REVISTA ELETRÔNICA
IURIS NOVARUM / ISSN 2764-247X

UNIR UNIVERSIDADE FEDERAL DE RONDÔNIA

PORTAL DE PERIÓDICOS · UNIR / PROPESQ periodicos.unir.br

ARTIGO

GROOMING NO AMBIENTE VIRTUAL: DESAFIOS PARA A PROTEÇÃO DE CRIANÇA E ADOLESCENTE E PARA A INVESTIGAÇÃO CRIMINAL NO BRASIL

Elimei Paleari do Amaral CAMARGO[1]
Emanuele Giachini BOTELHO[2]
Maurício Rogério BOTELHO[3]

DIREITO DIGITAL · PROTEÇÃO INTEGRAL · INVESTIGAÇÃO CRIMINAL

RESUMO

O presente artigo analisa os desafios jurídicos e investigativos no combate ao grooming (aliciamento virtual) contra crianças e adolescentes no Brasil. A transição para a sociedade da informação reconfigurou as dinâmicas de socialização, expondo o público infantojuvenil a uma condição de hipervulnerabilidade no ciberespaço, decorrente tanto do desenvolvimento neurocognitivo incompleto quanto da lógica do capitalismo de vigilância. Fundamentando-se na sociologia de Zygmunt Bauman sobre a modernidade líquida e na ética do Princípio Responsabilidade de Hans Jonas, o estudo discute como o anonimato e a fluidez das identidades digitais facilitam a criação de vínculos de "confiança enganosa" para fins de exploração sexual.

Embora o ordenamento jurídico brasileiro seja balizado pela Doutrina da Proteção Integral e pelo Princípio da Prioridade Absoluta (Art. 227, CF/88), a investigação criminal enfrenta obstáculos severos, como a volatilidade da prova eletrônica, a transnacionalidade das redes e a morosidade dos ritos judiciais frente à velocidade das interações virtuais. Analisou-se a eficácia de mecanismos como a infiltração policial virtual (Lei nº 13.441/2017) e as recentes atualizações do ECA Digital (Lei nº 15.211/2025). Conclui-se que a repressão isolada é insuficiente, sendo imperativa uma convergência entre o rigor legislativo, o Safety by Design nas plataformas tecnológicas e a promoção do letramento digital como política pública de prevenção.

Palavras-chave: *Grooming; Proteção Integral; Direito Digital; Investigação Criminal; Sociedade da Informação.*

ABSTRACT

This article analyzes the legal and investigative challenges in combating virtual grooming against children and adolescents in Brazil. The transition to the information society has reconfigured socialization dynamics, exposing the youth to a state of hyper-vulnerability in cyberspace, stemming from both incomplete neurocognitive development and the logic of surveillance capitalism. Based on Zygmunt Bauman's sociology of liquid modernity and Hans Jonas's Ethics of the Imperative of Responsibility, the study discusses how anonymity and the fluidity of digital identities facilitate the creation of "deceptive trust" bonds for sexual exploitation purposes.

Although the Brazilian legal system is guided by the Doctrine of Integral Protection and the Principle of Absolute Priority (Art. 227, Federal Constitution), criminal investigation faces severe obstacles, such as the volatility of electronic evidence, the transnational nature of networks, and the sluggishness of judicial proceedings compared to the speed of virtual interactions. The effectiveness of mechanisms such as virtual police infiltration (Law No. 13.441/2017) and recent updates to the Digital ECA (Law No. 15.211/2025) was analyzed. The study concludes that isolated repression is insufficient, requiring a convergence between legislative rigor, Safety by Design in technological platforms, and the promotion of digital literacy as a public prevention policy.

Keywords: *Grooming; Integral Protection; Digital Law; Criminal Investigation; Information Society.*

INTRODUÇÃO

A transição para a denominada sociedade da informação reconfigurou profundamente as dinâmicas de socialização de crianças e adolescentes. No cenário contemporâneo, o ciberespaço deixou de ser uma ferramenta acessória para tornar-se uma extensão da própria realidade concreta, onde esse público, em pleno processo de formação neurológica e emocional, habita um ecossistema de hiperconectividade. Esta imersão digital, contudo, revela uma "hipervulnerabilidade" infantojuvenil, acentuada pelo desenvolvimento incompleto de funções cognitivas e pelo controle de impulsos ainda em maturação.

