ISSN: 2675-7222

SAS
South American Sciences

GROOMING ALGORÍTMICO E DEVER DE CUIDADO DAS PLATAFORMAS DIGITAIS: RESPONSABILIDADE JURÍDICA E PROTEÇÃO INTEGRAL DA CRIANÇA NO AMBIENTE VIRTUAL

ALGORITHMIC GROOMING AND THE DUTY OF CARE OF DIGITAL PLATFORMS: LEGAL LIABILITY AND COMPREHENSIVE PROTECTION OF THE CHILD IN THE VIRTUAL ENVIRONMENT

https://doi.org/10.63330/sasciencesv6n2-042

Submetido em: 28/05/2026 e Publicado em: 26/06/2026

SAS: e26263

Emanuele Giachini Botelho
Doutoranda em Direito
Universidade Estadual do Norte do Paraná – UENP
E-mail: emanuelegbotelho@gmail.com
Lattes: http://lattes.cnpq.br/5541364008034113
ORCID: https://orcid.org/0009-0005-2928-8620

Maurício Rogério Botelho
Mestrando em Direito
Fundação Iberoamericana – FUNIBER
E-mail: mauricioescrivao@gmail.com
Lattes: http://lattes.cnpq.br/9391084571668397
ORCID: https://orcid.org/0009-0006-8647-2456

RESUMO

O artigo analisa o fenômeno do grooming algorítmico e a responsabilidade jurídica das plataformas digitais na proteção de crianças e adolescentes no ambiente virtual. Parte-se da constatação de que a sociedade algorítmica transformou menores em fontes de dados no contexto do capitalismo de vigilância, ampliando sua exposição a riscos sistêmicos. Diferentemente do aliciamento tradicional, o grooming algorítmico ocorre de forma mediada por sistemas de recomendação, que exploram vulnerabilidades cognitivas por meio do perfilamento comportamental . O estudo demonstra que a Doutrina da Proteção Integral e o princípio do melhor interesse da criança exigem a superação da neutralidade das plataformas, reconhecendo sua atuação como agentes ativos na curadoria de conteúdo. Argumenta-se que a arquitetura algorítmica gera riscos previsíveis, impondo um dever jurídico de prevenção baseado no conceito de risco tecnológico e na segurança por design. A pesquisa sustenta a aplicação da responsabilidade civil objetiva, fundamentada na teoria do risco da atividade digital e no Código de Defesa do Consumidor, especialmente diante de falhas sistêmicas de moderação e omissões tecnológicas. Destaca-se ainda o papel da LGPD na proteção de dados de menores e a convergência com modelos regulatórios internacionais. Conclui-se que as plataformas

devem assumir responsabilidade reforçada, atuando como garantidoras de um ambiente digital seguro, mediante a implementação de mecanismos preventivos eficazes .

Palavras-chave: Grooming algorítmico; Plataformas digitais; Proteção de dados de crianças e adolescentes; Responsabilidade civil; Algoritmos de recomendação.

ABSTRACT

This article examines the phenomenon of algorithmic grooming and the legal responsibility of digital platforms in protecting children and adolescents within virtual environments. It is based on the premise that the algorithmic society has transformed minors into data sources within the framework of surveillance capitalism, significantly increasing their exposure to systemic risks. Unlike traditional grooming, algorithmic grooming is mediated by recommendation systems that exploit cognitive vulnerabilities through behavioral profiling and automated content curation. The study demonstrates that the Doctrine of Integral Protection and the principle of the best interests of the child require overcoming the notion of platform neutrality, recognizing digital platforms as active agents in content governance. It argues that algorithmic architecture creates foreseeable risks, thereby imposing a legal duty of prevention grounded in the concepts of technological risk and safety by design. The research supports the application of strict civil liability, based on the theory of digital activity risk and consumer protection law, especially in cases involving systemic moderation failures and technological omissions. It also highlights the role of the Brazilian General Data Protection Law (LGPD) in safeguarding minors' data, as well as its convergence with international regulatory models.The article concludes that platforms must assume enhanced legal responsibility, acting as guarantors of a safe digital environment through the implementation of effective preventive mechanisms.

Keywords: Algorithmic grooming; Digital platforms; Data protection for children and adolescents; Civil liability; Recommendation algorithms.

1 INTRODUÇÃO

A transição da modernidade líquida para uma sociedade algorítmica reconfigurou o estatuto ontológico da infância, transmutando-a em uma infância datificada (Mascheroni, Datafied childhoods, 2020, p. 798). Neste cenário, a criança e o adolescente não são apenas usuários, mas fontes primárias de um fluxo ininterrupto de metadados que alimentam o chamado capitalismo de vigilância, sistema no qual o comportamento humano é expropriado como matéria-prima para práticas comerciais de predição e vendas (Zuboff, The age of surveillance capitalism, 2019, p. 8). A arquitetura das plataformas digitais, sustentada

por algoritmos de aprendizado de máquina, opera uma curadoria de conteúdo que, sob o pretexto de personalização, acaba por moldar identidades e ditar padrões de consumo (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 250). Ocorre que essa mesma engenharia tecnológica, ao buscar maximizar o engajamento através de mecanismos como o *feed* infinito e as "tocas de coelho" algorítmicas, catalisou o surgimento de novas patologias sociais, entre as quais se destaca o grooming algorítmico.

Diferente do aliciamento convencional, que demanda uma abordagem interpessoal direta e manual por parte do predador para estabelecer confiança (Wendt, Pedofilia Repressão aos crimes de violência sexual contra crianças e adolescentes, 2017, p. 507), o grooming algorítmico caracteriza-se pela exploração das vulnerabilidades cognitivas do menor através do próprio *design* da plataforma. Aqui, o algoritmo atua como um facilitador sistêmico: ao coletar e processar dados sensíveis de menores para fins de perfilamento (*profiling*), a plataforma pode, inadvertidamente ou por omissão deliberada, direcionar a criança a conteúdos e contatos de risco, potencializando a exposição a abusadores que se valem das mesmas métricas de relevância para identificar alvos (Teffé, Metaverso e infância, 2024, p. 657). A hipervulnerabilidade infantojuvenil, decorrente da incompletude do desenvolvimento psíquico e sensorial, encontra-se, assim, em rota de colisão com a opacidade dos sistemas automatizados que priorizam o lucro em detrimento do dever de cuidado (Maciel, Curso de Direito da Criança e do Adolescente, 2021, p. 76).

