas sem plena consciência de seus efeitos.

Índices crescentes de *cyberbullying* cometidos por adolescentes revelam uma faceta raramente discutida com a seriedade necessária: o menor que, desprovido de

[160] FERRACIOLI, Jéssica Cristina. **Neurociência e Direito Penal:** a culpabilidade na perspectiva biopsicológica do adolescente. 2018. Tese (Doutorado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2018, p. 107-108, 257.
[161] *Ibid.,* pp. 241–243.

orientação ética e submetido à pressão algorítmica por engajamento, assume o papel de agente da violência.

A acepção do menor como perpetrador de crimes cibernéticos exige análise multidisciplinar que vai do Direito a Medicina. Em 2024, o Anuário Brasileiro de Segurança Pública registrou 452 boletins de ocorrência por cyberbullying (números que ainda não demonstram a realidade, seja por subnotificação ou ausência do devido enquadramento na denúncia), com 70% envolvendo autores adolescentes de 12 a 17 anos, frequentemente em contextos de pressão social e exposição algorítmica (Fórum Brasileiro de Segurança Pública, 2025)[162].

A inversão do menor como sujeito protegido para agente de dano expõe dilemas éticos e jurídicos: **até que ponto a imaturidade neurobiológica justifica a inimputabilidade penal (art. 27, CP), e como equilibrar a doutrina da proteção integral (art. 227, CF) com a necessidade de responsabilização**?

Este fenômeno foi documentado com precisão cirúrgica na série "Adolescência" (Netflix)[163], que retrata como a necessidade de pertencimento e a ausência de mediação adulta convertem dinâmicas de grupo em tribunais de exceção digital, muitas vezes sem que os jovens tenham plena consciência da lesividade de seus atos[164].

A neurociência oferece embasamento sólido. Telma Pantano, fonoaudióloga do IPqHC, explica que o cérebro adolescente, com sistema límbico hiperdesenvolvido, responde a estímulos digitais com euforia imediata (dopamina liberada por "likes" e interações), enquanto o córtex pré-frontal (responsável por controle impulsivo) amadurece tardiamente, tornando-os vulneráveis a radicalização online[165].

---

[162] FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2025**. São Paulo: FBSP, 2025. p. 112-115.
[163] BBC BRASIL. **O que a série Adolescência nos ensina sobre bullying e responsabilidade**. 2025. Disponível em: https://www.bbc.com/portuguese/articles/cde27d4kzwjo. Acesso em: 16 nov. 2025.
[164] LUNETAS. **Série Adolescência lança olhar profundo às relações parentais**. 2025. Disponível em: https://lunetas.com.br/. Acesso em: 16 nov. 2025.
[165] PANTANO, Telma. Cérebro imaturo torna crianças e jovens vulneráveis a perigos das redes sociais: entenda. **Folha de S. Paulo**, Equilíbrio e Saúde, 22 maio 2023. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2023/05/cerebro-imaturo-torna-criancas-e-jovens-vulneraveis-a-perigos-das-redes-sociais-entenda.shtml. Acesso em: 9 nov. 2025.

Na série "Adolescência" é dramatizada essa dinâmica: personagens adolescentes, vítimas de abandono digital, convertem-se em agressores via radicalização misógina (influenciada por comunidades como "machosfera"),[166] sem consciência plena das consequências. Deve-se observar que tais atos não são isolados, mas produtos de falhas educacionais sistêmicas, onde a lei penaliza o sintoma (o agressor) sem atacar a causa (omissão parental e algorítmica).

E o questionamento permanece: se a sociedade e Estado falham em educar digitalmente seus jovens, via políticas públicas deficientes e plataformas predatórias, pode responsabilizá-los criminalmente por comportamentos emergentes dessa falha?

3.4.5 A omissão ativa da sociedade civil: quando todos somos cúmplices

A exploração infantil digital não se resume à negligência estatal ou familiar, mas configura uma conivência ativa da sociedade civil que consome, compartilha e monetiza conteúdos que violam a dignidade de menores. Enquanto cada cidadão reproduz vídeos de crianças dançando sensualmente, compra produtos anunciados por influencers mirins ou simplesmente engaja com conteúdo que sexualiza menores, consolida-se uma cadeia de cumplicidade coletiva.

Esta dinâmica perversa encontra fundamento teórico na responsabilidade por equidade trabalhada por Othon de Azevedo Lopes, para quem "a autonomia ética, na sociedade complexa, não se resume ao controle da própria conduta, mas principalmente das consequências sociais desta"[167]. O professor sustenta que "aquele que se aproveitasse dos benefícios de uma atividade deveria ser responsável pelo prejuízo dela advindo, assim como o que iniciasse voluntariamente um processo que gerasse riscos anormais deveria responder por suas consequências"[168].

---

[166] BBC BRASIL, *op. cit*.
[167] LOPES, Othon de Azevedo. **Fundamentos da responsabilidade civil**. Rio de Janeiro: Processo, 2019, p. 411.
[168] *Ibid*., p. 410.

O caso Hytalo Santos exposto no vídeo “Adultização” realizado pelo influenciador Felca[169], transcende a esfera da crônica policial para se estabelecer como a materialização empírica da cumplicidade estrutural e a falência dos mecanismos de controle social difuso. As investigações do Ministério Público da Paraíba (MPPB) desvelaram não apenas um esquema delitivo individual, mas um modelo de negócio fundamentado na exploração comercial da vulnerabilidade infantojuvenil. Sob a roupagem de entretenimento e promessas de ascensão social, adolescentes foram inseridos em uma dinâmica de confinamento e controle, onde a intimidade e a integridade física tornaram-se ativos transacionáveis mediante aliciamento e fraude[170]. A gravidade do episódio reside na reificação do corpo do menor: a submissão de vítimas a intervenções estéticas precoces e invasivas (como o caso da adolescente Kamylinha) não visava o bem-estar do sujeito, mas a adequação do 'produto' às demandas estéticas do algoritmo, convertendo a saúde infantojuvenil em insumo para monetização[171].

Nesse contexto, a audiência não figura como mera espectadora, mas como financiadora do risco. A passividade coletiva sustentou a operação desse sistema até que a denúncia viral de um terceiro (o influenciador Felca), e não a fiscalização estatal preventiva, impelisse as autoridades a agir. A decisão judicial de agosto de 2025, que determinou o bloqueio de redes sociais, a prisão preventiva dos envolvidos e o pedido ministerial de indenização coletiva de R$ 10 milhões, expõe a natureza reativa e tardia da tutela jurisdicional[172].

Resta evidente que o Estado falhou em seu dever preventivo, agindo somente quando o patrimônio dos agressores já estava inflado à custa da dignidade alheia.

---

[169] FELCA. **Adultização.** [S.l.]: YouTube, 6 ago. 2024. 1 vídeo. Disponível em: https://www.youtube.com/watch?v=2TguKe0Y7zI. Acesso em: 30 ago. 2025.

[170] MPPB denuncia Hytalo Santos e o marido Israel por crimes contra menores. **CNN Brasil**, 26 ago. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/nordeste/pb/mppb-denuncia-hytalo-santos-e-o-marido-israel-por-crimes-contra-menores/. Acesso em: 1 nov. 2025

[171] CONTA de influenciador Hytalo Santos sai do ar no Instagram após vídeo de Felca denunciando exploração de menores. **G1 Paraíba**, 8 ago. 2025. Disponível em: https://g1.globo.com/pb/paraiba/noticia/2025/08/08/conta-de-influenciador-hytalo-santos-sai-do-ar-no-instagram.ghtml. Acesso em: 1 nov. 2025

[172] MP sobre prisão de Hytalo Santos: 'Compromisso com defesa de crianças'. **CNN Brasil**, 15 ago. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/sp/mp-sobre-prisao-de-hytalo-santos-compromisso-com-defesa-de-criancas/. Acesso em: 1 nov. 2025.

Esse atraso consolidou a equação fundamental da negligência: a concentração privada dos lucros obtidos com o abuso e a distribuição coletiva dos danos irreparáveis, transformando o sofrimento infantojuvenil em uma externalidade negativa suportada por todos.

A partir da análise desse caso, é possível questionar a sociedade e sua indignação seletiva, será que apenas casos que alcançam viralização recebem atenção, enquanto inúmeras situações similares permanecem na invisibilidade?

Assim, cada visualização, like ou compartilhamento constitui proveito extraído de atividade de risco - e nos torna corresponsáveis pela reparação dos danos causados à infância, na exata medida em que, nas palavras de Lopes, "a responsabilidade por equidade obriga a que o empreendedor da atividade altere o seu comportamento" [173]. O caso Hytalo Santos expõe a hipocrisia de uma sociedade que só enxerga a exploração quando ela é denunciada por vozes com alcance equivalente ao dos exploradores, revelando uma cumplicidade difusa que se esconde atrás do anonimato dos algoritmos e da passividade do consumo digital.

3.6 A síntese da arquitetura: retroalimentação negativa

A compreensão da **"arquitetura da negligência"** exige ultrapassar a análise isolada das condutas para observar sua dinâmica relacional. As três dimensões da falha — estatal, corporativa e sociofamiliar — não operam em paralelo, mas em regime de interdependência funcional, criando um sistema de retroalimentação negativa onde cada omissão legitima e amplifica a seguinte.

O ciclo se inicia na inércia estatal: quando o Poder Público fracassa em investigar e prevenir ilícitos digitais, consolida-se um ambiente de impunidade que incentiva a atuação de predadores e aumenta a demanda por material de abuso sexual infantil (CSAM). Esse aumento de tráfego, por sua vez, é absorvido pelas plataformas digitais que, movidas pela lógica do lucro e pela ausência de *enforcement*

[173] LOPES, *op. cit.*, 2019, p. 414.

legal, deixam de implementar mecanismos de *safety by design*, permitindo que seus algoritmos amplifiquem conteúdos danosos em busca de engajamento.

Nesse cenário de risco normalizado e onipresente, a esfera familiar desamparada por referências institucionais de proteção e muitas vezes desprovida de letramento digital, entrega-se ao fatalismo ou à exploração (no caso do *sharenting*), expondo a criança novamente ao sistema. Cria-se, assim, uma sinergia da violência cibernética: o Estado que não investiga, não gera dados para políticas públicas; plataformas que lucram com a desregulação não têm incentivo para proteger; e famílias que não veem tutela estatal perdem a capacidade de mediação. A criança, portanto, não é vítima de um erro do sistema, mas do sucesso de sua operação desregulada.

A "arquitetura da negligência", trazida como tese até aqui, não se trata de uma metáfora retórica, mas de um diagnóstico estrutural de um arranjo institucional que opera exatamente conforme seu desenho implícito: privatiza-se o lucro corporativo dos conglomerados tecnológicos, mantém-se a inércia burocrática estatal e socializa-se a culpa de forma difusa entre famílias e vítimas.