Nesse contexto, o ambiente virtual não se apresenta como um espaço neutro, mas como um território que potencializa riscos sistêmicos, sendo o aliciamento virtual, ou grooming[4], uma de suas faces mais insidiosas. O agressor utiliza-se do anonimato e de sofisticadas técnicas de manipulação psicológica para construir uma "confiança enganosa", explorando a curiosidade e a necessidade de afeto da vítima para fins de exploração sexual. A complexidade desse fenômeno exige uma análise que ultrapasse a técnica jurídica, buscando nos fundamentos da ética tecnológica de Zygmunt Bauman e Hans Jonas o suporte para compreender a fluidez das identidades digitais e a responsabilidade necessária diante do poder tecnológico.

O problema central desta pesquisa reside em questionar se o ordenamento jurídico brasileiro e os atuais mecanismos de investigação criminal são efetivamente suficientes para prevenir e reprimir o grooming, aliciamento virtual, praticado contra crianças e adolescentes no ambiente virtual. A hipótese levantada é que, embora o Brasil possua normas protetivas robustas — como a Doutrina da Proteção Integral e o Princípio da Prioridade Absoluta (Art. 227, CF/88) — a natureza transnacional da rede, o anonimato digital e as dificuldades técnicas na preservação da prova eletrônica constituem obstáculos severos à eficácia da repressão estatal.

Os objetivos deste trabalho consistem em analisar a transformação das relações sociais pela internet e a vulnerabilidade do menor; fundamentar a necessidade de uma ética de preservação baseada na "Heurística do Medo" de Jonas; e examinar os desafios operacionais da investigação criminal, como a volatilidade da prova digital e a morosidade dos ritos judiciais frente à velocidade das interações virtuais. Por meio de uma revisão bibliográfica e documental, busca-se demonstrar que a proteção integral no ciberespaço exige não apenas punição, mas uma convergência entre Direito, tecnologia e letramento digital.

1. A VULNERABILIDADE INFANTOJUVENIL NA SOCIEDADE DA INFORMAÇÃO

A transição para a denominada sociedade da informação reconfigurou profundamente as dinâmicas de socialização e desenvolvimento de crianças e adolescentes, que agora habitam um ambiente onde o ciberespaço não é apenas uma ferramenta, mas uma extensão da realidade concreta. Inseridos em um panorama de hiperconectividade, esses grupos encontram-se em pleno processo de formação neurológica, emocional e social, o que lhes confere uma vulnerabilidade agravada ou "hipervulnerabilidade" no ecossistema digital (Maciel, 2021).

Sob a ótica da neurociência, essa condição decorre do desenvolvimento incompleto do córtex pré-frontal, região cerebral responsável por funções cognitivas complexas, tomadas de decisão racionais e, fundamentalmente, pelo controle de impulsos e emoções, que termina de se desenvolver apenas por volta dos 25 anos de idade. Consequentemente, a ausência de um controle inibitório consolidado e de um senso crítico plenamente maduro torna os menores alvos estratégicos de um sistema que opera sob a lógica do "capitalismo de vigilância", o qual frequentemente transforma a infância em mercadoria e lucra com a exploração da subjetividade desses indivíduos (Grossi, 2024).

O ambiente digital, portanto, não pode ser compreendido como um espaço neutro ou meramente lúdico; ele funciona como um território que reflete e potencializa as desigualdades e violências estruturais já presentes na sociedade. A arquitetura das plataformas digitais, muitas vezes desenhada para maximizar o tempo de tela e a coleta massiva de dados, acaba por expor o público infantojuvenil a riscos sistêmicos, como a desinformação, a publicidade abusiva e, de forma mais insidiosa, o aliciamento virtual, grooming (Estudos Universitários, 2025).

No grooming, aliciamento virtual, o agressor utiliza-se do anonimato e da manipulação psicológica para criar uma "confiança enganosa", explorando a necessidade de afeto e a curiosidade inerente à idade da vítima para conduzi-la ao abuso sexual online ou offline. Diante dessa "adultização" precoce e da fragilidade dos mecanismos de controle parental, a proteção desses sujeitos no meio digital deixa de ser uma mera opção ética para se tornar um dever jurídico e constitucional, pautado na Doutrina da Proteção Integral e no Princípio da Prioridade Absoluta, conforme preceitua o Art. 227 da Constituição Federa de 1988 (Revista Caderno Pedagógico, 2025).