A relevância jurídica do tema reside na insuficiência dos marcos regulatórios tradicionais diante da agência ativa dos algoritmos. No Brasil, o debate oscila entre a tese da responsabilidade subjetiva mitigada, fulcrada no Artigo 19 do Marco Civil da Internet — que condiciona a responsabilização do provedor ao descumprimento de ordem judicial (Brasil, Lei 12.965, 2014) — e a antítese da responsabilidade objetiva pelo risco da atividade, sustentada pelo Código Civil e pelo Código de Defesa do Consumidor (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 94). A lacuna científica que este estudo visa preencher situa-se precisamente na intersecção entre a proteção de dados pessoais e o Direito Penal, investigando se o tratamento de dados de menores por sistemas de recomendação configura um vício de segurança apto a atrair a responsabilidade solidária das plataformas pelo grooming ocorrido em seus domínios.

Dessa forma, o problema de pesquisa que orienta este trabalho pode ser formulado nos seguintes termos: em que medida a neutralidade técnica dos provedores de aplicação é comprometida pela intervenção ativa de algoritmos de perfilamento, gerando um dever de diligência específica que autoriza a flexibilização da imunidade do Artigo 19 do Marco Civil da Internet nos casos de grooming algorítmico? A hipótese científica aventada sustenta que a atividade de curadoria algorítmica transborda a mera intermediação passiva de conteúdo, configurando uma conduta comissiva da plataforma que, ao processar dados de vulneráveis para otimizar lucros, assume o risco de criar ambientes propícios ao aliciamento,

devendo, por conseguinte, responder objetivamente pelos danos decorrentes da falha no dever de proteção integral e prioridade absoluta previstos no Artigo 227 da Constituição Federal (Souza, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 346).

A metodologia empregada ancora-se no método dedutivo, partindo das normas constitucionais e dos princípios gerais de proteção de dados para analisar a responsabilidade civil e penal das plataformas no caso concreto. A escolha justifica-se pela necessidade de confrontar a norma infraconstitucional (Marco Civil) com o sobreprincípio da prioridade absoluta e com as diretrizes da Lei Geral de Proteção de Dados (LGPD), especialmente no que tange ao "melhor interesse do menor" (Pinheiro, Direito Digital, 2021, p. 101). Realiza-se, complementarmente, uma revisão bibliográfica exaustiva de doutrina nacional e estrangeira, além de análise da jurisprudência do Superior Tribunal de Justiça e de Cortes internacionais, visando fundamentar a proposta de um novo paradigma de responsabilidade digital que considere a transparência algorítmica e a segurança por *design* como obrigações jurídicas indelegáveis das grandes corporações tecnológicas.

2 PROTEÇÃO INTEGRAL DA CRIANÇA NO AMBIENTE DIGITAL

A proteção jurídica da infância e da juventude no ordenamento brasileiro encontra sua norma estruturante no Artigo 227 da Constituição Federal de 1988, que institucionalizou a transição paradigmática da "doutrina da situação irregular" para a Doutrina da Proteção Integral (Amin, Curso de Direito da Criança e do Adolescente, 2021, p. 58; SEABRA, Manual de Direito da Criança e do Adolescente, 2017, p. 44). Esta evolução, descrita como uma verdadeira "revolução copernicana", retirou o menor da condição de mero objeto de intervenção assistencialista e repressiva do Estado para alçá-lo ao status de sujeito de direitos fundamentais (Costa, A mutação social, 1990, p. 71; Maciel, Curso de Direito da Criança e do Adolescente, 2021, p. 51). Sob a lente de Luís Roberto Barroso, a dignidade da pessoa humana opera aqui como uma cláusula geral de tutela, exigindo que a prioridade absoluta não seja apenas uma diretriz programática, mas um comando de eficácia imediata que obriga a família, a sociedade e o Estado a salvaguardar o desenvolvimento físico e mental do infante (Barroso, A dignidade da pessoa humana no direito constitucional contemporâneo, 2014, p. 64; Seabra, Manual de Direito da Criança e do Adolescente, 2017, p. 47).

A transposição desta doutrina para o ambiente digital revela o descompasso entre uma arquitetura tecnológica projetada para adultos e a realidade de uma infância que acessa a rede de forma cada vez mais precoce (Teffé, Metaverso e infância, 2024, p. 95, 694). No cenário da Web 3.0 e da datificação massiva, a proteção integral exige uma releitura dos institutos civilistas. Enquanto a tese clássica de proteção focava na integridade física e moral "offline", a antítese contemporânea sustenta que a vulnerabilidade informacional e a coleta indiscriminada de metadados constituem riscos sistêmicos que podem causar danos

irreversíveis ao livre desenvolvimento da personalidade (Doneda, Da privacidade à proteção de dados pessoais, 2006, p. 35; Schreiber, Manual de Direito Civil Contemporâneo, 2020, p. 516). Como observa Danilo Doneda, o poder informático e o deslocamento da vigilância física para a vigilância de dados pessoais exigem que o titular seja o "monarca de seus dados", exercendo a autodeterminação informativa para mitigar o exercício abusivo do poder por grandes corporações (Doneda, Da privacidade à proteção de dados pessoais, 2019, p. 496; Abrão; Bouix, A preservação do direito à privacidade e a LGPD, 2022, p. 394).

