

**A PROTEÇÃO AOS MENORES CONTRA CRIMES CIBERNÉTICOS:
RESPONSABILIDADE PENAL E O PAPEL DAS PLATAFORMAS DIGITAIS**

***PROTECTING MINORS AGAINST CYBERCRIMES: CRIMINAL LIABILITY AND
THE ROLE OF DIGITAL PLATFORMS***

***PROTECCIÓN DE LOS MENORES CONTRA LOS DELITOS CIBERNÉTICOS:
RESPONSABILIDAD PENAL Y EL PAPEL DE LAS PLATAFORMAS DIGITALES***

Lucas Gabriel Rocha Mamede Reis

Graduando em Direito, Faculdade de Ensino Superior de Linhares, Brasil

E-mail: lucasgabrielrochareis@gmail.com

Alexandre Jacob

Mestre, Faculdade de Ensino Municipal de Linhares, Brasil

E-mail: alexandre.jacob10@gmail.com

Resumo:

O presente artigo analisa a proteção de menores frente aos crimes cibernéticos no Brasil, enfocando a eficácia da legislação penal vigente e a responsabilidade das plataformas digitais. A pesquisa é de caráter qualitativo, baseada em revisão bibliográfica, análise legislativa e estudo de casos. Verificou-se que, apesar de instrumentos normativos relevantes, subsistem lacunas na prevenção, na investigação e na responsabilização de agentes que atuam no ambiente digital, impondo a necessidade de aprimoramentos legislativos e de investimento em capacitação técnica e cooperação internacional.

Palavras-chave: Direito penal; Crimes cibernéticos; Crianças e adolescentes; Plataformas digitais; Proteção de dados.

Abstract:

This article examines the protection of minors against cybercrimes in Brazil, focusing on the effectiveness of current criminal legislation and the liability of digital platforms. The qualitative research relies on bibliographic review, legislative analysis and case studies. Despite relevant legal

instruments, gaps persist in prevention, investigation and accountability, requiring legislative updates and investments in technical capacity and international cooperation.

Keywords: Criminal law; Cybercrimes; Children and adolescents; Digital platforms; Data protection.

Resumen:

Este artículo analiza la protección de los menores contra los delitos informáticos en Brasil, centrándose en la eficacia de la legislación penal vigente y la responsabilidad de las plataformas digitales. Esta investigación cualitativa se basa en una revisión bibliográfica, un análisis legislativo y estudios de caso. Se constató que, a pesar de la existencia de instrumentos regulatorios relevantes, persisten lagunas en la prevención, la investigación y la rendición de cuentas de los actores que operan en el entorno digital, lo que requiere mejoras legislativas e inversión en capacitación técnica y cooperación internacional.

Palabras clave: Derecho penal; Delitos informáticos; Niños, niñas y adolescentes; Plataformas digitales; Protección de datos.

1. Introdução

O fenômeno da digitalização e a intensificação do uso de plataformas on-line por crianças e adolescentes introduziram novas modalidades de risco que exigem resposta articulada do Direito Penal, do Direito da Criança e do Adolescente e do Direito Digital. A presença crescente de menores em redes sociais, aplicativos de mensagens e ambientes de jogos criou oportunidades para a prática de delitos como *grooming* (aliciamento), assédio sexual, divulgação de material de natureza sexual e *cyberbullying*, cujos impactos ultrapassam a esfera individual e atingem a ordem pública e a dignidade da pessoa humana.

O conceito de modernidade líquida, de Zygmunt Bauman (2001), já explorado em estudos recentes, contribui para a compreensão da vulnerabilidade infantojuvenil em ambientes digitais. A fluidez e instabilidade das relações virtuais tornam crianças e adolescentes mais suscetíveis a práticas como cyberbullying, grooming e sextorsão. Essa abordagem sociológica complementa a visão normativa identificada no presente estudo, permitindo uma análise interdisciplinar que associa Direito, tecnologia e sociologia.