2. FUNDAMENTOS DA ÉTICA TENOLÓGICA: BAUMAN E JONAS

Para compreender a complexidade das relações no ambiente virtual, é imperativo recorrer à sociologia de Zygmunt Bauman. Em sua tese sobre a modernidade líquida, o autor descreve uma transição civilizatória onde as estruturas sólidas de convivência e as instituições tradicionais perdem sua rigidez, dando lugar a vínculos marcados pela transitoriedade e pela superficialidade. No ecossistema digital, essa "liquidez" manifesta-se de forma aguda na construção de identidades. A rede permite que os sujeitos se apresentem de forma fragmentada, permitindo que o agressor assuma personas fictícias, perfis fakes para estabelecer laços de "confiança enganosa" com o menor.

Nesse cenário, a identidade deixa de ser um dado estável para tornar-se um projeto contínuo e volátil, sujeito exclusivamente à "intensidade do jogo conexão-desconexão". Essa facilidade de mimetização é um dos principais vetores que facilitam o aliciamento virtual (grooming), uma vez que o agressor, protegido pelo anonimato e pela falta de barreiras físicas, consegue isolar a criança de seu círculo protetor real, operando em zonas da rede de difícil detecção, como a dark web. A vida líquida, portanto, potencializa o risco de que crianças e adolescentes, em busca de aceitação e pertencimento, tornem-se alvos de manipulações afetivas sofisticadas que visam a exploração sexual ou a pornografia infantil.

Complementarmente, a ética de Hans Jonas e seu "princípio responsabilidade" oferecem a fundamentação necessária para uma tutela jurídica que transcenda a imediatidade da rede. Jonas argumenta que o poder tecnológico moderno atingiu tal escala que suas consequências superam a imaginação moral tradicional, exigindo uma nova ética que visualize os efeitos futuros e irreversíveis das ações humanas. Na sociedade da informação, o agir sob "aguda incerteza" onde os algoritmos e a coleta massiva de dados operam de forma opaca impõe ao Estado, à família e à sociedade o dever de adotar a denominada "Heurística do Medo" (Jonas, 1984).

Este postulado jonasiano sugere que, diante de tecnologias cujos riscos são potencialmente catastróficos para o desenvolvimento humano, deve-se priorizar a "profecia de ruína" sobre a de felicidade, estabelecendo uma ética de preservação e prevenção. No contexto jurídico brasileiro, esse princípio harmoniza-se com a Doutrina da Proteção Integral, que exige o resguardo preventivo do menor de toda forma de negligência, violência e exploração. Assim, a responsabilidade estatal e social pela segurança digital não é apenas administrativa, mas um imperativo categórico que visa proteger o ser humano em sua condição mais vulnerável e "em desenvolvimento" (Bauman, 1997).

O ordenamento jurídico brasileiro, ancorado no Art. 227 da Constituição Federal, alça a criança e o adolescente ao status de prioridade absoluta, consolidando o dever coletivo e solidário entre a família, a sociedade e o Estado visando assegurar-lhes a dignidade e a segurança (Brasil, 1988). Esta norma rompeu definitivamente com a antiga "doutrina da situação irregular", que enxergava o menor apenas como objeto de repressão, para reconhecê-lo como sujeito pleno de direitos.

No ambiente digital, a aplicação desse "tripé de corresponsabilidade" exige que as plataformas tecnológicas e os desenvolvedores de sistemas também sejam integrados ao sistema de garantia de direitos. A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, e o Marco Civil da Internet, Lei nº 12.965/2014, materializam esse dever ao estabelecer diretrizes para o tratamento de dados de menores no seu "melhor interesse" e ao prever mecanismos de controle parental para mitigar riscos. A proteção integral, portanto, deixa de ser um conceito abstrato para tornar-se um comando jurídico ativo que demanda vigilância constante contra o anonimato malicioso e a transnacionalidade dos crimes digitais.

3. O ARTIGO 227 DA CF/88 E A DOUTRINA DA PROTEÇÃO INTEGRAL

O ordenamento jurídico brasileiro, sob a égide da "Constituição Cidadã" de 1988, estabeleceu um marco regulatório revolucionário ao colacionar, de forma inédita, um rol de direitos dos quais são titulares todas as crianças e adolescentes, instituindo o que a doutrina denomina como uma verdadeira "Declaração dos Direitos e Garantias Infantojuvenis Fundamentais". Ancorado no Art. 227 da Carta Magna, o sistema jurídico passou a operar sob o princípio da prioridade absoluta, que impõe à família, à sociedade e ao Estado o dever solidário de assegurar ao menor o direito à vida, saúde, dignidade e convivência familiar, colocando-os a salvo de toda forma de negligência, exploração e violência (Brasil, 1988).