Estamos diante do que a sociologia do risco define como "irresponsabilidade organizada": um sistema onde a produção de danos é sistêmica, mas a atribuição de culpa é individualizada e diluída, permitindo que todos os agentes causalmente relevantes se eximam de reparação[174]. Enquanto o Estado tratar a proteção digital como pauta acessória e não como imperativo de soberania e direitos humanos, a Doutrina da Proteção Integral (art. 227 da CF/88) permanecerá como uma promessa constitucional vazia, e a infância seguirá sendo reduzida a matéria-prima para uma engrenagem de exploração sistemática. O colapso, portanto, não é apenas técnico-jurídico; é ético, político e social.

[174] BECK, Ulrich. **Sociedade de risco:** rumo a uma outra modernidade. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2011, p. 39.

CAPÍTULO 4 SISTEMAS DE GOVERNANÇA DIGITAL PARA GARANTIA DA PROTEÇÃO INTEGRAL: ESTRUTURA NORMATIVA E ADAPTAÇÃO REGULATÓRIA

Os três capítulos precedentes demonstraram a magnitude da violência cibernética contra a infância brasileira e a arquitetura sistêmica de omissões que a viabiliza. Este capítulo propõe a Governança Digital de Proteção Integral (GDPI) como modelo normativo capaz de superar a lógica reativa do Marco Civil da Internet e inaugurar um regime de responsabilidade civil objetiva baseado em gestão de riscos sistêmicos, transparência algorítmica e inversão do ônus probatório.

A GDPI fundamenta-se em três pilares: **(i)** análise de direito comparado para identificação de paradigmas regulatórios; **(ii)** imposição de deveres estruturais às plataformas digitais (*duty of care e safety by design*); e **(iii)** investimento em educomunicação, capacitação pericial e cooperação jurídica internacional. Trata-se da transição da regulação por responsabilização *ex post* para a regulação por conformidade *ex ante*, reconhecendo que o dano à criança no ciberespaço é, na maioria das vezes, irreversível no momento de sua consumação.

4.1 Paradigmas regulatórios comparados: assimetrias e lições

A construção de modelo regulatório adequado à proteção infantojuvenil no ambiente digital exige análise criteriosa dos sistemas normativos já implementados em jurisdições estrangeiras, identificando tanto acertos a serem transplantados quanto falhas a serem evitadas.

O direito comparado revela três paradigmas principais: **(i)** o modelo estadunidense, fundado na imunidade quase absoluta das plataformas (*Section 230 do Communications Decency Act*) e na autorregulação corporativa fiscalizada precariamente pelo *Children's Online Privacy Protection Act* (COPPA); **(ii)** o modelo britânico, híbrido, que introduz deveres de segurança proativa mediante o *Online Safety Act* mas não prioriza adequadamente o *safety by design* sobre a moderação reativa de conteúdo; e **(iii)** o modelo europeu, materializado no *Digital Services Act*

(DSA), que inaugura regime de responsabilidade baseado em gestão de riscos sistêmicos e devida diligência corporativa, superando a lógica subjetiva da ciência de conteúdos específicos.

4.1.1 A falência do modelo estadunidense: Section 230 e o risco moral

A *Section 230* do *Communications Decency Act* estabelece que provedores de serviços interativos não serão tratados como editores ou locutores de informações publicadas por terceiros, isentando-os de responsabilidade civil por conteúdo gerado por usuários. Essa imunidade, originalmente concebida em 1996 para proteger a internet nascente de responsabilização desproporcional, consolidou-se como blindagem quase absoluta que permite às plataformas lucrar com conteúdos ilícitos sem internalizar os custos sociais decorrentes[175].

Essa imunidade gera aquilo que a teoria econômica denomina risco moral: ausência de incentivos econômicos para adoção voluntária de salvaguardas protetivas, uma vez que o custo da não-conformidade é zero e o lucro da exploração, máximo[176].

O COPPA (*Children's Online Privacy Protection Act*), promulgado em 1998 e reformado em 2013, busca mitigar essa falha mediante imposição de requisitos de consentimento parental para coleta de dados de menores de 13 anos. Contudo, após mais de 25 anos de vigência, o COPPA revelou-se estruturalmente ineficaz por três razões: **primeira**, a ausência de fiscalização rigorosa pela Federal Trade Commission (FTC), que jamais aplicou sanção criminal corporativa, tornando o custo de não-conformidade meramente administrativo e economicamente desprezível; **segunda**, a exceção educacional, que permite às escolas consentirem em nome dos pais, gerando coleta massiva de dados infantis por plataformas *EdTech* sem conhecimento ou autorização das famílias; **terceira**, a adoção generalizada de mecanismos de

[175] NASH, Victoria; FELTON, Lisa. **Treating the symptoms or the disease?** Analysing the UK Online Safety Act's approach to digital regulation. **Policy & Internet**, v. 16, n. 3, p. 1-20, 2024, p. 820.
[176] *Ibid.*, pp. 820 – 821.

autodeclaração de idade, sabidamente ineficazes e facilmente burlados por crianças[177].

Skowronski denuncia que a falta de execução efetiva (*enforcement*) do COPPA tornou sua aplicação às escolas confusa e inoperante, permitindo que instituições educacionais divulguem informações pessoais de estudantes sem consentimento parental simplesmente porque o COPPA não se aplica rigorosamente às escolas enquanto entidades[178].

A fragmentação do modelo estadunidense é evidenciada pela tentativa de entes subnacionais preencherem o vácuo federal. Oliveira, Silveira e Oliveira (2025) destacam o California Consumer Privacy Act (CCPA) como uma resposta legislativa estadual que, embora inspire-se na proteção europeia ao garantir direitos de acesso e exclusão (*opt-out*), limita-se geograficamente e não resolve a ausência de um padrão nacional robusto de proteção de dados infantis comparável ao modelo europeu ou brasileiro[179].

A ineficácia da autorregulação é corroborada por uma série de ações de enforcement. Apenas entre 2023 e 2025, a FTC aplicou multas multimilionárias por violações graves à COPPA a empresas como Microsoft, Amazon, NGL Labs e Disney. Evidenciando que a autorregulação corporativa, sem fiscalização estatal robusta, converte-se em simulacro regulatório. Este cenário não é hipotético, mas materializa-se em sanções aplicadas a gigantes do setor, como a multa de US$ 20 milhões à Microsoft (2023) por coletar dados de crianças sem consentimento, e a de US$ 25 milhões à Amazon (2023) por reter indefinidamente gravações de vozes infantis[180].

---

[177] SKOWRONSKI, Diana S. COPPA and Educational Technologies: The Need for Additional Online Privacy Protections for Students. Georgia State University Law Review, v. 38, n. 4, p. 1219-1251, 2022. Disponível em: https://readingroom.law.gsu.edu/gsulr/vol38/iss4/12. Acesso em: 12 nov. 2025.
[178] SKOWRONSKI, *op. cit.,* p. 1226.
[179] OLIVEIRA, Marcos Martins de; SILVEIRA, Daniel Barile da; OLIVEIRA, Maria das Graças Macena Dias de. **Análise comparada das normas de proteção de dados do Brasil, da União Europeia e do Estado da Califórnia** - EUA: LGPD x GDPR x CCPA. Revista de Direito, Governança e Novas Tecnologias, São Paulo, v. 10, n. 2, p. 45-79, jan./jul. 2025. Disponível em: https://doi.org/10.56260/dgnt.v10i2.XXX. Acesso em: 1 nov. 2025.
[180] PRIVO. **History of COPPA & GDPR Violations**. [S. l.], [2025?]. Disponível em: https://www.privo.com/history-of-coppa-gdpr-violations. Acesso em: 2 nov. 2025.

O modelo estadunidense exemplifica, portanto, aquilo que Stigler denomina regulação capturada[181]: arcabouço normativo desenhado mediante pressão corporativa, implementado precariamente e fiscalizado simbolicamente, que permite às plataformas alegarem conformidade formal enquanto perpetuam práticas sistematicamente violadoras dos direitos infantis.

4.1.2 O Modelo Britânico e a insuficiência da moderação reativa

O Reino Unido buscou superar as deficiências do modelo estadunidense mediante promulgação do Online Safety Act em 2023, introduzindo deveres de segurança proativa e responsabilização das plataformas independentemente de ordem judicial. Conforme Santos, o OSA tenta estabelecer o *duty of care* como o pilar central da "confiança digital", obrigando as plataformas a realizarem avaliações de risco prévias e a garantirem a segurança de seus usuários, especialmente crianças, sob a supervisão do órgão regulador OFCOM[182].

Diferente do Marco Civil da Internet brasileiro, que opera sob lógica reativa, o modelo britânico impõe uma obrigação proativa de segurança. Contudo, a eficácia desse dever de cuidado é severamente questionada pela doutrina e pela realidade fática. Kurschner observa que, embora o OSA exija que as empresas identifiquem, mitiguem e gerenciem riscos de danos, ele ainda delega às próprias plataformas uma discricionariedade excessiva na definição do que constitui um risco aceitável, criando um sistema de autorregulação supervisionada que pode ser capturado pela lógica econômica das *big techs*[183].

---

[181] STIGLER, George J. The Theory of Economic Regulation. **The Bell Journal of Economics and Management Science**, v. 2, n. 1, p. 3-21, 1971.
[182] SANTOS, Franklin Jeferson. **O dever de cuidado como pilar da confiança digital:** comparando a legislação do Reino Unido e a proposta brasileira. Consultor Jurídico, 2 set. 2025. Disponível em: https://www.conjur.com.br/2025-set-02/o-dever-de-cuidado-como-pilar-da-confianca-digital-comparando-a-legislacao-do-reino-unido-e-a-proposta-brasileira/. Acesso em: 1 nov. 2025.
[183] KURSCHNER, Rafael de Lima. Moderação de conteúdo e responsabilidade das empresas na proteção de crianças e adolescentes no ambiente digital. **Revista de Direito**, Viçosa, v. 17, n. 2, 2025, p. 22-23.

A crítica de Nash e Felton (2024) aprofunda esse diagnóstico ao apontar uma falha estrutural de concepção: o OSA padece de uma confusão entre tratar os "sintomas" (conteúdos danosos) e curar a "doença" (o design sistêmico). As autoras sustentam que, na prática, a lei prioriza a moderação de conteúdo (*content takedown*) em detrimento de deveres robustos de *safety by design*[184]. A metáfora clínica é precisa: remover um vídeo de exploração sexual após sua publicação não impede que o algoritmo de recomendação, desenhado para maximizar engajamento via viés de confirmação, continue a sugerir conteúdos análogos ou a conectar predadores a vítimas potenciais.

A prova empírica da insuficiência desse modelo materializou-se rapidamente com a crise da pornografia sintética gerada por Inteligência Artificial. Reportagem recente do Estadão (2025) denuncia que, mesmo sob a vigência do OSA, o Reino Unido precisou endurecer a fiscalização e ameaçar novas sanções diante da proliferação descontrolada de deepfakes pornográficos envolvendo menores. O episódio revelou que o "dever de cuidado" genérico falhou em antecipar os riscos da IA generativa, obrigando o Estado a atuar novamente de forma reativa e policialesca, correndo atrás do prejuízo tecnológico enquanto a dignidade de vítimas reais era violada em escala industrial[185].