O Estatuto da Criança e do Adolescente consagra a proteção integral como princípio basilar (Brasil, 1990); contudo, a aplicação prática dessa proteção no espaço virtual revela desafios investigativos, probatórios e normativos. Rogério Greco (2020) aponta que a natureza descentralizada da internet e a possibilidade de ocultação da identidade dificultam a identificação e responsabilização dos autores.

Ademais, a tipificação de condutas digitais sofreu avanços com as alterações no Código Penal (1940), o Marco Civil da Internet (2014) e a Lei Geral de Proteção de Dados Pessoais (2018). Entretanto, há crítica doutrinária quanto à fragmentação normativa e à insuficiência de mecanismos de responsabilização penal das plataformas, conforme argumenta Aury Lopes Jr. (2022).

A gravidade do problema também fica evidenciada em operações policiais de grande envergadura, como as fases da Operação Luz na Infância e as denominações correlatas (Operação Anjos da Guarda/Anjo Guardião), que mostram a dimensão e a recorrência dos crimes envolvendo material de abuso sexual infantil e aliciamento por meios digitais. Esses eventos demonstram que a resposta estatal possui capacidade operacional, mas carece de medidas legislativas e procedimentais complementares.

O problema de pesquisa que orienta este estudo pode ser formulado da seguinte maneira: de que forma a legislação penal brasileira e as plataformas digitais têm contribuído para a proteção de crianças e adolescentes contra crimes cibernéticos, e quais são as principais lacunas regulatórias e institucionais existentes?

A hipótese central formulada é a de que a legislação brasileira, embora contenha instrumentos importantes, apresenta lacunas e desafios que impedem proteção efetiva, sendo necessário o fortalecimento da responsabilização das plataformas digitais, a especialização dos órgãos de investigação e a atualização normativa para abarcar condutas emergentes.

O objetivo geral deste trabalho é avaliar a eficácia da legislação penal brasileira na proteção de menores contra crimes cibernéticos e examinar a responsabilização das plataformas digitais. Os objetivos específicos incluem:

mapear a legislação e a doutrina pertinente; analisar casos e operações policiais representativas; e identificar lacunas e propor medidas legislativas e administrativas.

2. Os Crimes Cibernéticos e a Proteção aos Menores

Os crimes cibernéticos, no sentido lato, compreendem condutas delituosas em que o meio eletrônico é utilizado como instrumento, meio ou fim da prática criminosa. Greco (2020) ressalta que a delimitação conceitual deve considerar tanto os delitos que têm natureza informacional (invasão de dispositivos, adulteração de dados) quanto aqueles que, embora clássicos, ganharam nova expressão no ambiente digital (extorsão, difamação, corrupção de menores).

A Lei nº. 12.737/2012 introduziu no ordenamento brasileiro tipos penais específicos voltados à proteção do patrimônio informático, tipificando, por exemplo, a invasão de dispositivo eletrônico para obtenção de dados (art. 154-A do Código Penal, inserido pela referida lei). Porém, a tipificação legal não abrange de forma exaustiva condutas como grooming e formas complexas de exploração sexual que utilizam redes sociais como meio de aproximação, restando espaço para a construção jurisprudencial e para a adequação legislativa.

Guilherme de Souza Nucci (2015) observa que o reconhecimento de condutas velhas em novas esferas exige interpretação teleológica dos tipos penais, a fim de que o Direito Penal não se torne ineficaz diante da reconfiguração tecnológica das condutas criminosas.

O Estatuto da Criança e do Adolescente (Lei nº. 8.069/1990) dedica diversos dispositivos para a repressão de atos de exploração e violência sexual contra menores. Em particular, os arts. 240 a 241-E tipificam condutas relativas à produção, oferta, divulgação e armazenamento de material pornográfico envolvendo crianças e adolescentes. A doutrina, representada por Nucci (2015), enfatiza a amplitude protetiva do ECA, que transcende a mera sanção penal, abrangendo medidas socioassistenciais e protetivas.