Este novo paradigma representou uma ruptura definitiva com a antiga "Doutrina da Situação Irregular" (consolidada pelos Códigos de Menores de 1927 e 1979), que tratava crianças e adolescentes apenas como objetos de intervenção estatal e medidas punitivas quando em estado de abandono ou criminalidade. Em substituição, a Doutrina da Proteção Integral elevou-os ao status de sujeitos plenos de direitos, reconhecendo sua condição peculiar de pessoa em desenvolvimento. No contexto da sociedade da informação, essa proteção integral exige uma interpretação dinâmica e adaptativa. O ambiente digital não é mais um espaço apartado, mas uma extensão da realidade onde a vulnerabilidade desse grupo é agravada pela hiperconectividade, exigindo que o Estado atue preventivamente contra novas formas de violação, como o aliciamento e a exploração de dados.

Para garantir a efetividade dessa proteção no ciberespaço, as normas do Estatuto da Criança e do Adolescente (ECA) e da Lei Geral de Proteção de Dados (LGPD) devem ser aplicadas de forma concomitante e sinérgica. O Art. 14 da LGPD estabelece que o tratamento de dados pessoais de menores deve ser realizado estritamente em seu "melhor interesse", pautado pelo princípio da transparência e pela necessidade de consentimento específico e em destaque por parte dos responsáveis legais (Brasil, 2018). Ademais, a elevação da proteção de dados pessoais à categoria de direito fundamental, por meio da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, reforça a necessidade de blindar a privacidade infantojuvenil contra o perfilamento algorítmico[5] e a exploração comercial (Brasil, 2022).

Nesse cenário, emerge o conceito de "Safety by Design"6 ou "Rights by Design", conforme preconizado pela Resolução nº 245/2024 do Conselho Nacional da Criança e do Adolescente - CONANDA. As empresas provedoras de serviços digitais detêm a responsabilidade ética e jurídica de conceber produtos e interfaces que integrem salvaguardas de proteção desde a sua concepção técnica, garantindo ambientes apropriados a cada faixa etária e minimizando riscos sistêmicos de forma proativa. Somente através dessa abordagem integrada que une o rigor legislativo, a fiscalização da Autoridade Nacional de Proteção de Dados (ANPD) e o compromisso das plataformas será possível converter a promessa constitucional de proteção integral em uma realidade palpável para as novas gerações no mundo conectado (Henriques; Ribeiro, 2025).

4. O ANONIMATO E OS DESAFIOS DA INVESTIGAÇÃO DO GROOMING

O anonimato proporcionado por redes sociais e, de maneira proeminente, por jogos online, atua como um catalisador fundamental para a prática do aliciamento virtual. Conforme aponta Castelo Branco (2025), os criminosos virtuais aproveitam-se do fato de estarem ocultos "por trás de uma câmera ou de algum elemento" para predar suas vítimas, o que gera uma pseudossensação de impunidade. Esse ambiente permite que o agressor utilize o "jogo de máscaras" do ciberespaço, operando em zonas onde a fiscalização ainda é insuficiente e a identidade pode ser facilmente forjada através de perfis falsos (fakes) que mimetizam a idade e os interesses do público infantojuvenil.

Em plataformas de jogos e comunidades adjacentes, como o Discord ou Twitch, predadores sexuais utilizam-se de técnicas sofisticadas de engenharia social e manipulação emocional. O processo de grooming, aliciamento virtual, envolve o desenvolvimento de uma "confiança enganosa", na qual o infrator, agindo de forma carinhosa e paciente, cria laços de amizade para isolar o menor de seu círculo protetor real. O objetivo é a dessensibilização sexual gradual da vítima, muitas vezes culminando na exigência de conteúdos íntimos ou na proposição de encontros físicos.

A hipótese de que o anonimato e a transnacionalidade da rede são obstáculos à eficácia da prova eletrônica encontra respaldo na extrema complexidade técnica da investigação forense. A identificação do sujeito ativo é rotineiramente dificultada pelo emprego de tecnologias de despersonalização, como o uso de disfarces no endereço de IP, roteadores abertos e programas de mascaramento ou falsificação de localização. Segundo Emmerich (2017), a criminalidade virtual caracteriza-se por uma "alta tecnicidade de proteção de dados", onde o uso de criptografia avançada e sistemas de encriptação torna o rastreamento da produção de provas uma tarefa de execução morosa e incerta.

Além disso, a acessibilidade do mundo virtual permite que ações criminosas sejam executadas em nanosegundos, o que contrasta com a lentidão dos mecanismos de requisição de dados. A prova digital é marcada por sua volatilidade. Se não houver uma preservação imediata dos vestígios eletrônicos e dos protocolos de internet, os criminosos podem apagar evidências ou desfazer-se das máquinas utilizadas antes que o Poder Judiciário autorize a quebra de sigilo telemático.