O modelo britânico constitui, portanto, avanço em relação ao estadunidense, tendo em vista que reconhece a responsabilidade corporativa e exige ação proativa, mas permanece aquém do necessário ao não atacar a raiz do problema: a arquitetura predatória das plataformas digitais. Além disso, falha na antecipação de riscos emergentes como os *deepfakes*. Posto isso, o OSA corre o risco de se tornar uma ferramenta de gestão de crises, e não de proteção integral, perpetuando o ciclo de revitimização digital sob um verniz de regulação estatal.

---

[184] NASH, Victoria; FELTON, Lisa. Treating the symptoms or the disease? Analysing the UK Online Safety Act's approach to digital regulation. **Policy & Internet**, v. 16, n. 4, p. 818-832, 2024, p. 828.
[185] REINO UNIDO endurece fiscalização a gigantes da tecnologia para acabar com pornografia deepfake. **O Estado de S. Paulo**, 2025. Disponível em: https://www.estadao.com.br/link/reino-unido-endurece-fiscalizacao-a-gigantes-da-tecnologia-para-acabar-com-pornografia-deepfake-nprei/. Acesso em: 1 nov. 2025.

4.1.3 O Digital Services Act Europeu e a transição para Governança de Risco Sistêmico

O Digital Services Act (DSA), vigente plenamente na União Europeia desde fevereiro de 2024, representa a ruptura paradigmática mais relevante com os modelos anteriores. A norma afasta-se da lógica de responsabilidade baseada no conhecimento reativo de conteúdos específicos para inaugurar um modelo de governança baseado na devida diligência e gestão de risco sistêmico[186].

Farrand explica que o DSA não exige que a plataforma saiba de cada vídeo abusivo publicado; exige, antes, que ela projete sistemas que mitiguem preventivamente o risco de que tais vídeos sejam produzidos, recomendados ou monetizados em sua infraestrutura. A mudança do verbo — de conhecer para gerenciar — altera radicalmente a distribuição do ônus probatório e cria incentivos empresariais para investir em proteção preventiva[187].

O DSA impõe às Plataformas Online de Grande Porte (*Very Large Online Platforms — VLOPs*) deveres específicos de: **(i)** avaliação anual de riscos sistêmicos, com foco explícito na proteção de menores; **(ii)** auditoria independente por entidades certificadas; **(iii)** transparência algorítmica dos sistemas de recomendação; **(iv)** acesso a dados para pesquisadores qualificados; e **(v)** responsabilização administrativa com multas de até 6% do faturamento global[188].

A pertinência desse modelo para a realidade brasileira é direta. Viana argumenta que a experiência europeia oferece o roteiro técnico para combater fenômenos como a "adultização" e a erotização infantil denunciadas no caso do influenciador Hytalo Santos (exposto pelo youtuber Felca). O autor sustenta que a raiz do problema não é apenas o post ilegal, mas a "engrenagem das plataformas" que,

[186] FARRAND, B. How do we understand online harms? The impact of conceptual divides on regulatory divergence between the Online Safety Act and Digital Services Act. **Journal of Media Law**, v. 16, n. 2, p. 258, 2024.
[187] *Ibid.,* pp. 258 – 259.
[188] *Ibid.,* p. 260.

sem filtro ético, direciona o consumo de conteúdos sexualizantes para maximizar engajamento. Para Viana, a solução passa pela adoção de mecanismos inspirados no DSA, como a avaliação de risco obrigatória que force as *big techs* a provarem que seus algoritmos não estão aliciando crianças para lucrar[189].

É crucial compreender que o DSA não opera no vácuo, mas forma um "mosaico regulatório" com o *General Data Protection Regulation* (GDPR). Bone e Momo analisam que o GDPR consolidou princípios como *privacy by design* e minimização de dados, criando um "efeito Bruxelas" que influenciou diretamente a LGPD brasileira[190].

Enquanto o DSA regula o *design* e o conteúdo, o GDPR blinda o tratamento dos dados que alimentam esses sistemas, exigindo bases legais robustas para o tratamento de dados de menores e vedando o perfilamento para fins de marketing.

Essa simbiose normativa é estratégica para o Brasil. A harmonização da legislação brasileira com o padrão europeu, integrando LGPD e uma futura regulação de plataformas nos moldes do DAS, é condição essencial não apenas para a proteção de direitos fundamentais, mas para a manutenção do status de adequação comercial e fluxo de dados com o bloco europeu[191].

Apesar da robustez teórica, o modelo europeu não é isento de falhas estruturais. Farrand adverte sobre a possibilidade de que as plataformas transformem a avaliação de riscos em um exercício meramente burocrático, produzindo relatórios volumosos que satisfazem os reguladores formalmente, mas não alteram a arquitetura predatória de seus negócios na prática[192].

---

[189] VIANA, Davi Tavares. **Experiência europeia pode ajudar no combate à erotização infantil.** Consultor Jurídico, 2 set. 2025. Disponível em: https://www.conjur.com.br/2025-set-02/experiencia-europeia-pode-ajudar-no-combate-a-erotizacao-infantil/. Acesso em: 1 nov. 2025.

[190] BONE, Leonardo Castro de; MOMO, Maria Vitória Galvan. **Da privacidade à proteção de dados pessoais:** uma análise comparada da GDPR e a LGPD brasileira. **Revista de Direito**, v. 13, n. 1, 2021, p. 15.

[191] UNIÃO Europeia reconhece nível de proteção de dados adequado em diversos países; Brasil segue em negociação. **Mattos Filho**, 17 jan. 2024. Disponível em: https://www.mattosfilho.com.br/unico/ue-reconhecimento-brasil-protecao-dados/. Acesso em: 1 nov. 2025.

[192] FARRAND, *op. cit.,* p. 260 – 261.

A escolha pelo paradigma europeu não é aleatória, mas fundamentada na natureza jurídica da proteção. Oliveira *et al.*, em análise comparada, concluem que enquanto o modelo da Califórnia (CCPA) possui um escopo voltado precipuamente para o comércio e para a regulação da venda de dados, o modelo europeu (GDPR), que inspirou a LGPD brasileira, estrutura-se sobre a defesa de direitos fundamentais e da dignidade da pessoa humana.

Os autores destacam que a superioridade do modelo europeu para a proteção da infância reside na sua abrangência: diferentemente do modelo norte-americano, que foca na relação de consumo, o GDPR e a LGPD impõem obrigações rigorosas a qualquer operação de tratamento de dados, exigindo bases legais claras e princípios de transparência que blindam o titular dos dados contra abusos, independentemente de haver transação comercial direta[193].

4.2 Deveres estruturais da GDPI: da moderação de conteúdo à regulação de sistemas

A Governança Digital de Proteção Integral (GDPI) fundamenta-se na superação do paradigma da moderação de conteúdo reativa para a imposição de deveres estruturais (*system-based duties*). Não basta remover o conteúdo danoso; é necessário redesenhar a arquitetura que o impulsiona. Nash e Felton demonstram que as plataformas operam sob uma lógica de maximização de engajamento que, sem freios de design (*safety by design*), tende invariavelmente a amplificar riscos para usuários vulneráveis em busca de atenção monetizável [194].

Nesse sentido, a responsabilidade civil objetiva das plataformas não deve decorrer apenas do conteúdo de terceiros, superando a lógica do art. 19 do Marco Civil da Internet, mas do risco da atividade (art. 927 do Código Civil). Ao desenhar

[193] OLIVEIRA, Marcos Martins de; SILVEIRA, Daniel Barile da; OLIVEIRA, Maria das Graças Macena Dias de. Análise comparada das normas de proteção de dados do Brasil, da União Europeia e do Estado da Califórnia - EUA: LGPD x GDPR x CCPA. **Revista de Direito, Governança e Novas Tecnologias**, v. 1, n. 1, 2025, p. 11-12.
[194] NASH; FELTON, op. cit., p. 819-820.

algoritmos que exploram a hipervulnerabilidade cognitiva da criança para fins de lucro, a plataforma assume o risco dos danos psíquicos e morais decorrentes dessa arquitetura. Como aprendido com Frazão, a hipervulnerabilidade infantil justifica um regime de proteção qualificado, invertendo a lógica de neutralidade da rede para uma lógica de cuidado ativo[195].

4.2.1 O Duty of Care e a responsabilidade corporativa

A implementação de um dever de cuidado (*duty of care*) exige que as empresas realizem a devida diligência em direitos humanos, identificando, prevenindo e mitigando os impactos adversos de suas operações. Kurschner critica a postura atual de "autorregulação", apontando que a ausência de mecanismos vinculantes de *enforcement* permite que as plataformas priorizem seus termos de uso privados em detrimento da legislação pública de proteção à infância. Para o autor, a moderação de conteúdo não pode ser obscuro, ela deve seguir princípios de transparência e devido processo, alinhados aos padrões internacionais de direitos humanos[196].

O Tribunal de Contas da União (TCU), no Acórdão 2515/2025, incorporou essa tese ao afirmar que torna-se imperativo avançar para um modelo jurídico que imponha às plataformas medidas proativas de mitigação de riscos sistêmicos. O TCU reconhece que o modelo atual é estruturalmente inadequado para tutelar direitos indisponíveis de crianças, dada a velocidade de propagação viral e a irreversibilidade do dano psíquico no momento de sua consumação[197].

---

[195] FRAZÃO, Ana. **Dever geral de cuidado das plataformas digitais e proteção de crianças e adolescentes**. Parecer jurídico. São Paulo: Instituto Alana, 2021, p. 42.

[196] KURSCHNER, Rafael de Lima. Moderação de conteúdo e responsabilidade das empresas na proteção de crianças e adolescentes no ambiente digital. **Revista de Direito**, Viçosa, v. 17, n. 2, p. 28-30, 2025.

[197] BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025** – Plenário. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025, p. 41.

4.2.2 Safety by Design: privacidade e criptografia

O mais recente ciclo de propostas regulatórias (Online Safety Act, DSA, LGPD, projetos brasileiros de proteção à infância digital) converge para a imposição de deveres estruturais às plataformas digitais, deslocando o foco do mero cumprimento reativo para a exigência de medidas preventivas voltadas à proteção integral de crianças e adolescentes no ambiente digital. Nesse contexto, passam a figurar, como pilares dos novos marcos legais, a responsabilidade civil objetiva qualificada pela teoria do risco, a exigência de safety by design na arquitetura dos serviços e a inversão do ônus probatório em litígios de danos digitais graves envolvendo hipervulnerabilidade infantojuvenil[198].