Por outro lado, a aplicabilidade eficaz do ECA nos crimes digitais encontra dificuldade prática, especialmente quanto ao acesso e à preservação de provas digitais, à identificação de autores que ocultam sua identidade e à atuação de provedores sediados no exterior. Aury Lopes Jr. (2022) destaca a necessidade de mecanismos processuais céleres para preservar o conteúdo e viabilizar a persecução penal.

Cabe ressaltar que a definição de pornografia infantil no ECA tem sido interpretada de forma extensiva pelo STJ, que admite a caracterização mesmo na ausência de completa nudez, quando há finalidade sexual evidente nas imagens, o que amplia o alcance protetivo do estatuto em face de condutas modernas de exploração (STJ, jurisprudência).

3. Responsabilidade Penal das Plataformas Digitais

O Marco Civil da Internet (Lei nº 12.965/2014) consagrou princípios basilares como a neutralidade de rede, a proteção da privacidade e a responsabilidade civil dos provedores de aplicações, condicionada à ordem judicial para a remoção de conteúdo ilícito. A doutrina de Danilo Doneda (2019) e Lopes Jr. (2022) debate a extensão dessa responsabilização quando se trata de omissões que facilitam a prática de crimes contra menores.

Doneda (2019) aponta que a proteção de dados, prevista na LGPD, impõe às plataformas obrigações de tratamento responsável dos dados pessoais, o que pode ser coadunado com a adoção de medidas proativas para prevenir abusos, sem, entretanto, transformar a obrigação em um dever penal automático. A discussão gira em torno do equilíbrio entre proteção de direitos fundamentais (privacidade e liberdade de expressão) e a necessidade de tutela eficaz de menores.

O Habeas Corpus nº. 598.051-SP reforça a posição do STJ de que a posse de material pornográfico infantil é crime formal, ainda que não haja compartilhamento (STJ, 2021). Esse precedente fortalece a interpretação extensiva do ECA em ambientes digitais. Além disso, projetos legislativos recentes, como o

PL nº. 5.016/2019 (aumento de penas para crimes sexuais virtuais), PL nº. 4.806/2020 (tipificação do *cyberbullying*) e PL nº. 1.338/2022 (medidas protetivas específicas), revelam esforço contínuo de atualização normativa, ainda que enfrentem desafios de efetividade frente ao dinamismo tecnológico (Carbonieri *et al.*, 2025).

A bibliografia consultada sugere que a responsabilização penal das plataformas exigiria previsão legal clara e critérios objetivos que delimitem situações de culpa por omissão ou de autoria mediata, sem ferir princípios constitucionais e garantias processuais (Greco, 2020; Lopes Jr., 2022).

A análise normativa parte da identificação dos diplomas centrais. Cada norma desempenha papel específico: o ECA protege a pessoa e a integridade sexual de menores; a Lei 12.737/2012 tipifica delitos informáticos; o Marco Civil disciplina responsabilidades dos provedores; e a LGPD regula o tratamento de dados pessoais, incluindo os de crianças e adolescentes.

Artigo por artigo, verifica-se que o art. 240 do ECA tipifica a produção, reprodução e divulgação de material pornográfico envolvendo criança ou adolescente, com penas que variam conforme a conduta. A interpretação contemporânea admite aplicação extensiva diante de novas formas de ilicitude, como disseminação em redes sociais e aplicações de mensageria.

Quanto à Lei nº. 12.737/2012, o art. 154-A do Código Penal, introduzido pela norma, tipifica a invasão de dispositivo informático com o fim de obtenção, adulteração ou destruição de dados. Embora seja relevante, não resolve situações em que o crime é praticado sem invasão (por exemplo, quando o autor convence a vítima a enviar imagens). Isso evidencia a necessidade de tipificação específica do aliciamento (*grooming*) e de mecanismos que alcancem a conduta mediada por plataformas.

O Marco Civil estabelece que provedores de aplicações somente serão responsabilizados civilmente quando, após ordem judicial, não removerem conteúdo ilícito (art. 19). No entanto, em situações de menor em risco iminente, a tramitação judicial pode ser demasiado lenta, revelando a necessidade de

instrumentos que permitam atuação preventiva e cooperação eficaz entre provedores e autoridades.