A natureza globalizada da internet impõe desafios de competência territorial quase intransponíveis em casos isolados. É comum que agressores operem a partir de outras jurisdições ou utilizem servidores hospedados em países estrangeiros, o que demanda o acionamento de mecanismos de cooperação internacional via Interpol ou cartas rogatórias. Contudo, esse processo de intercâmbio policial e jurídico costuma demorar meses para ser concretizado, o que implica graves riscos à integridade física e psíquica da vítima, que permanece vulnerável durante o lapso temporal da investigação (Fernandes, 2019; Araújo, 2017).

Embora o Brasil tenha avançado com a Lei nº 13.441/2017, que permite a infiltração de agentes policiais no ambiente virtual para investigar crimes contra a dignidade sexual de crianças e adolescentes, a medida ainda enfrenta barreiras operacionais. A necessidade de treinamento especializado, o subfinanciamento das delegacias de repressão a crimes cibernéticos e a resistência de certas plataformas digitais em colaborar sem ordens judiciais específicas limitam a eficácia da repressão ao grooming. Assim, o conflito entre a proteção da privacidade e a necessidade de segurança digital exige uma regulação dinâmica que acompanhe a velocidade das inovações tecnológicas para garantir a efetiva punição dos infratores (Troiano, 2025).

5. INSUFICIÊNCIA DOS MECANISMOS DE INVESTIGAÇÃO E PERSPECTIVAS.

Embora o Brasil tenha consolidado avanços normativos significativos, como a Lei nº 13.441/2017, que introduziu no Estatuto da Criança e do Adolescente (ECA) a permissão para a infiltração de agentes policiais em ambientes virtuais, a efetividade prática desta medida permanece aquém do ideal. Esta normativa surgiu da necessidade imperativa de obter provas em casos de crimes contra a dignidade sexual infantojuvenil, permitindo que o Estado adentre não apenas a "internet superficial", mas também camadas como a deep web, onde o anonimato é sistematicamente utilizado para a prática de ilícitos.

Entretanto, a aplicação desta técnica enfrenta obstáculos estruturais severos. Observa-se que a proteção infantil frequentemente depende de ações fragmentadas entre os setores público e privado, sofrendo com o subfinanciamento das agências de aplicação da lei e a carência de pessoal qualificado. Dados indicam que aproximadamente 34% das capitais brasileiras ainda não contam com delegacias especializadas em crimes cibernéticos, o que desestimula denúncias e compromete a resposta rápida exigida pela volatilidade do meio digital. Ademais, a infiltração policial exige autorização judicial circunstanciada e não pode ser admitida se a prova puder ser obtida por outros meios, o que impõe um rigor procedimental que nem sempre acompanha a agilidade dos aliciadores (Luna; Brito, 2025).

O Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios e garantias fundamentais para o uso da rede no Brasil, priorizando a proteção à privacidade e ao sigilo das comunicações. Todavia, esse arcabouço gera uma tensão dialética no âmbito investigativo: enquanto o Art. 10 garante a reserva de jurisdição para a quebra de sigilo de dados, a extrema volatilidade da prova digital exige uma celeridade que o rito judicial muitas vezes não alcança (Brasil, 2014). Crimes virtuais, como o grooming, operam em nanossegundos, permitindo que agressores apaguem vestígios ou ocultem seus endereços de IP através de técnicas de criptografia e mascaramento antes mesmo que a ordem judicial seja cumprida (Emmerich, 2017).

A diferenciação entre dados estáticos (cadastrais) e dados dinâmicos (logs de conexão e conteúdo) é central nesta discussão. Embora autoridades policiais possam requisitar dados cadastrais diretamente às plataformas, o acesso aos registros de conexão e ao conteúdo das comunicações depende estritamente de decisão judicial, o que pode levar meses. Esse lapso temporal, aliado à resistência de plataformas estrangeiras em colaborar com as autoridades nacionais sem a intermediação de cartas rogatórias, cria zonas de impunidade que vulnerabilizam ainda mais o menor.

Diante do descompasso entre a legislação de 1990 e a evolução tecnológica, surge a Lei nº 15.211/2025 (ECA Digital) como uma tentativa de atualizar o arcabouço protetivo. Esta nova legislação prevê mecanismos de segurança reforçados por design (Safety by Design), obrigando as plataformas a oferecerem configurações padrão seguras para perfis de menores e estabelecendo parâmetros rigorosos para a coleta de dados de crianças e adolescentes. A nova norma busca integrar as diretrizes do Comentário Geral nº 25 da ONU, reforçando que os direitos de cada criança devem ser respeitados e realizados integralmente também no ambiente digital (Brasil, 2025).