O princípio de *Safety by Design* exige que a segurança seja um requisito de engenharia de software, e não uma funcionalidade opcional. Bone e Momo ao analisarem a transição do paradigma de privacidade, reforçam que mecanismos como *Privacy by Design* e *Privacy by Default* — pilares do GDPR e da LGPD — são essenciais para proteger os dados pessoais de crianças contra a coleta excessiva e o perfilamento comportamental. Os autores destacam que a proteção de dados não é apenas uma questão burocrática, mas a garantia da autodeterminação informativa do sujeito em desenvolvimento[199].

Contudo, a implementação de segurança não pode significar vigilância irrestrita. Dutra et al., em estudo pelo Instituto de Referência em Internet e Sociedade (IRIS), alertam para o risco de propostas regulatórias que, a pretexto de proteger crianças, enfraqueçam a criptografia de ponta a ponta (*client-side scanning*). Os autores argumentam que a quebra da criptografia exporia as próprias crianças a novos riscos de segurança da informação, defendendo que o safety by design deve focar em

[198] FRAZÃO, *op. cit.,* p. 78.
[199] BONE, Leonardo Castro de; MOMO, Maria Vitória Galvan. **Da privacidade à proteção de dados pessoais**: uma análise comparada da GDPR e a LGPD brasileira. **Revista de Direito**, v. 13, n. 1, p. 15-17, 2021.

funcionalidades (como impedir contato de estranhos) sem comprometer a integridade das comunicações[200].

Na lógica da responsabilidade civil digital, a doutrina nacional aponta para a necessidade de qualificar a responsabilidade das plataformas como objetiva (independentemente de culpa), à luz da teoria do risco do empreendimento (art. 927, parágrafo único, do Código Civil), especialmente diante da hipervulnerabilidade informacional e técnica da criança frente a algoritmos, coleta massiva de dados e mecanismos de persuasão onipresentes nas plataformas comerciais.

Nesse sentido, é imprescindível a formulação de normas que imponham não apenas obrigações à família e à sociedade, mas também ao setor privado, com adoção de salvaguardas *ex ante* e mecanismos auditáveis de monitoramento de riscos e transparência algorítmica.

O *safety by design* materializa-se em três dimensões técnicas obrigatórias: **(i)** arquitetura de fricção, mediante remoção de recursos que incentivem uso compulsivo por crianças, como autoplay infinito, notificações intermitentes e gamificação de permanência; **(ii)** privacidade por padrão (privacy by default), com configurações iniciais no nível mais protetivo, exigindo opt-in ativo para redução de proteção; e **(iii)** vedação absoluta de perfilamento comportamental, incluindo proibição de rastreamento, coleta de dados biométricos ou construção de perfis psicográficos de menores para fins publicitários.

A Lei 15.211/2025 já incorpora alguns desses deveres ao determinar que fornecedores deverão realizar, anualmente, avaliação de riscos sistêmicos, que considerará a eficácia dos mecanismos de verificação etária e a adequação dos sistemas de recomendação à proteção de crianças e adolescentes[201]. Contudo, a efetividade dessa disposição depende de regulamentação infralegal que estabeleça

[200] DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Segurança Da Informação E Proteção De Crianças E Adolescentes:** Discursos E Propostas Regulatórias no MERCOSUL. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024, p. 37.
[201] BRASIL. **Lei nº 15.211, de 17 de setembro de 2025.** Estatuto Digital da Criança e do Adolescente. Brasília: Presidência da República, 2025, arts. 3º, 6º e 22.

métricas objetivas, auditáveis e comparáveis de conformidade, sob risco de transformar a "avaliação de risco" em teatro regulatório.

4.2.3 Verificação etária, transparência e o combate ao grooming algorítmico

A intensificação dos riscos sistêmicos para crianças e adolescentes em ambientes digitais exige que políticas de proteção caminhem para a tríade composta por mecanismos robustos de verificação etária, transparência algorítmica e estratégias específicas de combate ao *grooming* (aliciamento) mediado por sistemas de recomendação. A experiência brasileira evidencia que, sem mecanismos efetivos nessas três frentes, as medidas de proteção ficam aquém dos desafios tecnológicos contemporâneos.

4.2.3.1 O fim da autodeclaração e os riscos da identificação

A proteção da infância exige o fim da "ficção jurídica" da autodeclaração de idade. No entanto, a solução técnica é complexa.

Conforme a taxonomia estabelecida no Radar Tecnológico nº 5 da ANPD, é necessário distinguir dois conceitos que muitas vezes são tratados como sinônimos: a Verificação de Idade (*Age Verification*) e a Garantia de Idade (*Age Assurance*)[202]. A Verificação busca a precisão exata é problemática como assim identificam Dutra et al. que destacam que métodos invasivos de verificação de idade (como envio de documentos ou biometria facial) podem criar bases de dados sensíveis que se tornam alvos de ataques cibernéticos[203].

Em contrapartida, a ANPD recomenda a adoção de mecanismos de Estimativa de Idade (uma subcategoria da Age Assurance)[204]. Essa abordagem utiliza sinais

[202] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Radar Tecnológico nº 5**: Mecanismos de Aferição de Idade. Brasília: ANPD, 2025, p. 12. Disponível em: https://www.gov.br/anpd. Acesso em: 1 nov. 2025.
[203] DUTRA *et al., op. cit.*, p. 52.
[204] BRASIL, ANPD, 2025, *op. cit.,* p. 15.

comportamentais, análise de padrões de navegação ou inferência facial para classificar o usuário em uma faixa etária provável, sem necessariamente identificar sua pessoa civil. Essa técnica atende ao princípio da minimização de dados da LGPD (Art. 6º, III), pois evita a coleta desnecessária de documentos de identificação civil para o simples acesso a uma rede social.

O obstáculo atual, contudo, é a insegurança jurídica. Como alertam Haikal e Sotomayor, o avanço da exigência de verificação no Brasil ocorre "sem base legal sólida". Embora o ECA Digital (Lei nº 15.211/2025) imponha o dever de cuidado, ele não define os padrões técnicos de verificação, criando um vácuo regulatório. Sem diretrizes claras, as plataformas tendem a adotar soluções invasivas por serem tecnicamente mais simples, ignorando que a solução não pode ser puramente tecnológica, sob pena de violar direitos fundamentais de privacidade de toda a população infantil e adulta[205].

Portanto, a solução tecnicamente viável e juridicamente adequada reside no modelo de "Duplo Anonimato" (*Double Blind*) ou no uso de tokens de terceiros auditados[206]. Nesse sistema, uma entidade independente atesta a faixa etária do usuário e fornece um token criptográfico à plataforma, garantindo que o provedor de conteúdo saiba que o usuário é adulto, sem saber quem ele é, equilibrando a barreira de entrada para menores com o direito à privacidade e ao anonimato na rede.

A solução recomendada passa pelo *age assurance* (estimativa de idade) com preservação de anonimato, utilizando sinais comportamentais ou tokens de terceiros auditados, equilibrando a barreira de entrada para menores em sites adultos com o direito à privacidade.

---

[205] HAIKAL, Beatriz; SOTOMAYOR, Gabriela. **Verificação de idade avança sem base legal sólida no Brasil. LexLegal**, São Paulo, 27 out. 2025. Disponível em: https://lexlegal.com.br/verificacao-de-idade-avanca-sem-base-legal-solida-no-brasil/. Acesso em: 01 nov. 2025

[206] BRASIL, ANPD, 2025, *op. cit*., p. 22

4.2.3.2 O Caso Felca e a resposta europeia à "Adultização"

A urgência dessas medidas foi evidenciada pelo caso do influenciador Hytalo Santos, exposto pelo youtuber Felca. Sob análise de Viana esse episódio como sintomático da "adultização" e erotização infantil impulsionadas por algoritmos. O autor argumenta que a raiz do problema não é apenas o *post* ilegal, mas a "engrenagem das plataformas" que, sem filtro ético, direciona o consumo de conteúdos sexualizantes para maximizar engajamento.

Para Viana, a experiência europeia (DSA) oferece o caminho regulatório: exigir que as plataformas avaliem o risco de seus sistemas de recomendação. Se o algoritmo entrega vídeos de crianças dançando de forma sexualizada para adultos desconhecidos, a plataforma falhou em seu dever de design seguro[207].

4.2.3.3 Transparência e auditoria: superação da cortina de fumaça

No tocante à transparência algorítmica, a opacidade dos sistemas de recomendação e priorização de conteúdo alimenta situações de risco, incluindo o chamado *grooming* algorítmico — situação em que, a partir de uma interação banal, crianças são progressivamente expostas por algoritmos de indicação a pessoas ou materiais que aumentam sua vulnerabilidade a contatos ou conteúdos lesivos.

A opacidade é o escudo das big *techs*. Archegas, em estudo pelo ITS Rio, demonstra que os atuais relatórios de transparência das plataformas são insuficientes, heterogêneos e muitas vezes incomparáveis. O autor aponta que, sem acesso a dados brutos para pesquisadores e auditores independentes, é impossível verificar se as políticas de moderação declaradas são efetivamente aplicadas. Archegas defende

[207] VIANA, Davi Tavares. **Experiência europeia pode ajudar no combate à erotização infantil**. Consultor Jurídico, 2 set. 2025. Disponível em: https://www.conjur.com.br/2025-set-02/experiencia-europeia-pode-ajudar-no-combate-a-erotizacao-infantil/. Acesso em: 1 nov. 2025.

a padronização das métricas de transparência, para que a sociedade possa auditar não apenas o que foi removido, mas o que foi mantido e impulsionado[208].

A GDPI exige, portanto, auditoria algorítmica independente. Não basta a plataforma dizer que removeu milhões de conteúdos; ela deve abrir a caixa preta de seus critérios de recomendação para que a sociedade civil verifique se o modelo de negócio continua a privilegiar o engajamento tóxico.

4.3 Inversão do ônus probatório

Dada a assimetria técnica informacional, a GDPI impõe a inversão do ônus da prova. Cabe à plataforma demonstrar, documentalmente e via auditoria forense, que seus sistemas foram desenhados para mitigar riscos (prova de compliance). A impossibilidade técnica da vítima (a criança/família) de produzir prova sobre o funcionamento do algoritmo configura a chamada “prova diabólica", justificando a inversão com base no risco do empreendimento e na proteção integral, conforme diretriz do TCU[209].

Como destaca Frazão, a regulação de plataformas digitais serve para evitar trajetórias mais tortuosas de responsabilização via litígios individuais — notoriamente marcados pela grande assimetria de poder entre vítimas e empresas. A regulação não visa banir ou censurar a inovação, mas garantir a incidência de um dever de cuidado desde o desenho dos sistemas, especialmente para públicos vulneráveis, como crianças e adolescentes, acostumados à exposição cotidiana a riscos de cyberbullying, assédio sexual, conteúdos perturbadores ou práticas algorítmicas de recomendação massiva (inclusive grooming algorítmico)[210].