A LGPD, por sua vez, trata do consentimento e do tratamento de dados de crianças e adolescentes (art. 14), exigindo maior proteção. Essa proteção de dados cria fundamento normativo para exigir que plataformas adotem medidas técnicas e administrativas de segurança que reduzam riscos de exposição e violação da privacidade dos menores.

O conceito de modernidade líquida, desenvolvido por Zygmunt Bauman (2001), explica a fragilidade das relações sociais e a fluidez dos vínculos institucionais na contemporaneidade. Essa visão contribui para a análise do ambiente digital, marcado pela instabilidade das interações e pela maior vulnerabilidade de crianças e adolescentes diante de crimes como *cyberbullying*, sextorsão e *grooming*. Tal abordagem complementa a dimensão normativa já discutida neste artigo, revelando a necessidade de respostas interdisciplinares que unam Direito, sociologia e tecnologia.

4. Estudo de Casos e Propostas de Alteração Legislativa

Caso Operação Luz na Infância: A Operação Luz na Infância, coordenada por forças policiais e órgãos de investigação em cooperação internacional, resultou em cumprimento massivo de mandados e na apreensão de grande volume de material ilícito. Esses números demonstram a dimensão do fenômeno e a necessidade de medidas estruturadas para investigação e prevenção.

Caso 2 Operação Anjos da Guarda/Anjo Guardião: operações deflagradas pela Polícia Federal para identificar agentes que armazenam, compartilham ou produzem material de abuso sexual infantojuvenil. Exemplo recente inclui prisões em 2024/2025 durante fases da operação, indicando a continuidade e recorrência desses crimes.

Caso Operação Caminhos Seguros: ação coordenada pelo Ministério da Justiça que alcançou resgates e prisões em larga escala, demonstrando que a violência contra menores no Brasil envolve múltiplas formas (abuso, abandono,

exploração) e exige resposta integrada entre segurança pública, assistência social e plataformas digitais.

Caso Plataformas de jogos e redes sociais: riscos e respostas

Jogos on-line vêm sendo explorados por criminosos para o aliciamento de menores. A Polícia Federal e polícias civis relataram em 2025 que suspeitos atraíam crianças por meio de partidas e recompensas virtuais, em casos que incluíram plataformas populares como Free Fire. A Garena, desenvolvedora do jogo, declara em sua política de privacidade que seus serviços não se destinam a menores de 13 anos, prevendo o encerramento de contas quando dados de crianças forem utilizados sem consentimento parental, um ponto central para o *age gating*. Nas redes sociais e aplicativos de mensagens, o Discord lançou em 2023 a Central da Família, permitindo maior supervisão de responsáveis sobre atividades de adolescentes.

Caso Felca: no panorama empírico recente no Brasil, após a denúncia pública do influenciador Felca, parlamentares passaram a defender a criação de uma CPI para investigar a adultização e a exploração de menores nas redes, sinalizando prioridade política para o tema no Senado (Barra; Leão, 2025). Entre 15 e 19 de agosto de 2025, as denúncias recebidas pela SaferNet Brasil cresceram 114% em relação à semana anterior, com predominância de casos ligados a abuso/exploração sexual infantil (SaferNet, 2025). O Ministério da Justiça e Segurança Pública (MJSP) deflagrou novas fases da Operação Luz na Infância em 2025, com prisões e apreensões no Brasil e no exterior para combater crimes de abuso sexual infantil on-line (Martins, 2025).

A jurisprudência recente reforça o caráter protetivo do ECA. O Habeas Corpus nº 598.051-SP consolidou o entendimento de que a posse de material pornográfico infantil constitui crime formal, ainda que não haja circulação das imagens. Paralelamente, tramitam projetos de lei sobre o tema. Além disso, após a denúncia do influenciador Felca em 2025, novas propostas legislativas foram apresentadas, refletindo a pressão social e midiática para reforço da proteção penal e regulatória (Martins, 2025; Nascimento, 2025).