Contudo, a eficácia do ECA Digital está intrinsecamente ligada à capacidade de fiscalização do Estado, em especial da Autoridade Nacional de Proteção de Dados (ANPD), e à construção de um ecossistema que penalize de forma severa as falhas na moderação de conteúdo e na verificação etária (age gate). Projetos como o PL 2.628/2022 corroboram essa tendência ao propor deveres específicos para plataformas, como o bloqueio automático de conteúdos abusivos e restrições a algoritmos que promovam a "adultização" ou o engajamento viciante de menores (Brasil, 2022).

A repressão ao grooming não pode esgotar-se na via punitiva. A literatura acadêmica e as diretrizes internacionais, como as da União Internacional de Telecomunicações (UIT), apontam que o sucesso da prevenção depende de um esforço coordenado entre governos, empresas de tecnologia, famílias e escolas. O letramento digital deve ser promovido como uma política pública de alfabetização que capacite não apenas os jovens, mas também pais e educadores a identificar e responder aos sinais insidiosos de violência digital.

Finalmente, a natureza global do ciberespaço exige o fortalecimento da cooperação internacional e a adesão a padrões normativos globais, como os previstos na Convenção de Budapeste. Sem um marco regulatório padronizado que facilite a responsabilização de criminosos que operam em múltiplas jurisdições, a luta contra o aliciamento virtual continuará a ser, em muitos aspectos, um esforço assimétrico. A segurança online deve transcender o caráter de mera proteção administrativa para transformar-se em um instrumento de cidadania digital e progresso social.

CONCLUSÃO

A presente investigação permitiu concluir que o fenômeno do grooming no ambiente virtual não é apenas um desafio técnico-jurídico, mas uma crise ética profunda que emerge das entranhas da sociedade da informação. A transição da modernidade para uma era de "liquidez" sistêmica, como preconizado por Zygmunt Bauman, fragilizou os vínculos de proteção tradicionais, permitindo que a arquitetura do ciberespaço se tornasse um terreno fértil para a manipulação e o aliciamento.

Ao longo deste estudo, ficou evidente que a criança e o adolescente habitam o ecossistema digital em uma condição de hipervulnerabilidade. Esta não decorre apenas de um desenvolvimento neurocognitivo ainda em formação, mas de um sistema que opera sob a lógica do capitalismo de vigilância, transformando a subjetividade juvenil em dado comercial e, por vezes, em alvo de predação. A aplicação do Princípio Responsabilidade de Hans Jonas revela-se, portanto, urgente: diante da incerteza e do potencial catastrófico das novas tecnologias sobre a dignidade sexual dos menores, o Estado e a sociedade devem adotar uma postura de prevenção ativa — a "heurística do medo" — priorizando a proteção da vida futura sobre a conveniência tecnológica imediata.

No que tange ao ordenamento jurídico brasileiro, observa-se um paradoxo. Se, por um lado, o país possui um arcabouço normativo robusto, ancorado na Doutrina da Proteção Integral e no Art. 227 da Constituição Federal, por outro, a eficácia desse sistema é severamente limitada pela realidade operacional. A investigação criminal do grooming enfrenta obstáculos quase intransponíveis:

- A volatilidade da prova digital e o anonimato sofisticado dos agressores;
- A lentidão dos ritos judiciais frente à velocidade de "nanossegundos" das interações virtuais;
- A barreira da transnacionalidade, onde a soberania nacional colide com a resistência de plataformas estrangeiras e a demora da cooperação internacional.

Embora iniciativas como a Lei 13.441/2017 (infiltração policial virtual) e o recente ECA Digital (Lei 15.211/2025) representem avanços necessários na atualização do Direito, a repressão isolada mostra-se insuficiente. A hipótese inicial deste trabalho confirmou-se: a natureza transnacional e o anonimato digital ainda superam a capacidade de resposta imediata do Estado brasileiro.

Em última análise, a proteção de crianças e adolescentes no ciberespaço exige uma convergência entre o Direito, a Tecnologia e a Educação. Não basta punir o infrator; é preciso que as plataformas incorporem o Safety by Design como imperativo categórico e que o letramento digital se torne uma ferramenta de emancipação e autodefesa para as novas gerações. Somente através de uma responsabilidade compartilhada e solidária será possível garantir que o ambiente virtual deixe de ser um território de incertezas para tornar-se, efetivamente, um espaço de desenvolvimento digno e seguro.

