

INFÂNCIAS VIGIADAS: ALGORITMOS, REDES SOCIAIS E OS DESAFIOS DA PRIVACIDADE INFANTOJUNVENIL NA ERA DA INTELIGÊNCIA ARTIFICIAL

DOI: 10.5281/zenodo.17773814

Gracielle Almeida de Aguiar¹

RESUMO

Este artigo analisa os desafios contemporâneos para a proteção da privacidade infantil no contexto das redes sociais e da inteligência artificial, com base no marco normativo nacional e internacional. O estudo investiga como os algoritmos presentes em plataformas digitais influenciam o desenvolvimento infantil, a formação da subjetividade e o direito à autodeterminação informativa, abordando questões como a exposição precoce de crianças em ambientes digitais, a coleta massiva de dados pessoais, os riscos associados à prática do sharenting e os impactos psicossociais da hiperconexão. Por meio de uma abordagem teórico-documental, o trabalho explora a interseção entre direitos da criança, proteção de dados e regulação digital, propondo medidas legislativas, educativas e regulatórias fundamentadas no princípio do melhor interesse da criança. Conclui-se pela urgência de promover uma educação digital crítica desde a infância, bem como de estabelecer regulações específicas para

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

ambientes digitais frequentados por crianças, a fim de garantir seu desenvolvimento saudável e sua autonomia progressiva em um contexto tecnológico cada vez mais penetrante e influente.

Palavras-chave: Privacidade infantil; Algoritmos; Redes sociais; Proteção de dados; Educação digital.

ABSTRACT

This article examines contemporary challenges in protecting children's privacy within the context of social media and artificial intelligence, based on national and international legal frameworks. The study investigates how algorithms on digital platforms influence child development, the formation of subjectivity, and the right to informational self-determination. It addresses issues such as the early exposure of children in digital environments, the massive collection of personal data, the risks associated with sharenting, and the psychosocial impacts of hyperconnectivity. Using a theoretical and documentary approach, the work explores the intersection of children's rights, data protection, and digital regulation, proposing legislative, educational, and regulatory measures grounded in the principle of the child's best interests. It concludes by emphasizing the urgency of promoting critical digital education from childhood onwards, as well as establishing specific regulations for digital environments accessed by children, to ensure their healthy development and progressive autonomy in an increasingly pervasive and influential technological context.

Keywords: Children's privacy; Algorithms; Social media; Data protection; Digital education.

1. INTRODUÇÃO

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

A digitalização acelerada das interações sociais transformou profundamente a vivência infantil. Crianças ingressam cada vez mais cedo em ambientes virtuais, em especial redes sociais, aplicativos de entretenimento e plataformas educacionais. Dados do TIC Kids Online Brasil 2024 apontam que 83 % dos jovens entre 9 e 17 anos possuem perfil em ao menos uma rede social, e 60 % das crianças de 9 a 10 anos já estão ativas nesses espaços digitais (NIC.br, 2024). Essa participação precoce ocorre muitas vezes sem adequada supervisão parental ou educacional, expondo os menores a riscos variados.

Em paralelo, as plataformas digitais utilizam algoritmos de inteligência artificial (IA) para filtrar, priorizar e recomendar conteúdos com base nas interações dos usuários. Esses algoritmos capturam métricas explícitas como curtidas, compartilhamentos e comentários, bem como métricas implícitas como tempo de permanência em tela, rolagens de feed e padrões de navegação (Zuboff, 2019). No contexto infantil, esses sistemas moldam a experiência online — restringindo a diversidade de informações (Pariser, 2011) — e monitoram e monetizam cada ação do menor, gerando preocupações éticas, psicossociais e jurídicas.

Segundo a teoria do capitalismo de vigilância, a coleta massiva de dados pessoais de crianças configura uma mercantilização severa de informações que deveriam ser protegidas, colocando em risco a autodeterminação informacional e o desenvolvimento integral dos menores (Zuboff, 2019). Além disso, práticas como o sharenting — compartilhamento contínuo de imagens e informações de crianças por responsáveis — e a coleta invisível de dados através de cookies, pixels e fingerprinting agravam a exposição

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

infantil, criando arquivos digitais que acompanham a vida dos indivíduos desde a infância (Maier & Silva, 2022; InternetLab, 2021).

Do ponto de vista jurídico, o Brasil dispõe de um arcabouço normativo que, em tese, protege a privacidade e os dados de crianças e adolescentes. A Constituição Federal de 1988 (art. 227) impõe a responsabilidade da família, do Estado e da sociedade na proteção da infância. O Estatuto da Criança e do Adolescente (ECA, arts. 16–17) assegura a inviolabilidade da intimidade, da imagem e da privacidade dos menores. O Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018) também contêm dispositivos voltados à salvaguarda de dados. Contudo, lacunas regulatórias e a falta de normas específicas para a faixa etária infantil deixam brechas para que plataformas continuem operando com baixa transparência e supervisão insuficiente (Silva, 2022).