Neste contexto, surge o conceito de hipervulnerabilidade tecnológica (ou algorítmica). Diferente da vulnerabilidade técnica ou jurídica comum ao consumidor, a hipervulnerabilidade infantojuvenil decorre da incompletude do desenvolvimento cognitivo, que impede a criança de discernir a finalidade mercadológica ou os riscos de aliciamento embutidos em sistemas de recomendação (Teffé, Metaverso e infância, 2024, p. 721; Alruwaily, TIC Kids Online Brasil, 2020, p. 703). A agência dos algoritmos, ao realizar o perfilamento (*profiling*) de menores para otimizar o engajamento, acaba por explorar o que Anderson Schreiber denomina como a falta de "senso crítico e resistência mental" desse público (Schreiber, Direitos da personalidade, 2014, p. 148). O diálogo entre a doutrina constitucional e o Direito Digital impõe, portanto, que o melhor interesse do menor, previsto no Artigo 14 da LGPD, seja interpretado de forma expansiva, superando o silêncio legislativo em relação aos adolescentes e garantindo que a proteção de dados seja um direito fundamental autônomo (Tepedino, Desafios da Lei Geral de Proteção de Dados, 2020, p. 32; Souza; Baptistelli; Siqueira, Tratamento de dados das crianças e adolescentes, 2022, p. 412).

A hipervulnerabilidade algorítmica é exacerbada pelo fenômeno da "toca de coelho", onde os sistemas automatizados de plataformas como o TikTok, ao buscarem a maximização do lucro através do engajamento, direcionam vulneráveis a conteúdos progressivamente nocivos, facilitando o grooming algorítmico (Instituto Alana, Manifestação no caso TikTok, 2024, p. 855). Confrontando-se a autonomia privada com a proteção de vulneráveis, Ingo Sarlet argumenta que o acesso indiscriminado a dados pode afetar direitos fundamentais básicos, tornando imperiosa a aplicação da técnica da prevenção por design (*privacy by design*) para conter a abusividade deliberada de agentes que condicionam o acesso a serviços a aceites irracionais de termos de uso (Sarlet, A eficácia dos direitos fundamentais, 2008, p. 364; Souza; Baptistelli; Siqueira, Tratamento de dados das crianças e adolescentes, 2022, p. 419).

Conclui-se que o microssistema do Estatuto da Criança e do Adolescente (ECA), lido à luz do Artigo 227 da Constituição, não admite a neutralidade das plataformas digitais diante da exploração de dados de menores. A proteção integral no ambiente digital transborda a mera mediação parental, configurando-se como um dever de responsabilidade primária e solidária de todos os atores sociais, visando neutralizar as assimetrias informacionais que colocam a infância em rota de colisão com o capitalismo de vigilância (Amin, Evolução histórica do direito da criança e do adolescente, 2021, p. 112; Zuboff, The age of

surveillance capitalism, 2019, p. 726). A hipervulnerabilidade, portanto, não é apenas um conceito descritivo, mas um vetor interpretativo que autoriza a imposição de padrões de segurança e transparência algorítmica mais rígidos, independentemente da verificação de culpa subjetiva dos provedores (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 256; Biolcati, Internet, fake news e responsabilidade civil, 2022, p. 341).

3 ALGORITMOS DE RECOMENDAÇÃO E RISCOS SISTÊMICOS

A funcionalidade técnico-jurídica das plataformas digitais contemporâneas transbordou a mera intermediação passiva para consolidar-se como uma agência de curadoria algorítmica ativa. Sob a égide do que Shoshana Zuboff denomina capitalismo de vigilância, a experiência humana é expropriada como matéria-prima gratuita para tradução em dados comportamentais, gerando um "superávit" que alimenta produtos de predição (Zuboff, The age of surveillance capitalism, 2019, p. 8; Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 513). Estes sistemas não são neutros; são, nas palavras de Tarleton Gillespie, "máquinas de visibilidade" desenhadas para organizar, priorizar e filtrar informações, estabelecendo o que deve ou não ser visto através de uma governança algorítmica opaca (Gillespie, Custodians of the Internet, 2018, p. 84).

A lógica de engajamento e retenção constitui o núcleo cinético dessa engenharia. Para maximizar o lucro, as plataformas operam sob a economia da atenção, utilizando algoritmos preditivos que calculam a "relevância pessoal" para manter o usuário conectado pelo maior tempo possível (Zuboff, The age of surveillance capitalism, 2019, p. 712). Ocorre que essa métrica de popularidade, frequentemente usada como *proxy* para mérito ou interesse, acaba por amplificar conteúdos tóxicos e interações perigosas, pois o algoritmo é indiferente à moralidade da interação, priorizando o volume de cliques e o tempo de tela (Gillespie, Custodians of the Internet, 2018, p. 90; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 449).

Neste cenário, o fenômeno da datificação (*datafication*) transmuta a subjetividade infantojuvenil em um conjunto de pontos de dados mineráveis. O profiling (perfilamento) comportamental permite que o sistema identifique não apenas preferências de consumo, mas vulnerabilidades psíquicas e estados emocionais (Doneda, Da privacidade à proteção de dados pessoais, 2020, p. 114; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 407). A antítese dogmática revela-se aqui: enquanto a tese da neutralidade técnica sustenta que o algoritmo apenas reflete o desejo do usuário, a antítese crítica demonstra que a arquitetura das plataformas molda o comportamento em escala, criando externalidades negativas sistêmicas (Zuboff, The age of surveillance capitalism, 2019, p. 514).

Uma das externalidades mais graves é a exposição a contatos desconhecidos e a amplificação de interações perigosas. Dados da pesquisa TIC Kids Online Brasil indicam que a procura por novos amigos

e o contato com estranhos são facilitados pelas próprias sugestões do sistema (CGI.BR, TIC Kids Online Brasil, 2024, p. 830). O grooming mediado por inteligência artificial surge quando o *design* da plataforma — como o *feed* "Para Você" do TikTok — cria o efeito de "toca de coelho" (*rabbit hole*), direcionando menores a comunidades onde predadores se infiltram utilizando as mesmas ferramentas de segmentação para identificar alvos hipervulneráveis (Instituto Alana, Manifestação no caso TikTok, 2024, p. 844). Aqui, a IA não é apenas um meio, mas um facilitador sistêmico que otimiza a conexão entre abusador e vítima através do pareamento de metadados comportamentais (Souza, Tratamento de dados das crianças e adolescentes, 2022, p. 541).