Nessa linha, alinha-se à Frazão no contexto de que:

> a ideia de um dever de cuidado que incidiria sobre o próprio design das plataformas é particularmente relevante para crianças e adolescentes, que

[208] ARCHEGAS, João Victor. **Proteção de Dados e Transparência em Moderação de Conteúdo na Europa, Reino Unido e Brasil.** Rio de Janeiro: ITS Rio, 2021, p. 19-23.
[209] BRASIL. TCU. **Acórdão nº 2515/2025**, *op. cit.*, p. 50.
[210] FRAZÃO, *op. cit.*, p. 78.

> são constantemente expostos a riscos no ambiente virtual – cyberbullying, assédio sexual, exposição a conteúdos violentos ou perturbadores ou a apelos publicitários massivos, grooming, etc. Muitas vezes, esses danos estão relacionados à própria concepção do modelo de negócio pelas plataformas. Daí a importância de um dever de cuidado, que, afastando-se da abordagem baseada apenas no conteúdo, também alcance o próprio desenvolvimento da plataforma[211].

O critério central para definição do cuidado é o risco: serviços dedicados ou amplamente usados por crianças e grupos vulneráveis devem, portanto, adotar formas de cautela superiores. Plataformas com grande audiência têm responsabilidade proporcionalmente maior e devem assegurar baixíssima tolerância a condutas danosas. O dever de cuidado, contudo, não exige proteção absoluta, mas a implementação de salvaguardas razoáveis e factíveis, tratando risco, custo e previsibilidade do dano como critérios fundamentais. Assim, só se admite afastar a responsabilidade se o risco for insignificante diante do sacrifício desproporcional para evitá-lo, ou se não houver razoável evidência do dano.

Portanto, exigir das grandes plataformas a demonstração pericial de compliance e a priorização do "*privacy and safety by design*" não é censura nem barreira à inovação, mas requisito mínimo de responsabilização e justiça para contextos de extrema assimetria e especial vulnerabilidade.

4.4 Educomunicação e Literacia Digital: A Vacina Cognitiva

A regulação algorítmica deve ser acompanhada de um eixo educacional robusto.

A literacia digital transcende o domínio técnico de ferramentas e se consolida como competência essencial para a cidadania democrática no século XXI. Gonçalves Junior sustenta que a educação midiática crítica deve funcionar como uma "vacina

[211] *Ibid.,* p. 78.

cognitiva”[212] contra a desinformação, o aliciamento digital e a manipulação algorítmica, capacitando jovens a compreender não apenas como usar a tecnologia, mas por que ela opera de determinada maneira[213]. Nesse contexto, a alfabetização não pode se limitar à dimensão instrumental — ensinar a clicar em botões — mas deve ser reflexiva, desvelando os mecanismos de curadoria algorítmica que privilegiam o engajamento emocional sobre a veracidade, amplificando discursos de ódio e polarização[214].

Essa perspectiva é corroborada por Fonseca e Borges-Tiago, que demonstram empiricamente como a literacia digital reduz a incidência de cyberbullying ao empoderar indivíduos para reconhecer sinais de violência online, compreender suas formas e intervir de maneira responsável, seja reportando às autoridades ou apoiando vítimas. Segundo os autores, a educação digital promove empatia ativa e desengajamento moral inverso, contrapondo-se ao fenômeno de dessensibilização ética que alimenta agressões virtuais[215].

Caroline Balduino complementa ao analisar que a arquitetura de vigilância digital, desde brinquedos conectados até plataformas educacionais, transforma crianças em "cidadãos de dados" desde o nascimento, justificando proteção diferenciada[216]. A autora cita Eberlin (2020) para destacar que a vigilância constante — exercida por pais, escolas e empresas — pode inibir o desenvolvimento da

---

[212] GONÇALVES, Reynaldo Aragon**. Rede Conecta de Inteligência Artificial e Educação Científica e Midiática**. 2025. 315 f. Tese (Doutorado em Comunicação) – Instituto de Arte e Comunicação Social, Universidade Federal Fluminense, Niterói, 2025, p. 132.

[213] HAIKAL, A. **Educação midiática forma jovens para combater desinformação**. [S.l.], [20--]. Disponível em: https://jornal.usp.br/campus-ribeirao-preto/educacao-midiatica-forma-jovens-para-combater-a-desinformacao/. Acesso em: 10 nov. 2025.

[214] PAULO, J.; DE, G.; CAMARGO, M. E. Educação digital e alfabetização midiática como ferramentas de combate ao discurso de ódio. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 8, p. 3248-3250, 28 ago. 2025.

[215] FONSECA, Joslia; BORGES-TIAGO, Teresa. Digital Literacy Education and Cyberbullying Combat: Scope and Perspectives. In: KAVOURA, A. et al. (Eds.). **Strategic Innovative Marketing and Tourism.** Springer Proceedings in Business and Economics. Cham: Springer, 2024. p. 157-164. DOI: 10.1007/978-3-031-51038-018, p. 161.

[216] SANTOS, Caroline Henriques Mota Balduíno. **A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021, p. 167.

privacidade intelectual e da autodeterminação decisional, essenciais à formação autônoma [217].

A literacia digital crítica, portanto, não se restringe à prevenção de danos, mas habilita jovens a questionar a economia da atenção, a verificar fontes antes de compartilhar conteúdos e a exercer agência ética nas redes sociais. Como sintetiza a educadora Caroline Fernandes Lira: "a desinformação está a todo momento tentando nos confundir, mas precisamos sempre verificar as informações corretas antes de repassar"[218].

Essa competência, estruturada no currículo, torna-se antídoto essencial à arquitetura da negligência que, ao omitir educação digital, perpetua vulnerabilidades sistêmicas.

4.4.1 Alfabetização digital parental

Como já demonstrado durante o trabalho, o fosso geracional entre pais e filhos no domínio das tecnologias digitais constitui fator de risco crítico para a segurança infanto-juvenil online, tendo em vista que pais frequentemente subestimam os riscos de plataformas populares entre crianças desconhecendo mecanismos de aliciamento, monetização de dados e exposição a conteúdos violentos ou sexualizados.

Caroline Balduino argumenta que a assimetria de competências digitais entre gerações cria paradoxo: enquanto crianças são "nativas digitais" com habilidades técnicas precoces, carecem de maturidade para decidir e avaliar riscos [219]. Pais, por

---

[217] EBERLIN, Fernando Büscher von Teschenhausen. **Direitos da criança na sociedade da informação:** ambiente digital, privacidade e dados pessoais. São Paulo: Thomson Reuters Brasil, 2020. p. 128 *apud* SANTOS, 2021, p. 168.

[218] LIRA, Caroline Fernandes. Depoimento no painel **"Protagonismo Juvenil na Educação Midiática"**. In: SEMANA BRASILEIRA DE EDUCAÇÃO MIDIÁTICA, 3., 2025, Brasília. Notícia. Brasília: Secom/MEC, 31 out. 2025. Disponível em: https://www.gov.br/secom/pt-br/assuntos/noticias/2025/11/3a-semana-brasileira-de-educacao-midiatica-reforca-importancia-de-articulacao-com-universidades-e-organizacoes-para-promocao-da-cidadania-digital. Acesso em: 15 nov. 2025.

[219] SANTOS, *op. cit.*, p. 168.

sua vez, possuem experiência de vida, mas não familiaridade com interfaces e códigos culturais das plataformas.

Esse descompasso fragiliza a mediação parental, essencial à proteção integral prevista no ECA (art. 227, CF). A autora cita Roberta Densa (2018) para destacar que "à medida que avança a idade de crianças e adolescentes, diminui a esfera de controle que tanto os pais quanto o Estado têm sobre eles, abrindo-se o campo a decisões livres" [220], o que torna a alfabetização parental preventiva — e não punitiva — indispensável para preparar famílias antes da autonomia digital dos filhos.

Estudos na área indicam que iniciativas organizadas de capacitação para pais com atividades práticas, demonstrações de situações de risco on-line e orientações sobre como ajustar ferramentas de privacidade podem diminuir significativamente o contato de crianças com conteúdos impróprios.

Observa-se, portanto, que esse tipo de formação fortalece as competências dos responsáveis, permitindo que adotem uma postura mais participativa e dialogada na mediação do uso da internet. Além disso, há consenso de que tais ações devem fazer parte de programas de apoio social, de modo a alcançar famílias que enfrentam limitações econômicas e dificuldades de acesso a informações adequadas.

No Brasil, o Guia de Uso de Telas por Crianças e Adolescentes (Secom, 2025) representa avanço institucional ao oferecer orientações práticas para pais sobre: (a) tempo saudável de exposição por faixa etária; (b) identificação de sinais de vício digital (irritabilidade ao desconectar, isolamento social); (c) configuração de ferramentas nativas de controle parental em sistemas operacionais; e (d) estratégias de comunicação não violenta para negociar limites[221].

É imperativo, contudo, que essas iniciativas não se restrinjam a classes médias urbanas. A implementação de programas públicos de letramento parental, articulados

[220] DENSA, Roberta. **Proteção jurídica da criança consumidora:** entretenimento, classificação indicativa, filmes, jogos eletrônicos, exposição de arte. Indaiatuba: Foco, 2018. p. 63 *apud* SANTOS, p. 168.
[221] BRASIL. Secretaria de Comunicação Social da Presidência da República. **Guia de Uso de Telas por Crianças e Adolescentes**. Brasília: Secom, 2025. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia. Acesso em: 1 nov. 2025.

com Centros de Referência de Assistência Social (CRAS) e Estratégia Saúde da Família (ESF), pode democratizar o acesso a essas competências, reconhecendo que a proteção digital de crianças é responsabilidade compartilhada entre família, Estado e plataformas. Como adverte Santos, "a alfabetização digital envolve não apenas a educação das crianças, mas de seus pais e educadores"[222], sob pena de perpetuar a arquitetura da negligência que, ao falhar em capacitar agentes protetores, expõe gerações inteiras a riscos evitáveis.

4.5 Síntese do capítulo: a necessidade de cooperação jurídica e instituição do GDPI

A análise dos paradigmas comparados confirma que a "Arquitetura da Negligência" é sustentada por um arcabouço jurídico reativo, hoje incompatível com a prioridade absoluta constitucional. A implementação da Governança Digital de Proteção Integral (GDPI) representa, portanto, uma ruptura epistemológica necessária: o deslocamento da lógica de responsabilização por conteúdo (*ex post*) para a gestão de riscos sistêmicos (*ex ante*).

Ao internalizar as premissas de *Safety by Design* e *Duty of Care*, inspiradas na regulação europeia (DSA), o Estado brasileiro retoma sua soberania para impor limites ao poder econômico, estabelecendo que modelos de negócio baseados na exploração algorítmica da hipervulnerabilidade infantil — seja via grooming algorítmico ou monetização de dados — são, por definição, ilícitos e passíveis de responsabilização objetiva pelo risco do empreendimento.

Ademais, a efetividade desse novo ecossistema regulatório depende da sinergia entre a cooperação jurídica internacional, instrumentalizada pela adesão à Convenção de Budapeste para superar barreiras jurisdicionais na obtenção de provas e o robusto investimento em literacia digital como vacina cognitiva para famílias e educadores.