NOTAS

[4] grooming (ou aliciamento infantil online) refere-se ao processo de manipulação e construção de um laço de confiança feito por um adulto junto a uma criança ou adolescente, com o objetivo de reduzir as inibições da vítima e prepará-la para uma futura exploração sexual.

[5] perfilamento algorítmico (ou algorithmic profiling) é o processo de utilização de algoritmos e técnicas estatísticas para analisar, agrupar e prever o comportamento, características ou interesses de indivíduos com base nos seus dados digitais.

[6] Safety by Design: Refere-se à integração proativa de medidas de segurança em todas as etapas de desenvolvimento de produtos e serviços digitais. No contexto da Resolução nº 245/2024 do CONANDA, exige que plataformas identifiquem e mitiguem riscos (como exploração e conteúdos inadequados) de forma preventiva, garantindo que o ambiente digital seja seguro para crianças e adolescentes por configuração padrão (default).

REFERÊNCIAS

AMIN, Andréa Rodrigues. Doutrina da proteção integral. In: 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.

ARAÚJO, José Fábio Rodrigues. Cooperação Jurídica Internacional: pedidos de assistência e provas digitais. 2. ed. São Paulo: Revista dos Tribunais, 2017.

BAUMAN, Zygmunt. Ética Pós-Moderna. Tradução de João Rezende Costa. São Paulo: Paulus, 1997.

BAUMAN, Zygmunt. Modernidade Líquida. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. Vida Líquida. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Ed., 2007.

BOTELHO, Marcos César. A legitimidade da jurisdição constitucional no pensamento de Jürgen Habermas. São Paulo: Saraiva, 2010.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei nº 13.441, de 16 de junho de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet. Brasília, DF: Presidência da República, 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. Lei nº 15.211, de 12 de março de 2025. Institui o ECA Digital e dá outras providências. Diário Oficial da União, Brasília, 2025.

CASTELLS, Manuel. A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CASTELO BRANCO, Pedro H. B. O anonimato como catalisador do aliciamento em jogos eletrônicos. Revista de Direito Digital e Novas Tecnologias, São Paulo, v. 10, n. 2, 2025.COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023. São Paulo: CGI.br, 2024.

CONSELHO Nacional dos Direitos da Criança e do Adolescente (Conanda). Resolução nº 245, de 5 de abril de 2024. Estabelece diretrizes para a promoção e a proteção dos direitos de crianças e adolescentes no ambiente digital. Brasília, DF: Diário Oficial da União, 2024.

EMMERICH, Fabrício. Cibercrime: investigação criminal e provas digitais. 3. ed. Curitiba: Juruá, 2017.

FERNANDES, Ricardo Vieira de Carvalho. Direito e Tecnologia: desafios da rede e soberania digital. Belo Horizonte: Fórum, 2019.

GRECO, Rogério. Curso de Direito Penal: parte geral. 24. ed. Rio de Janeiro: Atlas, 2022.

GROSSI, Fernanda. Infância e Capitalismo de Vigilância: a subjetividade como mercadoria. Revista Brasileira de Direito Civil, v. 31, p. 112-135, 2024.

HABIGZANG, Luisa F.; CAMINHA, Renato M. Abuso sexual contra crianças e adolescentes: conceituação e intervenção clínica. Porto Alegre: Artmed, 2002.

HENRIQUES, I.; RIBEIRO, T. Safety by Design e a Autoridade Nacional de Proteção de Dados: novos paradigmas. Revista de Direito e Tecnologia, v. 5, n. 1, 2025.

JONAS, Hans. The imperative of responsibility: in search of an Ethics for the technological age. Chicago: University of Chicago Press, 1984.

KANT, Immanuel. Fundamentação da Metafísica dos Costumes. Tradução de Paulo Quintela. Lisboa: Edições 70, 2007.

LÉVY, Pierre. Cibercultura. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2009.

LUNA, Maria José de Matos; BRITO, Renato Victor Lira. Proteção de crianças e adolescentes na era digital: uma revisão sistemática. Estudos Universitários, Recife, v. 42, n. 1, 2025.

MLADENOVIĆ, Miljana; OŠMJANSKI, Vera; STANKOVIĆ, Staša Vujičić. Cyber-aggression, cyberbullying, and cyber-grooming: A survey and research challenges. ACM Computing Surveys (CSUR), v. 54, n. 1, p. 1-42, 2021.