Dessa forma, o risco não é acidental, mas estrutural. A hipervulnerabilidade tecnológica da criança é explorada por sistemas que capturam dados subconscientes — como dilatação da pupila ou tempo de fixação ocular em ambientes de realidade virtual — para refinar o perfilamento e prever condutas futuras (Teffé, Metaverso e infância, 2024, p. 748, 751). Diante desse poder de modulação, a responsabilidade das plataformas deve ser reavaliada à luz dos riscos sistêmicos gerados por seu modelo de negócio. Se o algoritmo possui a capacidade técnica de detectar padrões para fins publicitários com precisão cirúrgica, a alegação de impossibilidade técnica de monitoramento para prevenir o aliciamento torna-se juridicamente insustentável, configurando uma omissão deliberada em face do dever de segurança por *design* (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 442, 458).

4 GROOMING ALGORÍTMICO E DEVER DE CUIDADO

A superação do paradigma da neutralidade técnica dos provedores de aplicação revela-se imperiosa diante da transição de meros hospedeiros passivos para agentes ativos de curadoria algorítmica. Sob a lente de Tarleton Gillespie, as plataformas contemporâneas atuam como "custódios da internet", operando uma governança invisível que seleciona o que deve ser mostrado e a quem, comprometendo a imunidade outrora conferida pelo Artigo 19 do Marco Civil da Internet (Gillespie, Custodians of the Internet, 2018, p. 61). Esta metamorfose jurídica transmuta a natureza do serviço: ao deixar de ser um "conduto passivo" equiparável a companhias telefônicas, o provedor assume a função de quase editor, exercendo controle editorial algorítmico que atrai a responsabilidade pelos riscos gerados por seu modelo de negócio (Pinheiro, Direito Digital, 2021, p. 285; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 413).

A previsibilidade do risco no grooming algorítmico decorre da própria arquitetura sistêmica voltada à maximização do engajamento. Na sociedade do risco, conforme a lição de Ulrich Beck, o perigo é criado voluntariamente pela ação humana e induzido pela tecnologia, operando sob uma lógica matemática que dilui o indivíduo em grandes números (Doneda, Da privacidade à proteção de dados pessoais, 2006, p. 65). Ocorre que, se a plataforma possui a capacidade técnica de perfilamento (*profiling*) cirúrgico para fins

publicitários, a exposição de menores a predadores através de sistemas de recomendação não é um evento fortuito, mas uma externalidade negativa previsível da economia da atenção (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 491). O risco tecnológico aqui configura uma periculosidade adquirida, onde a falha na segurança do sistema de recomendação permite que o algoritmo atue como um facilitador sistêmico do aliciamento (Martins, Responsabilidade civil por acidente de consumo na Internet, 2014, p. 334; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 487).

Neste cenário, o dever jurídico de prevenção fundamenta-se no dever geral de cuidado objetivo, transpondo-se do Direito Penal para o Digital a obrigação de adotar toda precaução para não causar lesão a bens jurídicos (Teles apud Greco, Curso de Direito Penal, 2021, p. 55). A tese da responsabilidade subjetiva mitigada do Marco Civil da Internet (Art. 19), que condiciona a ação do provedor à ordem judicial, confronta-se com a antítese da responsabilidade objetiva pelo risco da atividade, prevista no Artigo 927, parágrafo único, do Código Civil (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 74). A hipótese central deste estudo sustenta que a inação das plataformas diante de riscos sistêmicos para vulneráveis configura uma culpa por omissão tecnológica (*culpa in omittendo*), na medida em que a empresa, ao lucrar com o tratamento de dados comportamentais de menores, assume o dever de garantir a segurança por *design* (Pinheiro, Direito Digital, 2021, p. 136, 147).

A hipervulnerabilidade infantojuvenil exige que o dever de cuidado seja interpretado à luz da prioridade absoluta prevista no Artigo 227 da Constituição Federal, superando a visão meramente comercial das plataformas (Seabra, Manual de Direito da Criança e do Adolescente, 2017, p. 673). Quem se beneficia economicamente e estimula ativamente a criação de comunidades virtuais é corresponsável pela garantia dos direitos da personalidade, pois a inércia em impedir o surgimento de novos ambientes de risco prolonga a situação de exposição da vítima (STJ apud Maciel, Curso de Direito da Criança e do Adolescente, 2021, p. 60). Portanto, o grooming algorítmico não pode ser tratado como fato de terceiro isolado, mas como um vício na prestação do serviço que atrai a responsabilidade solidária do provedor pelo descumprimento do dever de proteção integral em face de perigos gerados por sua própria agência tecnológica (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 506, 509).

5 SAFETY BY DESIGN E RESPONSABILIDADE PREVENTIVA

A integração da segurança desde a fase de concepção dos ecossistemas digitais, paradigma conhecido como Safety by Design, representa o deslocamento da responsabilidade jurídica de um plano meramente repressivo para uma dimensão preventivo-estrutural. Sob a égide da Doutrina da Proteção Integral e do Artigo 227 da Constituição Federal, a arquitetura das plataformas deixa de ser uma escolha técnica discricionária para tornar-se um espaço de conformidade normativa vinculada ao melhor interesse

do menor (Teffé, Metaverso e infância, 2024, p. 608, 665). Diferente da abordagem tradicional, que foca na remoção *ex post* de conteúdos ilícitos, o *Safety by Design* exige que os provedores identifiquem riscos sistêmicos e implementem salvaguardas tecnológicas antes mesmo da interação do usuário, transmutando o dever de cuidado em um dever de arquitetura segura (Instituto Alana, Proteção de crianças e adolescentes na Internet, 2024, p. 712; Teffé, Metaverso e infância, 2024, p. 612).