[222] SANTOS, *op. cit.*, p. 170.

Em última análise, desmontar a arquitetura da negligência exige a compreensão de que a proteção digital é um dever compartilhado e irrenunciável; enquanto a lei impõe a barreira estrutural contra o abuso das plataformas, a educação constrói a resiliência do sujeito, assegurando que o melhor interesse da criança prevaleça, definitivamente, sobre a lógica da monetização da atenção.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa partiu da inquietação provocada pela disparidade entre a robustez do ordenamento jurídico brasileiro de proteção à infância e a escalada epidêmica da violência digital contra crianças e adolescentes. Ao investigar a questão central do trabalho como a persistência de uma arquitetura de negligência compartilhada compromete a efetividade da proteção integral, o percurso investigativo confirmou a hipótese inicial: a vulnerabilidade infantojuvenil no ciberespaço não resulta de falhas acidentais ou isoladas, mas de um arranjo estrutural de omissões interdependentes entre Estado, plataformas digitais e sociedade.

No primeiro momento, o diagnóstico fenomenológico demonstrou que a violência digital sofreu uma mutação qualitativa. Não se trata mais apenas de crimes cometidos através da internet, mas de violações produzidas pela própria lógica da rede. A tipificação das novas violências — do *grooming* ao *cyberbullying*, passando pela *sextortion* e pelos *deepfakes* sexuais — evidenciou que o ambiente digital não é neutro. A pesquisa comprovou que a "plataformização da vida" inseriu crianças e adolescentes em uma economia da atenção cujo modelo de negócios, pautado na maximização do engajamento e na coleta massiva de dados, colide frontalmente com o princípio do melhor interesse da criança.

No plano normativo, a análise revelou um paradoxo crítico. O Brasil ostenta um arcabouço legislativo de vanguarda — fundamentado no Art. 227 da Constituição Federal, consolidado no ECA e atualizado pelo Marco Civil da Internet, pela LGPD e pelo recente ECA Digital (Lei nº 15.211/2025). Contudo, identificou-se um abismo entre a densidade normativa e a eficácia social. A antinomia prática entre o regime de responsabilidade civil do Marco Civil (baseado na notificação judicial) e a proteção de dados da LGPD (baseada no consentimento parental) criou, durante anos, zonas de impunidade exploradas pelas corporações tecnológicas. A pesquisa concluiu que a mera existência da lei, desacompanhada de *enforcement* rigoroso e capacidade técnica estatal, é insuficiente para conter a velocidade do dano algorítmico.

A tese central da Arquitetura da Negligência, desenvolvida no terceiro capítulo, foi corroborada pela demonstração de que as três esferas de responsabilidade operam em um ciclo de retroalimentação negativa:

i) **a negligência Estatal** manifestou-se historicamente pela ausência de políticas públicas preventivas integradas e pela morosidade investigativa, transformando a impunidade em incentivo ao ilícito;

ii) **a negligência corporativa** restou caracterizada pela recusa sistemática das plataformas em adotar o princípio do *Safety by Design*, priorizando o lucro sobre a segurança e transferindo os custos sociais de seus modelos de negócio para as vítimas;

iii) **a negligência social e familiar**, materializada no conceito de "abandono digital", não foi tratada aqui como culpa individual dos pais, mas como sintoma de uma sociedade que naturalizou a entrega da educação moral e cívica aos algoritmos, agravada por profundas assimetrias de letramento digital e acesso a recursos de controle parental.

Diante desse cenário de colapso sistêmico, o trabalho não se limitou à crítica, propondo no capítulo final a implementação de uma **Governança Digital Protetiva da Infância (GDPI).** Conclui-se que a superação da arquitetura da negligência exige a transição de um modelo de responsabilidade reativa (reparação de danos pós-ocorrência) para um modelo de responsabilidade preventiva e estrutural.

A pesquisa sustenta que a proteção efetiva depende de três pilares indissociáveis:

i) **regulação de design e transparência:** a imposição legal de *Safety by Design* e *Privacy by Default*, obrigando as plataformas a configurarem seus ambientes, por padrão, no nível máximo de proteção para usuários menores, além da abertura das caixas-pretas algorítmicas para auditoria independente;

ii) **fim da ficção da autodeclaração:** a substituição dos ineficazes termos de uso e autodeclaração de idade por mecanismos robustos de *Age Assurance*

(estimativa de idade com preservação de anonimato), que equilibrem a proteção contra acesso a conteúdos nocivos com o direito à privacidade;

iii) educação como vacina cognitiva: a implementação curricular da literacia digital crítica e do letramento parental, não apenas como instrução técnica, mas como formação ética para a cidadania digital, capacitando jovens e famílias a compreenderem e resistirem às manipulações da economia da atenção.

Posto isso, este trabalho conclui que a proteção integral da criança na era digital é um dever que não comporta terceirizações absolutas. Enquanto o Estado não regular a arquitetura das plataformas, enquanto as empresas lucrarem com a vulnerabilidade e enquanto a sociedade confundir conexão com autonomia, a negligência continuará sendo a norma.

A resposta definitiva para a violência digital contra a infância não reside em uma única lei ou ferramenta tecnológica, mas na construção de um pacto ético intergeracional onde a segurança da criança se sobreponha, de forma inegociável, à lógica do algoritmo e do lucro.

Em última análise, desmontar a arquitetura da negligência é uma escolha não tão somente jurídica, mas política. Qual tipo de sociedade digital queremos construir? Se a infância é, na letra da lei, prioridade absoluta, ela não pode ser, na prática dos algoritmos, um ativo descartável. A proteção da criança no ciberespaço é a fronteira final dos direitos humanos no século XXI; cruzá-la com dignidade é o único caminho para que a tecnologia sirva à emancipação do sujeito, e não à sua exploração.

REFERÊNCIAS

AGÊNCIA BRASIL. Justiça do RS faz condenação inédita por "estupro virtual de vulnerável". **Exame**, São Paulo, 20 dez. 2018. Disponível em: https://exame.com/brasil/justica-do-rs-faz-condenacao-inedita-por-estupro-virtual-de-vulneravel/. Acesso em: 25 nov. 2025.

ALENCAR, Carolina Cavalcante de. **Sharenting Comercial**: A Exposição de Menores em Redes Sociais por seus Pais como Fonte de Renda. 2021. Monografia (Bacharelado em Direito) – Universidade do Estado da Bahia, Juazeiro, 2021.

ARCHEGAS, João Victor. **Proteção de Dados e Transparência em Moderação de Conteúdo na Europa, Reino Unido e Brasil**. Rio de Janeiro: ITS Rio, 2021.

BBC BRASIL. **O que a série Adolescência nos ensina sobre bullying e responsabilidade**. 2025. Disponível em: https://www.bbc.com/portuguese/articles/cde27d4kzwjo. Acesso em: 16 nov. 2025.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2011.

BIONI, Bruno. **Proteção de Dados Pessoais**. 3. ed. São Paulo: Revista dos Tribunais, 2023.

BONE, Leonardo Castro de; MOMO, Maria Vitória Galvan. Da privacidade à proteção de dados pessoais: uma análise comparada da GDPR e a LGPD brasileira. **Revista de Direito**, v. 13, n. 1, p. 1-22, 2021.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)**, Bebedouro, v. 8, n. 2, p. 197-230, 2020.

BRASIL. Agência Nacional de Telecomunicações. **Polícia Civil do Rio de Janeiro faz alerta sobre novos crimes virtuais praticados contra crianças e adolescentes**. Entrevista com Cristiano Vale Maia. Portal Anatel, out. 2025. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/policia-civil-do-rio-de-janeiro-faz-alerta-sobre-novos-crimes-virtuais-praticados-contra-contra-criancas-e-adolescentes. Acesso em: 3 nov. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Radar Tecnológico nº 5**: Mecanismos de Aferição de Idade. Brasília: ANPD, 2025. Disponível em: https://www.gov.br/anpd. Acesso em: 1 nov. 2025.

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

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil. Brasília: Presidência da República, 2002.

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

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 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência. Diário Oficial da União, Brasília, DF, 15 jan. 2024.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Estatuto Digital da Criança e do Adolescente. Diário Oficial da União, Brasília, DF, 17 set. 2025.

BRASIL. Ministério da Educação. **2º Boletim Técnico "Escola que Protege"**: Dados sobre Bullying e Cyberbullying. Brasília: MEC, 2025. Disponível em: https://www.gov.br/mec/pt-br/escola-que-protege/segundo-boletim-tecnico-escola-que-protege.pdf. Acesso em: 9 nov. 2025.

BRASIL. Ministério da Saúde. **Boletim Epidemiológico**, v. 54, n. 8, 2023. Disponível em: https://www.gov.br/saude/pt-br/centrais-de-conteudo/publicacoes/boletins/epidemiologicos/edicoes/2023/boletim-epidemiologico-volume-54-no-08. Acesso em: 12 nov. 2025.

BRASIL. Ministério dos Direitos Humanos e da Cidadania; Ministério da Saúde. **Guia sobre usos de dispositivos digitais por crianças e adolescentes**. Brasília: MDH/MS, 2025.

BRASIL. Presidência da República. Secretaria de Comunicação Social. **Guia de uso de telas, dispositivos digitais e internet por crianças e adolescentes**. Brasília: SECOM, 2024. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf. Acesso em: 01 nov. 2025.

BRASIL. Secretaria de Comunicação Social da Presidência da República. **Guia de Uso de Telas por Crianças e Adolescentes**. Brasília: Secom, 2025. Disponível em: https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia. Acesso em: 1 nov. 2025.

BRASIL. SUPREMO TRIBUNAL FEDERAL. **STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros**. Brasília: STF, 26 jun. 2025. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/. Acesso em: 4 nov. 2025.

BRASIL. Tribunal de Contas da União. **Acórdão nº 2515/2025 – Plenário**. Relator: Min. Jorge Oliveira. Sessão de 29 out. 2025. Brasília: TCU, 2025.

CAVALCANTE, Laylana Araújo *et al*. Psicologia forense aplicada à perícia de crimes sexuais contra crianças em ambiente digital. **Research, Society and Development**, v. 9, n. 10, e7129109181, 2020.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **TIC Kids Online Brasil 2024**: pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Cetic.br, 2024.

CHILDFUND BRASIL. **Mais da metade dos adolescentes brasileiros já sofreu violência sexual on-line**. ChildFund Brasil, 2025. Disponível em: https://childfundbrasil.org.br/mais-da-metade-dos-adolescentes-brasileiros-ja-sofreu-violencia-sexual-on-line/. Acesso em: 12 out. 2025.

CNN BRASIL. **Deepfakes e IA geram quase 50 mil denúncias de abuso infantil no Brasil**. CNN Brasil, ago. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/brasil/deepfakes-e-ia-geram-quase-50-mil-denuncias-de-abuso-infantil-no-brasil/. Acesso em: 25 out. 2025.