NUCCI, Guilherme de Souza. Estatuto da Criança e do Adolescente Comentado: em busca da Constituição Federal das Crianças e dos Adolescentes. 3. ed. Rio de Janeiro: Forense, 2017.

PINHEIRO, Patrícia Peck. Direito Digital. 7. ed. São Paulo: Saraiva, 2021.

REVISTA Caderno Pedagógico. Proteção integral e o Art. 227 da CF/88 no meio digital. v. 22, n. 3, 2025.

SOCIEDADE BRASILEIRA DE PEDIATRIA. Manual de Orientação: #MENOSTELAS #MAISSAÚDE. Grupo de Trabalho Saúde na Era Digital. Rio de Janeiro: SBP, 2019.

TROIANO, Anderson. Infiltração Policial Virtual e o combate ao Grooming: limites e eficácia. Revista de Ciências Policiais, v. 14, n. 2, 2025.

WENDT, Emerson. A validade jurídica das evidências digitais colhidas nos delitos informáticos praticados pela web. In: WENDT, Emerson; LOPES, Fábio Motta (org.). Investigação Criminal: Provas. Porto Alegre: Livraria do Advogado, 2015.

NOTAS BIOGRÁFICAS DOS AUTORES

Elimei Paleari do Amaral CAMARGO[1]

Professora adjunta B 4 da Universidade Federal de Rondônia - UNIR, com trajetória acadêmica interdisciplinar entre o Direito e a Educação. Doutora em Educação pela UNIMEP/Piracicaba (2016), mestre em Direito pela Universidade de Ribeirão Preto - UNAERP- (2003) e graduada em Direito pela Instituição Toledo de Ensino de Bauru- ITE- (1996). Exerceu a função de chefe de departamento de direito de março de 2023 a março de 2024. Atualmente realiza estágio pós-doutoral em Ciência Jurídica na UNEP, onde integra o grupo de pesquisa "Direito, Democracia e Novas Tecnologias".

Emanuele Giachini BOTELHO[2]

Doutoranda em Direito na FUNIBER - Fundación Universitaria Iberoamericana) desde Janeiro/2026. Mestra em Ciência Jurídica pela Universidade Estadual Norte do Paraná - UENP. Professora de Direito em Regime Especial (CRES) na UENP - Universidade Estadual Norte do Paraná, desde 07/2024. Professora de Ensino Superior no Centro Estadual de Educação Tecnológica Paula Souza/ Faculdade de Tecnologia de Jahu desde 05/02/2026. Pesquisadora integrante do Igualdade, Reconhecimento e Inclusão Social: Minorias e Grupos Vulneráveis - IRIS (endereço de acesso: dgp.cnpq.br/dgp/espelhogrupo/4411113930848069). Pesquisadora Integrante do Grupo de Pesquisa Direito, Democracia e Novas Tecnologias da UENP (endereço de acesso: http://dgp.cnpq.br/dgp/espelhogrupo/825800).

Professora Coordenadora do Projeto de Extensão "CARTILHAS DE INFORMAÇÃO DO PROGRAMA "EU ME PROTEJO": CAPACITAÇÃO DE PROFESSORES DA EDUCAÇÃO INFANTIL E DOS PRIMEIROS ANOS DO ENSINO FUNDAMENTAL PARA ABORDAGEM DE TEMAS RELACIONADOS À PREVENÇÃO E COMBATE À VIOLÊNCIA INFANTIL" na UENP. Professora colaboradora do Projeto de Extensão "CARTILHAS DE INFORMAÇÕES SOBRE JULGAMENTO COM PERSPECTIVA DE GÊNERO: ESCLARECIMENTO AOS SERVIDORES DOS TRIBUNAIS DE JUSTIÇA E DO MINISTÉRIO PÚBLICO DO PARANÁ". Professora integrante da Comissão de Eventos da Uenp. Professora Coordenadora da comissão da IV Feira de Profissões 2025 da UENP no Campus de Jacarezinho/PR. Professora de Pós-graduação em Direito Previdenciário da UNOESTE - Campus de Jaú/SP. Advogada. Atuante desde 2004, avaliadora da Revista Direito e Cidadania da UEMG Passos (ISSN: 2526-4753).

Maurício Rogério BOTELHO[3]

Mestrando em direito pela Fundação Iberoamericana - Funiber (2026). Especialista em Direito Penal e Direito Processual Penal pela FAMART (2024). Especialista em gestão ambiental pelo Centro Universitário Claretiano (2009). Bacharel em Direito pelas Faculdades Integradas de Jahu (2018). Técnologo em logística pela Fatec/Jaú (2006). Escrivão de polícia do estado de São Paulo.