A proteção infantil por padrão (*by default*) constitui o núcleo cinético dessa estratégia. Na sociedade da vigilância, as interações sociais migraram de uma lógica "privada por padrão" para uma dinâmica "pública por padrão", onde o estímulo ao compartilhamento massivo de dados atende aos interesses do capitalismo de dados (CGI.BR, TIC Kids Online Brasil, 2023, p. 591). A antítese regulatória impõe que, para usuários menores, a configuração inicial de qualquer aplicação deve ser a de máxima restrição de visibilidade e coleta de dados, incluindo a adoção compulsória de perfis privados e a vedação ao perfilamento comportamental para fins comerciais (Teffé, Metaverso e infância, 2024, p. 616, 619; CGI.BR, TIC Kids Online Brasil, 2023, p. 595). Conforme orienta o Comentário Geral nº 25 da ONU, o desenvolvimento progressivo das capacidades da criança exige que os serviços digitais sejam projetados para mitigar a exposição a riscos transversais, como a violação da privacidade e o aliciamento (ONU apud CGI.BR, TIC Kids Online Brasil, 2023, p. 583, 586).

O desafio técnico-jurídico mais sensível reside na verificação etária. A tese da autodeclaração, amplamente utilizada pelas plataformas, revela-se ineficaz e passível de fraude, permitindo que crianças acessem ambientes destinados a adultos onde o grooming é facilitado pela ausência de filtros (Teffé, Metaverso e infância, 2024, p. 614, 669). A antítese robusta, sustentada por organismos como a *5Rights Foundation*, propõe a aplicação de métodos proporcionais ao risco, transitando do uso de documentos oficiais e biometria até a inferência algorítmica de idade, desde que respeitados os limites da minimização de dados (5rights Foundation apud Teffé, Metaverso e infância, 2024, p. 613, 614, 668). A verificação de idade não deve ser vista como uma barreira à liberdade, mas como uma ferramenta de segregação de ambientes necessária para garantir que a experiência digital seja apropriada ao estágio de desenvolvimento psicofísico do vulnerável (Teffé, Metaverso e infância, 2024, p. 611; Instituto Alana, Proteção de crianças e adolescentes na Internet, 2024, p. 715).

A limitação de interações automatizadas surge como medida imperiosa para interromper o fenômeno da "toca de coelho" (*rabbit hole*). Sistemas de recomendação baseados em rolagem infinita e pareamento algorítmico muitas vezes direcionam menores a contatos perigosos, repetindo conteúdos abusivos em *loop* (Instituto Alana, Proteção de crianças e adolescentes na Internet, 2024, p. 721, 725). A integração entre tecnologia e regulação exige que o *design* das plataformas inclua mecanismos de interrupção do engajamento compulsivo e limites técnicos à interação com perfis desconhecidos,

neutralizando a agência algorítmica que, na busca por lucro, acaba por atuar como facilitadora sistêmica do aliciamento (CGI.BR, TIC Kids Online Brasil, 2024, p. 695; Teffé, Metaverso e infância, 2024, p. 621).

Dessa forma, a responsabilidade preventiva das plataformas transborda a mera mediação parental. Embora a vigilância dos pais seja essencial, ela é insuficiente diante da opacidade técnica dos sistemas (CGI.BR, TIC Kids Online Brasil, 2023, p. 596). O diálogo com normas internacionais, como o *California Age-Appropriate Design Code Act* e as diretrizes das autoridades de proteção de dados da Europa, sinaliza que a segurança deve vir "direto de fábrica" (Teffé, Metaverso e infância, 2024, p. 618, 673). No ordenamento brasileiro, a Resolução nº 245/2024 do CONANDA consolida este entendimento ao estabelecer deveres específicos de cuidado para as empresas, reforçando que a falha no dever de arquitetura segura caracteriza um descumprimento direto do mandamento constitucional de prioridade absoluta (CONANDA apud Teffé, Metaverso e infância, 2024, p. 615, 667; Instituto Alana, Proteção de crianças e adolescentes na Internet, 2024, p. 713).

6 RESPONSABILIDADE CIVIL DAS PLATAFORMAS

A superação do paradigma da irresponsabilidade civil das plataformas digitais exige uma densa análise crítica sobre a dicotomia entre a responsabilidade subjetiva agravada do Marco Civil da Internet e a responsabilidade objetiva pelo risco da atividade consagrada pelo Código Civil e pelo Código de Defesa do Consumidor (CDC). A tese clássica, sedimentada em uma leitura isolada do Artigo 19 da Lei nº 12.965/2014, sustenta que o provedor de aplicações apenas responde por danos decorrentes de conteúdo de terceiros após o descumprimento de ordem judicial específica, visando blindar a liberdade de expressão e a inovação tecnológica (Souza, As cinco faces da proteção à liberdade de expressão no Marco Civil da Internet, 2015, p. 398; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 386). Contudo, a antítese contemporânea, amparada na Teoria do Risco da Atividade Digital, demonstra que a arquitetura algorítmica de personalização e engajamento transborda a mera intermediação passiva, configurando uma conduta comissiva que incrementa riscos sistêmicos e atrai a incidência do Artigo 927, parágrafo único, do Código Civil (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 404, 453).

A aplicação do Código de Defesa do Consumidor ao ambiente digital é o fundamento cinético para a responsabilização objetiva por defeito na prestação do serviço. Nos termos do Artigo 14 do CDC, o serviço é defeituoso quando não oferece a segurança que o consumidor dele legitimamente espera, caracterizando-se como periculosidade adquirida quando a falha sistêmica permite que o algoritmo atue como facilitador do aliciamento (Martins, Responsabilidade civil por acidente de consumo na Internet, 2014, p. 334; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 447). Sob essa ótica, a hipervulnerabilidade do menor transubstancia o usuário em consumidor por equiparação

(*bystander*), estendendo a proteção legal a todos aqueles que, embora não sendo contratantes diretos, sofrem as externalidades negativas do risco-proveito gerado pela plataforma (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 126; Pinheiro, Direito Digital, 2021, p. 181).