CNN BRASIL. **MP sobre prisão de Hytalo Santos**: 'Compromisso com defesa de crianças'. CNN Brasil, 15 ago. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/sp/mp-sobre-prisao-de-hytalo-santos-compromisso-com-defesa-de-criancas/. Acesso em: 1 nov. 2025.

CNN BRASIL. **MPPB denuncia Hytalo Santos e o marido Israel por crimes contra menores**. CNN Brasil, 26 ago. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/nordeste/pb/mppb-denuncia-hytalo-santos-e-o-marido-israel-por-crimes-contra-menores/. Acesso em: 1 nov. 2025.

CNN BRASIL. **Polícia instaura inquérito após morte de criança em desafio pela internet**. CNN Brasil, 13 out. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/centro-oeste/df/policia-instaura-inquerito-apos-morte-de-crianca-em-desafio-pela-internet/. Acesso em: 25 nov. 2025.

COELHO, Gabi. **Nativos digitais ou crianças desprotegidas na internet?** Lunetas, São Paulo, 28 jul. 2025. Disponível em: https://lunetas.com.br/nativos-digitais-ou-criancas-desprotegidas-na-internet/. Acesso em: 10 set. 2025.

CONTA de influenciador Hytalo Santos sai do ar no Instagram após vídeo de Felca denunciando exploração de menores. **G1 Paraíba**, João Pessoa, 8 ago. 2025. Disponível em: https://g1.globo.com/pb/paraiba/noticia/2025/08/08/conta-de-influenciador-hytalo-santos-sai-do-ar-no-instagram.ghtml. Acesso em: 1 nov. 2025.

COSTELLO, Nancy *et al*. Algorithms, addiction, and adolescent mental health: an interdisciplinary study to inform state-level policy action to protect youth from the dangers of social media. **American Journal of Law & Medicine**, [S. l.], v. 49, n. 2-3, p. 135–172, 2023. DOI: 10.1017/amj.2023.25.

CÔRTES, T. da S.; MUNARO, L. F. As estratégias dos "novíssimos aliciadores" para difundir material digital pornográfico. **Brazilian Journal of Business**, v. 6, n. 3, p. 1-15, 2024.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2022.

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Segurança Da Informação E Proteção De Crianças E Adolescentes**: Discursos E Propostas Regulatórias no MERCOSUL. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS), 2024.

ECA Digital e IA: Limites jurídicos para a infância conectada. **Migalhas**, [S.l.], 2025. Disponível em: https://www.migalhas.com.br/depeso/443309/eca-digital-e-ia-limites-juridicos-para-a-infancia-conectada. Acesso em: 1 dez. 2025.

FACCHINI NETO, Eugênio; ANDRADE, Fábio Siebeneichler de. Notas sobre a indenização equitativa por danos causados por incapazes. **Revista Brasileira de Direito Civil**, v. 13, n. 3, p. 93-118, 2018.

FALEIROS, Eva. **Abuso sexual contra crianças e adolescentes**: os (des)caminhos da denúncia. Brasília: Presidência da República, Secretaria Especial dos Direitos Humanos, 2003.

FARRAND, Benjamin. How do we understand online harms? The impact of conceptual divides on regulatory divergence between the Online Safety Act and Digital Services Act. **Journal of Media Law**, v. 16, n. 2, p. 240-262, 2024.

FELCA. **Adultização**. [S.l.]: YouTube, 6 ago. 2024. 1 vídeo (50 min). Disponível em: https://www.youtube.com/watch?v=2TguKe0Y7zI. Acesso em: 30 ago. 2025.

FERRACIOLI, Jéssica Cristina. **Neurociência e Direito Penal**: a culpabilidade na perspectiva biopsicológica do adolescente. 2018. Tese (Doutorado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2018.

FERREIRA, Letícia Sthefane Santos. **Prática de crimes cibernéticos contra a criança e o adolescente**: mecanismos investigativos e combativos. 2025. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Lavras, Lavras, 2025.

FONSECA, Joslia; BORGES-TIAGO, Teresa. Digital Literacy Education and Cyberbullying Combat: Scope and Perspectives. In: KAVOURA, A. *et al.* (Eds.). **Strategic Innovative Marketing and Tourism**. Springer Proceedings in Business and Economics. Cham: Springer, 2024. p. 157-164.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2025**. São Paulo: FBSP, 2025. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025.pdf. Acesso em: 19 nov. 2025.

FRAZÃO, Ana. **Dever geral de cuidado das plataformas digitais e proteção de crianças e adolescentes**. Parecer jurídico. São Paulo: Instituto Alana, 2021.

FUNDAÇÃO MARIA CECILIA SOUTO VIDIGAL; DATAFOLHA. **Panorama da Primeira Infância**: o que o Brasil sabe, vive e pensa sobre os primeiros seis anos de vida. São Paulo: FMCSV, 2025. Disponível em: https://fundacaomariacecilia.org.br/noticias/primeira-infancia-brincar-livre-exposicao-a-telas-alta/. Acesso em: 2 nov. 2025.

G1. Pais de crianças e adolescentes que participam de vídeos de Hytalo Santos também são investigados na Paraíba. **G1 Paraíba**, João Pessoa, 11 ago. 2025. Disponível em: https://g1.globo.com/pb/paraiba/noticia/2025/08/11/pais-de-criancas-e-adolescentes-que-participam-de-videos-de-hytalo-santos-tambem-sao-investigados-na-paraiba.ghtml. Acesso em: 25 out. 2025.

GIMENEZ, Ana Paula. **Parentalidade e a Era Digital**: Abandono Digital, Oversharenting e Feed Zero. Instituto Brasileiro de Direito de Família (IBDFAM), Belo Horizonte, [s.d.]. Disponível em: https://ibdfam.org.br/artigos/2303/Parentalidade+e+a+Era+Digital%3A+Abandono+Digital%2C+Oversharenting+e+Feed+Zero. Acesso em: 25 nov. 2025.

GOMES, J. C. L. da C.; MEDRADO, L. C.; GAMA, G. B. A. C. R. N. Crimes cibernéticos: desafios jurídicos no processo e julgamento de infrações penais virtuais cometidas por agentes estrangeiros contra vítimas brasileiras. **Revista JRG de Estudos Acadêmicos**, São Paulo, v. 7, n. 15, p. e151563, 2024. DOI: 10.55892/jrg.v7i15.1563.

GONÇALVES, Reynaldo Aragon. **Rede Conecta de Inteligência Artificial e Educação Científica e Midiática**. 2025. 315 f. Tese (Doutorado em Comunicação) – Instituto de Arte e Comunicação Social, Universidade Federal Fluminense, Niterói, 2025.

GUTERRES, Isadora Balestrin; DUARTE, Hendrisy Araujo; CHAVES, Elisa Viana Dias. Limites entre autoridade parental e autonomia digital de crianças e adolescentes. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 6., 2022. **Anais** [...]. [S.l.: s.n.], 2022.

HAIKAL, A. **Educação midiática forma jovens para combater desinformação**. [S.l.]: USP, [20--]. Disponível em: https://jornal.usp.br/campus-ribeirao-preto/educacao-midiatica-forma-jovens-para-combater-a-desinformacao/. Acesso em: 10 nov. 2025.

HAIKAL, Beatriz; SOTOMAYOR, Gabriela. **Verificação de idade avança sem base legal sólida no Brasil**. LexLegal, São Paulo, 27 out. 2025. Disponível em: https://lexlegal.com.br/verificacao-de-idade-avanca-sem-base-legal-solida-no-brasil/. Acesso em: 01 nov. 2025.

INSTITUTO ALANA. **Proteção integral**. São Paulo, 2025. Disponível em: https://alana.org.br/glossario/protecao-integral/. Acesso em: 3 nov. 2025.

INTERNET WATCH FOUNDATION. **How AI is being abused to create child sexual abuse imagery**. July 2024 Report. Disponível em: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/. Acesso em: 2 nov. 2025.

KLUNCK, Patrícia; AZAMBUJA, Maria Regina Fay de. O abandono digital de crianças e adolescentes e suas implicações jurídicas. **Âmbito Jurídico**, Rio Grande, 2019.

KLUNCK, Patrícia; AZAMBUJA, Maria Regina Fay de. **O abandono digital de crianças e adolescentes e suas implicações jurídicas**. Porto Alegre: PUCRS, [20--?]. Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2020/04/patricia_klunck.pdf.

KLUNCK, Patrícia. **A Regulação da Inteligência Artificial e a Proteção de Crianças e Adolescentes**. Porto Alegre: PUCRS, 2020.

KOFFERMANN, Marcia; AGUADED, Ignacio. A influência das redes sociais sobre os adolescentes: ciberconsumo e educação crítica. **Lumina**, Juiz de Fora, v. 17, n. 1, p. 123-139, 2023.

KURSCHNER, Rafael de Lima. Moderação de conteúdo e responsabilidade das empresas na proteção de crianças e adolescentes no ambiente digital. **Revista de Direito**, Viçosa, v. 17, n. 2, p. 18-30, 2025.

LEITE, Thiago de Paula. **Responsabilização de plataformas por conteúdos de terceiros**. Estratégia Carreira Jurídica, [S.l.], 2 jul. 2025. Disponível em: https://cj.estrategia.com/portal/responsabilidade-plataformas-conteudos-de-terceiros/. Acesso em: 3 nov. 2025.

LIMA, Francisco Zamourano Silva de; FERNANDES, Maria Allice Dantas; PEDROSA, Eduarda Shirley Fernandes de Oliveira Vale. **A prática dos crimes cibernéticos como violação dos direitos da criança e do adolescente**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Potiguar, Natal, 2023.

LIMA, Jamile Moreira; VIANA, Johnnatan Reges. Crimes cibernéticos: aumento de crimes virtuais contra crianças e adolescentes pós-pandemia no Brasil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, p. 2051-2067, maio 2024.

LIMA, Reginaldo Soares de Sousa. Vulnerabilidade digital e riscos da adultização de menores em plataformas de mídia social. **Periódicos Brasil: Pesquisa Científica**, [S.l.], v. 4, n. 2, p. 321-331, 2025.

LIRA, Caroline Fernandes. Depoimento no painel "Protagonismo Juvenil na Educação Midiática". In: SEMANA BRASILEIRA DE EDUCAÇÃO MIDIÁTICA, 3., 2025, Brasília. **Notícia**. Brasília: Secom/MEC, 31 out. 2025. Disponível em: https://www.gov.br/secom/pt-br/assuntos/noticias/2025/11/3a-semana-brasileira-de-educacao-midiatica-reforca-importancia-de-articulacao-com-universidades-e-organizacoes-para-promocao-da-cidadania-digital. Acesso em: 15 nov. 2025.

LOPES, Othon de Azevedo. **Fundamentos da responsabilidade civil**. Rio de Janeiro: Processo, 2019.

LOUREIRO, Wilson *et al*. Capturados na Rede: um documentário para repensar os crimes sexuais online contra menores de idade no Brasil. **Retos XXI**, v. 9, p. 1-21, 2025.