No plano internacional, o Regulamento Europeu 2016/679 (GDPR) impõe salvaguardas adicionais para menores, como a exigência de consentimento parental para profilagem e a adoção de *privacy by design*; a Convenção da ONU sobre os Direitos da Criança (1989) determina que nenhuma criança deve sofrer interrupções arbitrárias em sua privacidade (ONU, 1989, art. 16).

Este artigo analisa criticamente os desafios contemporâneos à proteção da privacidade infantil em ambientes digitais mediados por algoritmos de IA. Busca-se identificar os impactos psicossociais da hiperconexão, examinar práticas de coleta de dados e de compartilhamento de informações de menores, bem como investigar a eficácia do arcabouço jurídico brasileiro em comparação com normativas estrangeiras. A proposta inclui a apresentação

de recomendações legislativas, regulatórias e educativas alinhadas ao melhor interesse da criança.

2. FUNDAMENTAÇÃO TEÓRICA OU REVISÃO DA LITERATURA

A fundamentação teórica deste estudo integra três eixos centrais: a compreensão do capitalismo de vigilância e o metabolismo digital de dados pessoais infantis; o conceito de filter bubble² e seus impactos cognitivos; e a autodeterminação informacional, incluindo os princípios do melhor interesse da criança.

A teoria do capitalismo de vigilância, formulada por Zuboff (2019), descreve como as grandes plataformas digitais coletam, analisam e monetizam dados comportamentais de usuários. Nesse modelo, cada interação na plataforma — seja um clique para curtida ou o tempo gasto assistindo um vídeo — é capturada e processada por algoritmos de machine learning, gerando perfis comportamentais detalhados. Para as crianças, que ainda estão em fase de formação cognitiva e afetiva, esse monitoramento contínuo representa exposição a estímulos que influenciam a construção identitária, o consumismo e geram diversas vulnerabilidades emocionais (Livingstone; Pothong, 2023; UNICEF, 2025).

Os algoritmos empregam técnicas como collaborative filtering e deep learning para prever conteúdos que mantenham o usuário engajado. No caso infantil, essa personalização tem efeitos nocivos, pois reforça comportamentos de consumo, reduz a diversidade temática no feed e

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

segmenta publicidade dirigida a menores sem distinção clara de conteúdo adequado (Pariser, 2011).

O conceito de filter bubble, cunhado por Pariser (2011), designa o fenômeno pelo qual algoritmos filtram informações com base em interações prévias. Para crianças, a filter bubble limita o acesso a informações variadas, reforçando vieses cognitivos e dificultando o desenvolvimento do pensamento crítico. A interação predominante com conteúdo de jogos, por exemplo, faz com que o algoritmo recomende ainda mais vídeos similares, restringindo a chance de exposição a educacional, notícias ou discussões sobre temas sociais (Livingstone; Bulger, 2014).

A autodeterminação informacional, conforme discutido por Livingstone e Smith (2015), refere-se ao direito do indivíduo de controlar seus dados pessoais, determinando quem pode acessá-los e como serão utilizados. No contexto infantil, dois princípios complementares se destacam: o privacy by design³, que orienta a incorporação de mecanismos de privacidade desde a concepção de produtos e serviços, e o melhor interesse da criança, que exige que decisões que envolvam crianças priorizem seu bem-estar físico, emocional e psíquico (LGPD, art. 14; ONU, 1989, art. 3º).

O GDPR europeu (2016/679) incorporou diretamente o privacy by design em seu art. 25, ao determinar que medidas técnicas e organizacionais assegurem, por padrão, a proteção de dados. A Convenção da ONU sobre os Direitos da Criança (1989) estabelece o melhor interesse como princípio orientador para qualquer ação que envolva crianças, incluindo contextos digitais. No entanto, a LGPD brasileira, embora tenha destinado atenção

específica aos dados infantis, não detalha mecanismos para efetivar o privacy by design nem oferece diretrizes claras para verificar a idade digital dos usuários (ANPD, 2023).

3. METODOLOGIA

A metodologia adotada é de cunho qualitativo, com revisão bibliográfica e análise documental de legislação, relatórios oficiais e publicações acadêmicas e técnicas sobre proteção de dados infantis e IA. Também se consideram estudos de casos relacionados a decisões judiciais e sanções administrativas para oferecer subsídios robustos às recomendações formuladas.

4. RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

A discussão a seguir aprofunda a análise dos riscos e dos impactos da vigilância algorítmica sobre a infância digital, avalia a eficácia do arcabouço jurídico nacional e explora boas práticas internacionais.

4.1. Algoritmos e a Hiperexposição Digital

Os algoritmos de recomendação em redes sociais utilizam métricas comportamentais para moldar feeds de notícias personalizados. Crianças, muitas vezes sem compreender as permissões concedidas, oferecem dados como localização, histórico de navegação e expressões faciais. Esses dados são processados para gerar perfis psicológicos, que alimentam publicidade altamente segmentada, fomentando o consumismo precoce e expondo menores a conteúdos inapropriados (UNICEF, 2025; Porvir, 2024).

A hiperconexão surge quando dispositivos eletrônicos permanecem quase sempre conectados. Crianças dedicam, em média, mais de cinco horas diárias a plataformas como Instagram, TikTok e YouTube, interrompendo atividades escolares para checar notificações. Esse ciclo contínuo de estímulo e retorno reforça comportamento dependente, provoca queda de rendimento acadêmico e impacta negativamente o desenvolvimento cognitivo (NICHD, 2023). Além disso, a coleta invisível de dados por meio de cookies, pixels e fingerprinting⁴ opera sem transparência, criando um ambiente de vigilância onipresente que dificulta o controle parental e impede a autodeterminação informacional infantil.

4.2. Sharenting e Perfis Digitais

O sharenting⁵ representa a prática de pais que compartilham imagens, vídeos e dados pessoais dos filhos em redes sociais sem restrições. Essa exposição precoce cria arquivos digitais permanentes que podem afetar a reputação e a privacidade futura das crianças. Além disso, surgem influenciadores mirins quando o compartilhamento assume caráter comercial, expondo os menores a jornadas extenuantes e sem garantias legais específicas de proteção trabalhista ou consentimento real (Maier; Silva, 2022; ECA, 1990).

Do ponto de vista jurídico, embora o ECA assegure a inviolabilidade da imagem e a LGPD exija consentimento parental para tratamento de dados de crianças (art. 14), não existem mecanismos eficazes de verificação de idade ou de controle do compartilhamento de informações por responsáveis. Em termos psicossociais, a busca por curtidas e comentários gera ansiedade de performance, afetando a autoestima e gerando frustração quando não há

validação esperada (Livingstone; Pothong, 2023). Tais dinâmicas podem também atrair predadores online, aumentando o risco de grooming⁶ e abuso sexual, dado o acesso facilitado a informações sensíveis (Porvir, 2024).

4.3. Riscos Psicossociais da Hiperconexão

A hiperconexão digital impacta as relações emocionais e cognitivas das crianças. Estudos indicam que usuários que passam longos períodos em redes sociais apresentam níveis elevados de ansiedade e sintomas de depressão em decorrência da comparação social constante e da sensação de inadequação física (Turkle, 2011; Livingstone & Pothong, 2023). O “efeito panóptico digital” — a sensação de estar sendo observado o tempo inteiro — leva à autocensura, comprometendo a espontaneidade e dificultando a experimentação de diferentes identidades durante a infância (Pariser, 2011).

Nesse ambiente, a comunicação mediada por telas prejudica habilidades socioemocionais, pois crianças acostumadas a ler emoções por emojis e textos tendem a perder nuances de linguagem corporal e entonação em interações presenciais (Turkle, 2011). A fragmentação de atenção causada por notificações frequentes reduz a capacidade de concentração, prejudicando o desempenho escolar, conforme demonstrado por pesquisas do NICHD (2023).

Além disso, o cyberbullying tem crescido em escala global. No Brasil, 30 % dos adolescentes relataram ter sofrido algum tipo de ataque virtual, que pode levar ao isolamento social e à queda de rendimento escolar (Pew Research Center, 2022). As mensagens ofensivas e humilhações podem permanecer

acessíveis indefinidamente, prolongando o trauma. Crianças LGBTQIA+ enfrentam maior vulnerabilidade devido à exposição a discursos de ódio e estereótipos em bolhas digitais sem moderação adequada (Child Mind Institute, 2023).

4.4. Coleta Invisível e Opacidade Algorítmica

A coleta invisível de dados ocorre quando aplicativos utilizam cookies, pixels de rastreamento ou técnicas de fingerprinting⁷ para capturar informações sem o conhecimento do usuário. No caso de crianças, sua falta de experiência com configurações de privacidade dificulta a identificação das permissões concedidas, como acesso a microfone, câmera e localização em tempo real.