A responsabilidade por risco criado sustenta-se no fato de que o provedor, ao extrair lucro da datificação comportamental de vulneráveis, assume o ônus de garantir a incolumidade do ambiente virtual (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 126). A jurisprudência do Superior Tribunal de Justiça, ao editar a Súmula 479, consolidou o entendimento de que danos gerados por fraudes de terceiros no âmbito de operações bancárias configuram fortuito interno, pois estão intrinsecamente ligados ao risco do negócio (Schreiber, Manual de Direito Civil Contemporâneo, 2020, p. 641). Analogamente, o grooming algorítmico deve ser interpretado como fortuito interno das redes sociais: se o sistema possui precisão para segmentar publicidade, a inação em detectar padrões de aliciamento configura uma omissão tecnológica (*culpa in omittendo*) juridicamente relevante, superando a tese do fato de terceiro (Pinheiro, Direito Digital, 2021, p. 175; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 491).

A falha de moderação e o descumprimento do dever de vigilância evidenciam o que Patricia Peck Pinheiro denomina como a necessidade de uma "blindagem legal" que nasça com o *design* do negócio (Pinheiro, Direito Digital, 2021, p. 172). Diante de conteúdos manifestamente ilícitos, a inércia do provedor após a ciência extrajudicial transborda o limite da liberdade de expressão e adentra o campo do abuso de direito previsto no Artigo 187 do Código Civil (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 457, 470). A neutralidade técnica é, portanto, mitigada pela agência algorítmica: quem estimula ativamente a criação de comunidades e manipula a visibilidade de conteúdos torna-se corresponsável pelos danos, uma vez que a falha em impedir a criação de ambientes de risco prolonga a situação de exposição da vítima (STJ apud Maciel, Curso de Direito da Criança e do Adolescente, 2021, p. 54). Conclui-se que a responsabilidade civil no grooming algorítmico é objetiva e solidária, fundamentada na falha do dever de segurança e na assunção do risco por parte daqueles que operam o capitalismo de vigilância (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 124; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 467).

7 LGPD E PROTEÇÃO DE DADOS DE MENORES

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no ordenamento jurídico pátrio operou uma densificação normativa sobre o tratamento de informações de vulneráveis, estabelecendo, em seu Artigo 14, o Princípio do Melhor Interesse da Criança e do Adolescente como o vetor axiológico proeminente e inafastável (Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 296; Oliveira, Os dados de crianças e adolescentes na Internet, 2022, p. 329). Este

dispositivo não configura mera recomendação ética, mas um comando de otimização que impõe ao controlador o dever de selecionar a base legal e o método de tratamento que garanta a máxima proteção ao livre desenvolvimento da personalidade (Maciel, Curso de Direito da Criança e do Adolescente, 2021, p. 61; Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 343). Sob a ótica do Comitê dos Direitos da Criança da ONU, o melhor interesse deve ser compreendido sob um conceito triplo: como um direito fundamental, um princípio jurídico interpretativo e uma norma de procedimento para a avaliação de impactos (ONU apud Seabra, Manual de Direito da Criança e do Adolescente, 2017, p. 472).

A controvérsia dogmática mais acentuada reside no regime do consentimento e seus limites. Enquanto a tese literalista sustenta que o § 1º do Artigo 14 exige o consentimento específico e em destaque apenas para crianças (até 12 anos incompletos), a antítese protetiva argumenta que o silêncio eloquente do legislador em relação aos adolescentes não autoriza a plena autonomia destes no ambiente digital (Souza, Tratamento de dados das crianças e adolescentes, 2022, p. 297, 298). Admitir que adolescentes possam dispor de seus dados sem intervenção parental colidiria com a Teoria das Capacidades do Código Civil e com o paradigma da prioridade absoluta (Souza, Tratamento de dados das crianças e adolescentes, 2022, p. 299; Teffé, Metaverso e infância, 2024, p. 643). De fato, a experiência comparada do GDPR europeu estabelece o limite de 16 anos para o consentimento direto, evidenciando que a fragilidade cognitiva persiste além da infância biológica (Souza, Tratamento de dados das crianças e adolescentes, 2022, p. 301).

O profiling algorítmico (perfilamento) e a publicidade comportamental constituem o núcleo das violações sistêmicas à privacidade infanto-juvenil. Conforme Danilo Doneda, o perfilamento utiliza estatística e inteligência artificial para extrair "metainformações" que sintetizam hábitos e predizem destinos (Doneda, Da privacidade à proteção de dados pessoais, 2020, p. 136). Quando aplicado a menores, esse tratamento transmuta-se em um mecanismo de induzimento e controle, onde a "máquina algorítmica" explora a hipervulnerabilidade para moldar desejos de consumo e comportamentos (Zuboff apud Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 258; Bioni apud Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 425). O risco é exacerbado pela coleta de dados sensíveis — incluindo biometria e padrões subconscientes no metaverso —, cujo tratamento pode resultar em discriminações abusivas e danos psíquicos irreversíveis (Teffé, Metaverso e infância, 2024, p. 646, 647; Souza, Tratamento de dados das crianças e adolescentes, 2022, p. 295).

A relação intrínseca entre o tratamento massivo de dados e o grooming algorítmico revela que a infraestrutura desenhada para o lucro comercial é a mesma que viabiliza o aliciamento. A plataforma, ao processar dados rastreados e inferidos para segmentar anúncios, acaba por criar o "mapa da mina" para o predador: a identificação de gostos, rotinas e fragilidades emocionais permite que o agressor estabeleça uma conexão de confiança personalizada (Wendt, Pedofilia Repressão aos crimes de violência sexual contra crianças e adolescentes, 2017, p. 527, 543). Assim, o tratamento de dados que ignore o dever de segurança

por *design* configura uma abusividade deliberada, na medida em que a empresa prioriza a monetização do engajamento em detrimento da neutralização de riscos de aliciamento mediado por IA (Souza, Tratamento de dados das crianças e adolescentes, 2022, p. 303, 318). A proteção integral, portanto, exige que a autodeterminação informativa do menor seja resguardada por mecanismos técnicos que impeçam o perfilamento predatório, sob pena de responsabilidade objetiva do agente de tratamento (Ferreira, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 421; Finkelstein, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 364).