LUNETAS. **Série Adolescência lança olhar profundo às relações parentais**. 2025. Disponível em: https://lunetas.com.br/. Acesso em: 16 nov. 2025.

MANDELLI, Mariana. Caso ‘Bel para meninas’ e a exposição infantil nas redes. **EducaMídia**, [s.d.]. Disponível em: https://educamidia.org.br/caso-bel-para-meninas-e-a-exposicao-infantil-nas-redes/. Acesso em: 27 out. 2025.

MARTIN, Júlia Saes. **Abandono digital e dever de vigilância parental sob a ótica do princípio da proteção integral à criança**. 2024. Monografia (Bacharelado em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2024.

MARUCO, Fábia de Oliveira Rodrigues; RAMPAZZO, Lino. O abandono digital de incapaz e os impactos nocivos pela falta do dever de vigilância parental. **Revista de Direito de Família e Sucessão**, v. 6, n. 1, p. 1-20, 2020.

MINKUS, Tehila; LIU, Kelvin; ROSS, Keith W. Children seen but not heard: When parents compromise children's online privacy. In: PROCEEDINGS OF THE 24TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB. Florence: ACM, 2015. p. 776-786.

MONTEIRO, Jarlene Aparecida Bandoli *et al*. Fatores, espaços e autores da violência sexual contra crianças e adolescentes na sociedade brasileira. **Revista Caderno Pedagógico**, Curitiba, v. 22, n. 9, p. 01-29, 2025.

MOURA, Andreina. **Alguns aspectos sobre o abuso sexual contra crianças**. Curitiba: Ministério Público do Estado do Paraná, [20--?]. Disponível em: https://site.mppr.mp.br/crianca/Pagina/Alguns-aspectos-sobre-o-abuso-sexual-contra-criancas. Acesso em: 01 nov. 2025.

NASH, Victoria; FELTON, Lisa. Treating the symptoms or the disease? Analysing the UK Online Safety Act's approach to digital regulation. **Policy & Internet**, v. 16, n. 4, p. 818-832, 2024.

NEXO JORNAL. **Como é a violência sexual infantil nas redes sociais**: o caso Felca e a adultização nas plataformas digitais. Podcast Nexo Políticas Públicas, 20 ago. 2025. Disponível em: https://www.nexojornal.com.br/podcast/2025/08/20/adultizacao-nas-redes-violencia-sexual-online-adolescentes-brasil. Acesso em: 11 nov. 2025.

NOGARO, A.; ANZOLIN, M. G.; PROVENZI, N. A. A economia da atenção e a fidelização de consumidores na era digital. **Revista Pedagógica**, [S. l.], v. 27, p. e8027, 2025. DOI: 10.22196/rp.v27i1.8027. Disponível em: https://bell.unochapeco.edu.br/revistas/index.php/pedagogica/article/view/8027. Acesso em: 12 nov. 2025.

OLIVEIRA, Marcos Martins de; SILVEIRA, Daniel Barile da; OLIVEIRA, Maria das Graças Macena Dias de. Análise comparada das normas de proteção de dados do Brasil, da União Europeia e do Estado da Califórnia - EUA: LGPD x GDPR x CCPA. **Revista de Direito, Governança e Novas Tecnologias**, São Paulo, v. 10, n. 2, p. 45-79, jan./jul. 2025. Disponível em: https://doi.org/10.56260/dgnt.v10i2.XXX. Acesso em: 1 nov. 2025.

PANTANO, Telma. Cérebro imaturo torna crianças e jovens vulneráveis a perigos das redes sociais: entenda. **Folha de S.Paulo**, Equilíbrio e Saúde, 22 maio 2023. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2023/05/cerebro-imaturo-torna-criancas-e-jovens-vulneraveis-a-perigos-das-redes-sociais-entenda.shtml. Acesso em: 9 nov. 2025.

PAULO, J.; DE, G.; CAMARGO, M. E. Educação digital e alfabetização midiática como ferramentas de combate ao discurso de ódio. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 8, p. 3248-3250, 28 ago. 2025.

PEREIRA, Débora Thais dos Santos; SANTOS, Jessica Lara dos Santos; MACENA, Cláudia Waléria Carvalho Mendes. Negligência do Estado em relação às denúncias realizadas contra abuso sexual infantil. **Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)**, São Paulo, v. 8, n. 10, p. 1343–1357, out. 2022.

PERRINO, John. **Using 'safety by design' to address online harms**. Brookings Institution, 26 jul. 2022. Disponível em: https://www.brookings.edu/articles/using-safety-by-design-to-address-online-harms/. Acesso em: 13 nov. 2025.

PINHEIRO, Patricia Peck. *apud* DIAS, Camila dos Reis. **O abandono digital**: análise jurídica da responsabilidade civil dos pais frente à desídia na supervisão da atividade online dos filhos. 2019. Monografia (Bacharelado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2019.

PORFÍRIO, Francisco. **Cyberbullying**. Brasil Escola, [s.d.]. Disponível em: https://brasilescola.uol.com.br/sociologia/cyberbullying.htm. Acesso em: 12 nov. 2025.

PRIVO. **History of COPPA & GDPR Violations**. [S.l.], [2025?]. Disponível em: https://www.privo.com/history-of-coppa-gdpr-violations. Acesso em: 2 nov. 2025.

REINO UNIDO endurece fiscalização a gigantes da tecnologia para acabar com pornografia deepfake. **O Estado de S. Paulo**, 2025. Disponível em: https://www.estadao.com.br/link/reino-unido-endurece-fiscalizacao-a-gigantes-da-tecnologia-para-acabar-com-pornografia-deepfake-nprei/. Acesso em: 1 nov. 2025.

REPÓRTER BRASIL. **Influencers mirins atuam em Big Techs sem alvará judicial; TV pede**. Repórter Brasil, 11 abr. 2025. Disponível em: https://reporterbrasil.org.br/2025/04/influencers-mirins-big-techs-alvara-judicial/. Acesso em: 2 nov. 2025.

SAFERNET BRASIL. **Nota Técnica nº 02/2025**: aumento de denúncias e uso de inteligência artificial na produção de conteúdo de abuso sexual infantil. Salvador: SaferNet Brasil, 19 ago. 2025.

SAFERNET BRASIL. **Relatório**: On Their Own Words - How Telegram has been used in Brazil as a marketplace for sexual abuse offenders. Salvador: SaferNet Brasil, 2024.

SANTOS, Caroline Henriques Mota Balduíno. **A privacidade e a publicidade dirigida à criança frente à Lei Geral de Proteção de Dados**. 2021. Dissertação (Mestrado em Direito) – Instituto de Ensino Superior de Brasília, Brasília, 2021.

SANTOS, Franklin Jeferson. **O dever de cuidado como pilar da confiança digital**: comparando a legislação do Reino Unido e a proposta brasileira. Consultor Jurídico, 2 set. 2025. Disponível em: https://www.conjur.com.br/2025-set-02/o-dever-de-cuidado-como-pilar-da-confianca-digital-comparando-a-legislacao-do-reino-unido-e-a-proposta-brasileira/. Acesso em: 1 nov. 2025.

SENADO NOTÍCIAS. **Mundo digital esconde perigos para as crianças**: saiba como protegê-las. Brasília, 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/09/mundo-digital-esconde-perigos-para-as-criancas-saiba-como-protege-las. Acesso em: 2 nov. 2025.

SILVA, Mariana Almeida da. A investigação de crimes cibernéticos contra crianças e adolescentes. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 189, p. 117-145, 2022.

SKOWRONSKI, Diana S. COPPA and Educational Technologies: The Need for Additional Online Privacy Protections for Students. **Georgia State University Law Review**, v. 38, n. 4, p. 1219-1254, 2022. Disponível em: https://readingroom.law.gsu.edu/gsulr/vol38/iss4/12. Acesso em: 12 nov. 2025.

SOARES, Rebeca Rodrigues; MORAIS, Rosângela Maria Rodrigues Medeiros Mitchell de. Abandono digital: a responsabilidade parental diante dos perigos das redes sociais. **Revista de Estudos Jurídicos do UNI-RN**, Natal, n. 6, p. 239-272, jan./dez. 2022.

SOCIEDADE BRASILEIRA DE PEDIATRIA. **SBP cobra do Congresso Nacional 'tolerância zero' a crimes virtuais contra crianças e adolescentes e exige aprovação de PL que aumenta rigor da lei**. Rio de Janeiro, 14 mar. 2024. Disponível em: https://www.sbp.com.br/imprensa/detalhe/news/sbp-cobra-do-congresso-nacional-tolerancia-zero-a-crimes-virtuais-contra-criancas-e-adolescentes-e-e/. Acesso em: 14 out. 2025.

SOUSA, Mykaele F. A. *et al*. Avaliação da Competência Parental na Gestão da Privacidade dos Filhos em Ambientes Digitais. In: SIMPÓSIO BRASILEIRO DE CIBERSEGURANÇA (SBSEG), 25., 2025, Foz do Iguaçu. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 1-14.

STIGLER, George J. The Theory of Economic Regulation. **The Bell Journal of Economics and Management Science**, v. 2, n. 1, p. 3-21, 1971.

TAQUARY, Eneida Orbage de Britto; TAQUARY, Catharina Orbage de Britto. Comércio de seres humanos: a influência da Convenção de Palermo sobre o novo modelo de Lei Penal brasileira. **Revista Jurídica**, Brasília, v. 9, n. 88, p. 1-26, 2007.

TEIXEIRA, Beatriz Quintas de Melo. **Sharenting e o uso indevido da imagem da criança para fins econômicos**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Presbiteriana Mackenzie, São Paulo, 2023.

UNIÃO Europeia reconhece nível de proteção de dados adequado em diversos países; Brasil segue em negociação. **Mattos Filho**, 17 jan. 2024. Disponível em: https://www.mattosfilho.com.br/unico/ue-reconhecimento-brasil-protecao-dados/. Acesso em: 1 nov. 2025.

UNIVERSA. **Ela foi abusada e torturada pelo padrasto por 9 anos**. UOL, 21 fev. 2019. Disponível em: https://www.uol.com.br/universa/noticias/redacao/2019/02/21/ela-foi-abusada-e-torturada-pelo-padrasto-por-9-anos-nao-vivi-sobrevivi.htm. Acesso em: mar. 2022.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society**: public values in a connective world. Oxford: Oxford University Press, 2018.

VIANA, Davi Tavares. **Experiência europeia pode ajudar no combate à erotização infantil**. Consultor Jurídico, 2 set. 2025. Disponível em: https://www.conjur.com.br/2025-set-02/experiencia-europeia-pode-ajudar-no-combate-a-erotizacao-infantil/. Acesso em: 1 nov. 2025.

WOLBERS, Heather; CUBITT, Timothy; CAHILL, Michael John. Artificial intelligence and child sexual abuse: a rapid evidence assessment. **Trends & issues in crime and criminal justice**, Canberra, n. 711, p. 1-17, jan. 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.