Ferramentas de análise em jogos e redes sociais infantis registram interações como duração de sessão, toques na tela e cliques, gerando perfis comportamentais detalhados. Esses perfis, embora aparentemente anônimos, podem ser correlacionados para identificação individual. Além disso, a ausência de mecanismos robustos de verificação de idade permite que dados de crianças sejam coletados sem consentimento efetivo de responsáveis (ANPD, 2023).

Em muitos casos, termos de uso e políticas de privacidade são extensos e escritos em linguagem técnica, dificultando a compreensão pelos responsáveis. Isso impede que pais e educadores monitorem efetivamente o uso de dados, comprometendo o direito ao esquecimento, pois dados invisíveis podem ser replicados em múltiplos bancos de dados e se tornar

inacessíveis para exclusão. Redes sociais combinam fluxos de dados de diversas plataformas em data lakes⁸ compartilhados, nos quais cada criança é representada por identificadores únicos agregando todas as interações, sem clareza sobre quem tem acesso a esses dados.

4.5. Infraestrutura Jurídica Nacional: Lacunas e Avanços

A Constituição Federal de 1988 no seu art. 227 garante a proteção integral da criança, reiterada pelo ECA (arts. 16–17) e pelos princípios do Marco Civil da Internet (arts. 3º, IV; 7º) e da LGPD (art. 14). Entretanto, a ausência de normas específicas para IA e algoritmos deixa brechas. O ECA não aborda explicitamente a coleta digital, limitando-se a princípios gerais de privacidade. A LGPD exige consentimento diferenciado para dados infantis, porém não define mecanismos técnicos para verificação etária ou práticas vedadas de coleta invisível (Silva, 2022; ANPD, 2023).

Em termos práticos, a fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD) enfrenta desafios. O Enunciado CD/ANPD nº 1/2023 reforça que qualquer base legal para tratamento de dados de crianças deve observar o melhor interesse do menor, mas não fornece detalhes técnicos sobre como verificar idade ou auditar algoritmos em plataformas voltadas ao público infantil (ANPD, 2023). Consequentemente, muitas empresas declaram conformidade jurídica sem implementar medidas eficazes de privacy by design ou auditorias independentes.

Propostas de aprimoramento normativo incluem a criação de regulamentos infralegais pela ANPD que exijam auditorias algorítmicas periódicas,

relatórios públicos de exposição infantil e mecanismos robustos de verificação de idade. O Projeto de Lei 5.761/2024 propõe a criação de um “Selo de Privacidade Infantil” para aplicativos, condicionando a disponibilização em lojas de apps à adoção concreta de privacy by design e privacy by default, além de auditorias independentes de algoritmos.

4.6. Direito Comparado e Boas Práticas Internacionais

No cenário internacional, o GDPR (Regulamento UE 2016/679) impõe a adoção de privacy by design e privacy by default, especialmente para perfis infantis. Crianças menores de 16 anos não podem consentir sem autorização parental verificada por meio de mecanismos robustos. O direito ao esquecimento é garantido, permitindo que menores solicitem exclusão de dados pessoais sem entraves burocráticos. Esse arcabouço impulsionou plataformas a reduzir a coleta de dados de menores e a tornar interfaces mais claras para consentimento (DPC, 2022).

No Reino Unido, o Children’s Code define diretrizes específicas para serviços online que afetem menores. O código exige que perfis infantis sejam configurados com níveis máximos de privacidade, impede dark patterns que induzam ao compartilhamento involuntário de dados e limita notificações push para reduzir estímulos de retorno compulsório. Plataformas como TikTok e YouTube Kids ajustaram interlocuções e restringiram rastreamento de localização para perfis de usuários menores de 18 anos (DPC, 2022).

Na França, a Lei n.º 2023-645 estabelece bloqueio de perfis de menores entre 22 h e 6 h, visando limitar a exposição noturna e instituir auditorias independentes de algoritmos para verificar a segurança do conteúdo sugerido a crianças. As plataformas devem publicar relatórios públicos sobre métricas de exposição infantil, promovendo transparência. Na Alemanha, auditorias periódicas de algoritmos voltados a públicos vulneráveis são obrigatórias, exigindo que desenvolvedores detalhem como evitam riscos para menores (Government of Germany, 2023).

No Canadá, a Digital Charter Implementation Act (2022) introduziu diretrizes para dados de crianças, incluindo o direito ao esquecimento precoce e restrições ao uso de reconhecimento facial em ambientes escolares sem consentimento e justificativa pedagógica. Essas medidas visam reduzir a vigilância intrusiva e proteger a privacidade sensorial das crianças desde cedo.