8 MODELOS REGULATÓRIOS INTERNACIONAIS

A arquitetura regulatória internacional das plataformas digitais atravessa uma inflexão paradigmática, abandonando o "porto seguro" da imunidade ampla em prol de modelos de regulação baseada em risco e deveres de diligência assimétricos. No cenário global, observa-se uma polarização entre a tese da imunidade estrita, personificada pela Seção 230 do *Communications Decency Act* (CDA) nos Estados Unidos — que blinda o provedor por considerar que a inovação exige a isenção de responsabilidade editorial (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 359) — e a antítese da responsabilidade integral, adotada por regimes como o chinês, que impõe o monitoramento proativo e a remoção compulsória sob pena de severas sanções administrativas e penais (Gillespie, Custodians of the Internet, 2018, p. 58; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 361).

A União Europeia, historicamente vinculada ao sistema de "proteção condicional" da Diretiva de Comércio Eletrônico 2000/31/CE, operou um salto qualitativo com a promulgação do Digital Services Act (DSA). Enquanto a Diretiva anterior imunizava o provedor de armazenamento (*hosting*) desde que este não tivesse "conhecimento efetivo" da ilicitude (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 369), o DSA introduz uma abordagem prospectiva. Para as chamadas *Very Large Online Platforms* (VLOPs), o DSA impõe a obrigação de realizar avaliações anuais de riscos sistêmicos, abrangendo especificamente os efeitos negativos sobre os direitos fundamentais e o bem-estar de menores (União Europeia, Digital Services Act, 2022 apud Biolcati, 2022, p. 413). Esta mudança transmuta o papel da plataforma de um mero "condutor passivo" para um agente de governança algorítmica, cuja responsabilidade exsurge não apenas do conteúdo postado, mas da falha sistêmica em mitigar vulnerabilidades exploradas por predadores em práticas de grooming (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 376).

Em paralelo, o Reino Unido avançou com o Online Safety Act, consolidando uma tendência de vigilância estatal sobre as redes sociais que transborda a mera remoção de conteúdos ilícitos. O modelo britânico, que já admitia remédios singulares em casos de *breach of confidence* (Paesani, Direito e Internet,

2013, p. 266), agora exige que as empresas demonstrem proativamente como protegem as crianças de conteúdos prejudiciais, ainda que não tecnicamente ilegais (*harmful but lawful*). Esta regulação impõe o que se denomina proceduralização, onde o Estado define parâmetros de segurança que o provedor deve implementar através de mecanismos de auditoria e transparência algorítmica (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 340). A crítica doutrinária a este modelo reside no risco de "censura privada", na medida em que as plataformas, sob pressão de multas que podem atingir bilhões de euros ou porcentagens significativas do volume de negócios global, tendem a realizar uma moderação excessivamente restritiva para evitar o risco jurídico (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 387, 409).

As tendências regulatórias globais sinalizam para o que Colin Bennett denomina de "convergência por determinismo tecnológico", onde a complexidade transfronteiriça da rede exige padrões internacionais mínimos de proteção (Doneda, Da privacidade à proteção de dados pessoais, 2020, p. 96). O "efeito dominó" gerado pelo marco regulatório europeu — agora expandido do GDPR para o DSA — compele nações de outros blocos, inclusive na América Latina, a elevar seu nível de proteção para garantir a interoperabilidade e a competitividade comercial (Pinheiro, Proteção de Dados Pessoais: comentários à LGPD, 2020 apud Biolcati, 2022, p. 251). A responsabilidade das plataformas, portanto, deixa de ser analisada sob o prisma da culpa individual para ser enquadrada na teoria do risco da atividade digital em nível supranacional: se a empresa manipula a visibilidade e o engajamento para maximizar o lucro, ela assume o dever de neutralizar as externalidades negativas, como o aliciamento automatizado, independentemente de onde o dano ocorra geograficamente (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 344, 402).

Em conclusão, o confronto entre o modelo liberal norte-americano e o modelo intervencionista europeu/britânico revela que a neutralidade técnica é um dogma em erosão. A regulação baseada em risco, ao exigir que as plataformas auditem seus próprios algoritmos de recomendação antes que eles facilitem o grooming, estabelece um novo patamar de diligência técnica. Este paradigma internacional exige que a responsabilidade civil seja interpretada não como uma punição ex post, mas como um mecanismo de incentivo à conformidade ética e à segurança por *design*, redefinindo o contrato social entre as *big techs* e as democracias contemporâneas (Paesani, Direito e Internet, 2013, p. 312; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 403).

9 CONCLUSÃO

A análise empreendida ao longo deste estudo permite concluir que a sociedade algorítmica impôs um desafio sem precedentes ao estatuto jurídico da infância, exigindo a superação definitiva da tese da neutralidade técnica dos provedores de aplicação. A síntese dos argumentos aqui expostos revela que o

grooming algorítmico não é um evento fortuito ou meramente atribuível a terceiros, mas uma externalidade negativa estrutural de um modelo de negócio fundado na economia da atenção e no perfilamento comportamental de vulneráveis (Zuboff, The age of surveillance capitalism, 2019, p. 8; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 453). A agência ativa dos algoritmos de recomendação, ao buscar a maximização do engajamento através do efeito de "toca de coelho", transmuta a plataforma de mera hospedeira em agente de governança e curadoria ativa, o que rompe com a lógica de imunidade prevista no Artigo 19 do Marco Civil da Internet (Gillespie, Custodians of the Internet, 2018, p. 84; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 413).