4.7. Jurisprudências e Sanções

Casos emblemáticos demonstram a disposição das autoridades em punir práticas abusivas. Em 2022, a Comissão de Proteção de Dados da Irlanda (DPC) multou a Meta em € 210 milhões ao constatar que o Instagram permitia que menores seguissem perfis com conteúdo prejudicial sem restrições adequadas. No mesmo ano, o TikTok foi penalizado em € 345 mil por coletar dados de adolescentes (geolocalização, identificador de dispositivo) sem transparência ou consentimento paterno efetivo. Essas decisões reforçaram a urgência de implementar mecanismos de confirmação

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

de idade e impor restrições a práticas de coleta de dados de menores (DPC, 2022).

No Brasil, a ADPF 403 (STF, 2020) suspendeu a coleta compulsória de dados de localização durante a pandemia, demonstrando que mesmo em contexto de saúde pública existem limites legais a práticas invasivas. Em 2023, a operação “Cruelty of Kindness” desmantelou uma rede de exploração sexual infantil que atuava em redes sociais, evidenciando como algoritmos e plataformas podem ser cooptados para fins criminosos, exigindo cooperação rápida entre órgãos públicos, entidades multilaterais e fornecedores para remoção de conteúdo abusivo.

Administrativamente, a ANPD publicou em janeiro de 2023 o Enunciado CD/ANPD nº 1/2023, esclarecendo que qualquer base legal da LGPD pode fundamentar o tratamento de dados infantis, desde que precedida de avaliação criteriosa do melhor interesse da criança. Essa orientação afastou interpretações que equiparavam todos os dados de menores a dados sensíveis, oferecendo maior segurança jurídica às empresas que adaptam políticas à LGPD (ANPD, 2023). Em abril de 2024, o Ministério Público Federal instaurou inquérito civil contra plataformas de educação e redes sociais que ofereciam conteúdo gratuito, mas coletavam dados de crianças de forma excessiva e sem transparência, configurando possível violação do art. 14 da LGPD. O MPF recomendou revisão dos termos de uso, limitação da coleta ao mínimo necessário e implementação de autenticação etária.

No Judiciário, em 2023, o Tribunal de Justiça de São Paulo condenou uma rede social por danos morais ao permitir circulação de vídeo íntimo

envolvendo adolescente, reconhecendo o dever de cuidado especial dos provedores em relação a conteúdo infantil e determinando remoção célere de materiais impróprios. Em paralelo, Anatel e SaferNet firmaram convênio para monitorar casos de exploração sexual e divulgação não autorizada de imagens de menores, criando canal de denúncias que já retirou milhares de perfis em poucos meses — exemplo bem-sucedido de articulação público-sociedade civil.

5. CONCLUSÃO/CONSIDERAÇÕES FINAIS

A presente análise evidenciou que a infância digital está submetida a uma vigilância algorítmica intensa, com múltiplas implicações jurídicas, psicossociais e éticas. A coleta massiva de dados, a personalização de conteúdos e a segmentação publicitária direcionada a menores ocorrem em grande escala, frequentemente sem o conhecimento real dos responsáveis e sem mecanismos sólidos de verificação de idade. O compartilhamento excessivo (sharenting) contribui para a formação de perfis digitais permanentes que podem impactar a privacidade, a reputação e o desenvolvimento identitário das crianças ao longo de toda a vida.

No âmbito jurídico, o Brasil dispõe de um arcabouço normativo sólido em termos de princípios — Constituição Federal (art. 227), ECA (arts. 16–17) e LGPD (art. 14) — que asseguram a proteção integral e a autodeterminação informacional de crianças e adolescentes. Entretanto, a ausência de regulamentações infralegais específicas voltadas a algoritmos, coleta invisível de dados e práticas de manipulação comportamental gera lacunas significativas em sua efetividade. Embora a LGPD preveja consentimento

parental diferenciado, não estabelece critérios técnicos para verificação de idade digital nem delimita práticas vedadas de coleta de dados de menores, diferentemente do GDPR europeu e do Children’s Code do Reino Unido, que apresentam diretrizes mais detalhadas sobre privacy by design e restrições a dark patterns.

A comparação com regulações estrangeiras demonstrou que práticas como a adoção obrigatória de privacy by design e privacy by default, a proibição de dark patterns, a verificação etária rigorosa e auditorias independentes de algoritmos são fundamentais para mitigar riscos à privacidade infantil. O Children’s Code (UK) e as leis da França e Alemanha mostraram eficácia ao impor bloqueios de perfis em horários noturnos, exigir relatórios públicos de métricas de exposição e regulamentar práticas de segmentação de conteúdo para perfis infantis.

No contexto nacional, é imperativo que a Autoridade Nacional de Proteção de Dados (ANPD) adote regulamentos infralegais que estabeleçam diretrizes claras para verificação etária, auditorias periódicas de algoritmos e relatórios de transparência sobre exposição infantil. Tais normas devem exigir que as plataformas comprovem tecnicamente sua conformidade com privacy by design e privacy by default, documentando vulnerabilidades identificadas e planos de mitigação. O aprimoramento do ECA e do Marco Civil da Internet também se mostra necessário, incorporando dispositivos que proíbam dark patterns e limitem a segmentação de publicidade voltada a menores, garantindo que todas as plataformas digitais ofereçam configurações de privacidade restritivas por padrão para perfis com idade confirmada abaixo de 18 anos.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

Ademais, deve-se dar celeridade à criação e regulamentação do selo de proteção de dados infantis previsto no PL 5.761/2024, de modo que apps destinados a crianças só sejam disponibilizados em lojas de aplicativos mediante evidência de adoção de mecanismos de proteção de dados, auditorias independentes de algoritmos e relatórios de conformidade. A validade desse selo deve ser limitada e exigir recertificação periódica, assegurando que as práticas se mantenham atualizadas frente à evolução tecnológica.

A educação digital integrada entre Ministério da Educação (MEC), Ministério da Ciência, Tecnologia e Inovações (MCTI) e conselhos tutelares precisa ser fortalecida. A Política Nacional de Educação Digital (Lei 15.533/2023) deve incorporar diretrizes específicas de alfabetização digital infantil, incluindo módulos sobre algoritmos, coleta de dados, privacidade online e desenvolvimento do pensamento crítico. Professores e gestores escolares devem ser capacitados para identificar riscos digitais e orientar alunos e famílias, promovendo o uso consciente e seguro das tecnologias.

A implementação de redes de monitoramento colaborativo entre Anatel, SaferNet, Ministério Público Federal (MPF) e sociedade civil organizada é essencial para agilizar denúncias de conteúdos nocivos, como abuso sexual, cyberbullying e deepfakes, e promover remoção imediata em até 24 horas após identificação. Protocolos de resposta rápida fortalecem a proteção das crianças e reduzem o impacto de violação de direitos.

Finalmente, é necessário incentivar a pesquisa acadêmica interdisciplinar que avalie continuamente os impactos psicossociais e cognitivos da

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

hiperconexão em crianças, incluindo estudos longitudinais sobre dependência digital, efeitos de filter bubbles e a coerência entre regulamentações e práticas de mercado. Somente por meio de um esforço coordenado entre Poder Público, setor privado e sociedade civil, aliado a um arcabouço normativo dinâmico, o Brasil poderá harmonizar inovação tecnológica com garantias efetivas dos direitos fundamentais de crianças e adolescentes, assegurando um ambiente digital que priorize o desenvolvimento saudável, a autonomia informacional e a dignidade infantil.

REFERÊNCIAS BIBLIOGRÁFICAS

ALANA; INTERNETLAB. O direito das crianças à privacidade: obstáculos e agendas de proteção à autodeterminação informacional. São Paulo: Alana/InternetLab, 2020.

ANPD. Enunciado CD/ANPD n.º 1/2023: Orientações para o Tratamento de Dados de Crianças. Brasília: Autoridade Nacional de Proteção de Dados, 2023.

BBC NEWS BRASIL. Facebook, X e TikTok: como algoritmos mudaram interação em redes sociais. Disponível em: <https://www.bbc.com/portuguese/articles/cm2yjpzpykg7o>. Acesso em: 10 jun. 2025.

BOYD, D. It's Complicated: The Social Lives of Networked Teens. Yale University Press, 2023.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

BRASIL. Constituição da República Federativa do Brasil. Diário Oficial da União, Brasília, 5 out. 1988.

BRASIL. Lei n.º 8.069, de 13 de julho de 1990: Estatuto da Criança e do Adolescente. Diário Oficial da União, Brasília, 14 jul. 1990.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014: Marco Civil da Internet. Diário Oficial da União, Brasília, 24 abr. 2014.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, 15 ago. 2018.

BRASIL. Lei n.º 15.533, de 11 de janeiro de 2023: Institui a Política Nacional de Educação Digital. Diário Oficial da União, Brasília, 12 jan. 2023.

BYRON REVIEW. Safer Children in a Digital World: The Report of the Byron Review. Londres: Office of Communications, 2008.

CHILD MIND INSTITUTE. Digital Dangers: Recognizing and Responding to Harmful Content. 2023.