Nesse sentido, a hipótese científica aventada inicialmente resta plenamente confirmada: a curadoria algorítmica automatizada gera um dever de diligência específica que autoriza a responsabilização objetiva das plataformas por falhas de segurança sistêmicas. O diálogo entre a Doutrina da Proteção Integral (Art. 227, CF) e o Princípio do Melhor Interesse (Art. 14, LGPD) impõe que as empresas sejam reconhecidas como garantidoras do ambiente seguro, assumindo a responsabilidade primária e solidária pelos riscos que criam ao datificar a subjetividade infantojuvenil (Maciel, Curso de Direito da Criança e do Adolescente, 2021, p. 61; Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 296). A inobservância do dever de Safety by Design e de proteção por padrão (*by default*) caracteriza um vício na prestação do serviço, atraindo a incidência da Teoria do Risco da Atividade Digital e do regime protetivo do Código de Defesa do Consumidor (Tartuce, Direito das Obrigações e Responsabilidade Civil, 2017, p. 126; Teffé, Metaverso e infância, 2024, p. 612).

A responsabilidade jurídica reforçada das plataformas é o corolário lógico da assimetria informacional e técnica que define a hipervulnerabilidade algorítmica. Se o sistema possui precisão matemática para segmentar publicidade comportamental, a alegação de impossibilidade técnica para prevenir o aliciamento mediado por IA torna-se juridicamente insustentável, configurando uma omissão tecnológica reprovável (Pinheiro, Direito Digital, 2021, p. 147; Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 491). Portanto, o ordenamento brasileiro deve caminhar para uma regulação preventiva e procedimentalizada, alinhada às tendências internacionais como o *Digital Services Act*, exigindo auditorias algorítmicas e mecanismos eficazes de verificação etária que superem a mera autodeclaração fraudulenta (Biolcati, Internet, fake news e responsabilidade civil das redes sociais, 2022, p. 413; Teffé, Metaverso e infância, 2024, p. 614).

Em remate, o fechamento lógico desta investigação aponta que a liberdade de expressão não pode ser utilizada como um "cheque em branco" para a exploração econômica de crianças e adolescentes. O fortuito interno das redes sociais — o risco intrínseco ao aliciamento facilitado pelo *design* — deve ser absorvido por quem lucra com a arquitetura da rede (STJ, Súmula 479 apud Tartuce, 2017, p. 126). Como caminhos futuros de pesquisa, indica-se a necessidade de aprofundar o debate sobre a transparência

algorítmica e a responsabilidade civil no metaverso, onde a captura de dados biométricos e subconscientes elevará a vigilância a novos patamares de intrusividade, exigindo que o Direito Digital redefina, com urgência, as fronteiras entre a inovação tecnológica e a dignidade da pessoa humana (Teffé, Metaverso e infância, 2024, p. 748, 751; Vigliar, LGPD e a Proteção de Dados Pessoais na Sociedade em Rede, 2022, p. 425).

REFERÊNCIAS

AMIN, Andréa Rodrigues [et. al]; MACIEL, Kátia Regina Ferreira Lobo Andrade (Coord.). Curso de direito da criança e do adolescente: aspectos teóricos e práticos. 13. ed. São Paulo: Saraiva Educação, 2021..

BARROSO, Luís Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo: natureza jurídica, conteúdos mínimos e critérios de aplicação. Belo Horizonte: Fórum, 2013..

BIOLCATI, Fernando Henrique de Oliveira. Internet, fake news e responsabilidade civil das redes sociais. São Paulo: Almedina, 2022..

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020..

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988..

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, ..

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

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, ..

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

COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023. São Paulo: CGI.br, 2024..

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020..

FERREIRA, Rafael Freire. Autodeterminação informativa e a privacidade na sociedade da informação: atualizado com a LGPD. Rio de Janeiro: Lumen Juris, 2020..

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, fev. 2020..

GILLESPIE, Tarleton. Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media. New Haven: Yale University Press, 2018..

GRECO, Rogério. Curso de Direito Penal: parte geral. 24. ed. São Paulo: Atlas, 2022..

INSTITUTO ALANA. Proteção de crianças e adolescentes na Internet. São Paulo: Instituto Alana, 2024..

MACIEL, Kátia Regina Ferreira Lobo Andrade (Coord.). Curso de direito da criança e do adolescente: aspectos teóricos e práticos. 11. ed. São Paulo: Saraiva Educação, 2018..

MARTINS, Guilherme Magalhães. Responsabilidade civil por acidente de consumo na Internet. 2. ed. São Paulo: Revista dos Tribunais, 2014..

OLIVEIRA, Inessa; NUNES, Milena; SOUZA, Carlos. O discurso jornalístico na mediação de conflitos. *In*: Mediação, linguagem, comportamento e multiculturalismo. São Luís: Cultura, Direito e Sociedade, 2014..

PAESANI, Liliane Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. 6. ed. São Paulo: Atlas, 2013..

PINHEIRO, Patricia Peck. Direito digital. 7. ed. São Paulo: Saraiva Educação, 2021..

SARLET, Ingo Wolfgang. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988. 10. ed. Porto Alegre: Livraria do Advogado, 2019..

SCHREIBER, Anderson. Manual de Direito Civil Contemporâneo. 7. ed. São Paulo: SaraivaJur, 2024..

SEABRA, Gustavo Cives. Manual de Direito da Criança e do Adolescente. Belo Horizonte: CEI, 2020..

SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coords.). Direito e Internet III – tomo II: Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015..

TARTUCE, Flávio. Direito civil: direito das obrigações e responsabilidade civil. 12. ed. Rio de Janeiro: Forense, 2017. v. 2..

TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Foco, 2022..

TEPEDINO, Gustavo. Desafios da Lei Geral de Proteção de Dados (LGPD). Revista Brasileira de Direito Civil — RBDCivil, Belo Horizonte, v. 26, p. 11-15, out./dez. 2020..

VIGLIAR, José Marcelo Menezes (Coord.). LGPD e a proteção de dados pessoais na sociedade em rede: dados de crianças e adolescentes na Internet, tratamento de proteção de dados no comércio eletrônico, proteção de dados de falecidos, violação de direitos da personalidade e responsabilidade civil. São Paulo: Almedina, 2022..

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes cibernéticos: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013..

ZUBOFF, Shoshana. A Era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder. 1. ed. Rio de Janeiro: Intrínseca, 2021..