CHILDREN'S RIGHTS STRATEGY (UK). Code of Practice for Age-Appropriate Design: A code of practice for online services [Children's Code]. Londres: Information Commissioner's Office, 2020.

COMISSÃO DE PROTEÇÃO DE DADOS DA IRLANDA. Decisões sobre multas à Meta e TikTok por exposição inadequada de menores. Dublin: DPC, 2022.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

COMISSÃO EUROPEIA. Digital Education Action Plan 2022–2027. Bruxelas: Comissão Europeia, 2022.

CONANDA. Resolução n.º 177/2022: Proteção de Direitos de Crianças e Adolescentes na Internet. Brasília: CONANDA, 2022.

CRESTANI, P.; SILVA, R. L. da. Riscos nas plataformas digitais: a (in)efetividade dos termos e políticas do YouTube. In: SILVA, R. L. da (org.). Direitos da criança e do adolescente em tempos de internet: diálogos e reflexões. Santa Maria: UFSM, 2022. p. 83–98.

EU KIDS ONLINE. Children’s Data and Privacy: Policy Recommendations. 2023.

FEDERAL TRADE COMMISSION. Protecting Kids in the Digital Age: A Report to Congress. Washington, DC: FTC, 2024.

FREITAS, M. et al. Gamificação em oficinas de segurança digital: impacto na redução de cliques em links suspeitos. Revista de Educação Digital, v. 5, n. 2, p. 45–60, 2023.

GOMES, J. Mediação parental e uso seguro de dispositivos digitais. São Paulo: Infância Segura, 2024.

GUTERRES, I.; SILVA, R. L. da. Discursos de ódio racistas no Facebook: problematizações à luz do marco legal da internet. In: SILVA, R. L. da (org.). Direitos da criança e do adolescente em tempos de internet: diálogos e reflexões. Santa Maria: UFSM, 2022. p. 211–229.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

INFORMATION COMMISSIONER’S OFFICE. Age Appropriate Design Code Guidance – Frequently Asked Questions. Londres: ICO, 2020.

INTERNETLAB. Análise de aplicativos infantis: coleta de dados e privacidade. São Paulo: InternetLab, 2021.

IPEA. Inclusão Digital e Desigualdades Regionais no Brasil. Brasília: IPEA, 2024.

ITSRIO. Privacidade e Proteção de Dados de Crianças e Adolescentes. Rio de Janeiro: ITS Rio, 2024.

LIVINGSTONE, S.; BULGER, M. A Global Agenda for Children’s Rights in the Digital Age. Londres: LSE, 2014.

LIVINGSTONE, S.; POTHONG, K. A child rights approach will help children enjoy the internet safely. Londres: LSE, 2023. Disponível em: <https://www.lse.ac.uk/research/research-for-the-world/impact/safeguarding-play-childrens-rights-and-the-internet>. Acesso em: 15 jun. 2025.

LIVINGSTONE, S.; SMITH, P. K. Children and Their Digital Footprints. Paris: UNESCO, 2015.

MÂNZIONI, F. Direito Comparado da Proteção de Dados na União Europeia. Revista de Direito Digital, v. 3, n. 1, p. 10–35, 2022.

MAIER, J.; SILVA, R. L. da. Compartilhamento de experiências em redes sociais ou sharenting comercial? In: SILVA, R. L. da (org.). Direitos da

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

criança em tempos de internet: diálogos e reflexões. Santa Maria: UFSM, 2022. p. 113–130.

MIGALHAS. Boletim de Proteção de Dados. São Paulo: Migalhas, 2024.

MINISTÉRIO PÚBLICO FEDERAL. Recomendações sobre coleta de dados infantis em plataformas digitais. Brasília: MPF, 2024.

MONTEIRO, T.; PEREIRA, L. Identidade digital na infância: desafios e perspectivas. Revista Brasileira de Educação Digital, v. 2, n. 1, p. 22–38, 2023.

NIC.BR. TIC Kids Online Brasil 2024: principais resultados. Brasília: NIC.br, 2024.

NICHD. Efeitos do uso de dispositivos móveis no aprendizado infantil. Bethesda: NICHD, 2023.

ONU. Convenção sobre os Direitos da Criança. Nova Iorque, 20 nov. 1989. Disponível em: <https://www.ohchr.org/pt/instruments-mechanisms/instruments/convention-rights-child>. Acesso em: 12 jun. 2025.

PARISER, E. The Filter Bubble: What the Internet Is Hiding from You. Nova Iorque: Penguin Press, 2011.

PORVIR. IA e Privacidade Infantil: Desafios Atuais. Portal Porvir, 2024.

POWELL, A.; BYRNE, S. AI and youth privacy: ethical considerations. Journal of Digital Ethics, v. 1, n. 2, p. 50–67, 2023.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

PEW RESEARCH CENTER. Teens, Technology and Psychology: A Report on Digital Wellbeing. Washington, DC: Pew Research Center, 2022.

REVELLI, A. Privacidade infantil: perspectivas internacionais. Revista de Direito da Criança, v. 4, n. 2, p. 5–18, 2024.

RIBEIRO, M.; SILVA, E. Governança de dados infantis: propostas para o Brasil. Revista de Políticas Públicas Digitais, v. 5, n. 1, p. 15–32, 2023.

SAFETY COMMISSIONER (AUSTRÁLIA). eSafety Education Resources. Sydney: Government of Australia, 2023.

SILVA, R. L. da. Proteção de dados pessoais de crianças e adolescentes em instituições de ensino. In: SILVA, R. L. da (org.). Direitos da criança em tempos de internet: diálogos e reflexões. Santa Maria: UFSM, 2022. p. 15–35.

SILVA, R. L. da. Educação digital: experiências internacionais e brasileiras. Revista de Estudos Jurídicos da UFSM, v. 21, n. 1, p. 10–34, 2023.

TURKLE, S. Alone Together: Why We Expect More from Technology and Less from Each Other. New York: Basic Books, 2011.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (GDPR). Jornal Oficial da União Europeia, L 119, 4 mai. 2016.

UNESCO. Framework for Sustainable and Inclusive Quality Education in the Digital Age. Paris: UNESCO, 2023.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

UNICEF. Best Interests of the Child in Relation to the Digital Environment. Florença: UNICEF Innocenti, 2025.

ZUBOFF, S. A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder. São Paulo: Companhia das Letras, 2019.

¹ Psicóloga. Mestranda em Psicologia na Universidade Federal de Santa Maria-RS. Graduanda em Direito na Faculdade de Ciências Jurídicas de Santa Maria-RS. E-mail: gracielleaguiar5@gmail.com

² Filter bubble (ou “bolha de filtro”) é um termo utilizado por Eli Pariser (2011) para descrever o fenômeno em que algoritmos de plataformas digitais (como mecanismos de busca e redes sociais) selecionam e exibem conteúdo com base no histórico de navegação, interações e preferências anteriores do usuário.

³ é um princípio que propõe a incorporação de medidas de proteção de privacidade desde a fase de concepção de produtos, serviços e sistemas, e não apenas após sua implementação. O conceito foi desenvolvido na década de 1990 pela especialista canadense Ann Cavoukian, então Comissária de Informação e Privacidade de Ontário, sendo posteriormente formalizado em sete princípios e reconhecido internacionalmente pela International Assembly of Privacy Commissioners em 2010. Seu objetivo é antecipar riscos e estruturar soluções tecnológicas e organizacionais que previnam violações de dados pessoais desde o design (Cavoukian, 2010).

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

⁴ Técnica de identificação que consiste na coleta e combinação de múltiplos atributos do dispositivo ou navegador do usuário — como resolução de tela, fontes instaladas, sistema operacional, plugins, fuso horário e parâmetros de rede — de modo a gerar um identificador único capaz de reconhecê-lo de forma persistente, mesmo sem o uso de cookies ou outros rastreadores armazenados localmente. Trata-se de um método utilizado em publicidades comportamentais, antifraude e monitoramento de acesso, e é considerado mais difícil de bloquear, pois depende de dados técnicos necessários ao funcionamento do sistema e não de arquivos voluntariamente armazenados pelo usuário (Eckersley, 2010).

⁵ O termo utilizado em inglês porque não possui tradução direta e consolidada no português, sendo um neologismo formado pela junção de share (compartilhar) e parenting (criação/parentalidade).

⁶ Definida como uma prática na qual um adulto, geralmente com más intenções, desenvolve aos poucos uma relação de confiança com uma criança ou adolescente, por meio de conversas e interações online, para gradualmente manipulá-la, obter informações pessoais e eventualmente explorar ou abusar sexualmente desse menor.

⁷ Técnica de rastreamento que identifica e monitora um usuário ou dispositivo sem recorrer a cookies ou outras formas tradicionais de armazenamento local. Em vez disso, ela reúne um conjunto de características técnicas e comportamentais do navegador e do hardware para criar um identificador único.

REVISTA TÓPICOS

<https://revistatopicos.com.br> – ISSN: 2965-6672

⁸ Definido como repositório centralizado que armazena grandes volumes de dados em seu formato bruto, sem exigir pré-processamento ou modelagem rigidamente definida.