Esses casos evidenciam que as investigações dependem fortemente da cooperação entre provedores, capacidade técnica dos órgãos e marcos legais que permitam acesso a dados preservados. A doutrina (Lopes Jr., 2022; Greco, 2020) enfatiza a importância da tipificação adequada e da produção de provas digitais confiáveis para a persecução penal.

Com base nas lacunas identificadas, considera-se adequado a tipificação autônoma e qualificada do aliciamento (*grooming*) digital, com agravantes quando houver emprego de artifícios para manter contato continuado; a previsão legal de deveres mínimos de diligência para plataformas digitais relativas à detecção e comunicação de conteúdo envolvendo menores, respeitados os direitos fundamentais; mecanismo de cooperação célere entre provedores e autoridades, com normas para preservação e transferência segura de dados; incentivos à capacitação e à criação de unidades especializadas em pericial e investigação de crimes cibernéticos envolvendo menores.

A discussão doutrinária sugere cautela para não converter obrigações administrativas em responsabilidade penal automática, sendo essencial fixar critérios objetivos para a responsabilização por omissão, com observância do princípio da legalidade e do devido processo (Greco, 2020; Lopes Jr., 2022; Doneda, 2019).

No entanto, são medidas urgentes a obrigação de diligência técnica para plataformas com alto risco infantojuvenil, exigindo *hash matching*, detectores de grooming e controles parentais auditáveis, o estabelecimento de KPIs regulatórios como tempo de remoção e prevalência por milhão de conteúdos, auditorias externas periódicas para avaliar eficácia dos sistemas de moderação, exigência de *age assurance* e moderação de voz em tempo real em jogos com grande participação de crianças e adolescentes.

Os casos concretos analisados evidenciam que a resposta isolada do Estado não é suficiente. O aumento expressivo das denúncias na SaferNet após o caso Felca (2025) comprova a importância da sociedade civil na conscientização e no monitoramento. Do lado das plataformas, exemplos como a criação da Central da Família pelo Discord (2024) demonstram que o setor privado também pode

implementar soluções de design seguro e controles parentais. Assim, a proteção efetiva exige cooperação tripartite entre Estado, sociedade civil e empresas de tecnologia.

Além disso, recomenda-se regulamentação complementar ao Marco Civil que permita instrumentos emergenciais para remoção imediata de conteúdo de risco, em hipóteses de prova robusta de perigo iminente, com supervisão judicial posterior, para conciliar celeridade e garantia de direitos.

5. Conclusão

A proteção de menores contra crimes cibernéticos no Brasil apresenta avanços significativos, mas ainda carece de efetividade prática diante das rápidas transformações tecnológicas. A análise legislativa, jurisprudencial e dos casos concretos confirma a necessidade de atualização normativa, responsabilização mais eficaz das plataformas digitais e fortalecimento da investigação criminal.

Ao mesmo tempo, o emprego de soluções técnico-tecnológicas, tais como:

A adoção de algoritmos de *hash matching* (PhotoDNA, PDQ, CSAI Match) e inteligência artificial para identificar conteúdos de abuso sexual infantil, a implementação de sistemas de detecção de grooming em chats e jogos, incluindo moderação de voz em tempo real, a verificação de idade (*age assurance*) baseada em inteligência artificial, documentos e consentimento parental verificável, a expansão de controles parentais como Family Center e Family Pairing, com maior transparência sobre contatos e atividades, elaboração de relatórios de segurança auditáveis, com métricas como prevalência de conteúdos nocivos e tempo médio de remoção, o fortalecimento da cooperação internacional e da preservação de provas digitais, por meio de redes como INHOPE, NCMEC e SaferNet.

No campo educacional e psicossocial, destaca-se a importância de programas escolares de conscientização sobre riscos digitais, capacitação de professores e apoio psicológico às vítimas, em consonância com o princípio da proteção integral do ECA. Aliada a políticas educativas e de apoio psicossocial, revela-se indispensável para reduzir a vulnerabilidade infantojuvenil no espaço

virtual, a integração entre Estado, sociedade civil, setor privado e órgãos de investigação deve ser vista como um eixo estruturante: somente por meio dessa cooperação será possível assegurar a proteção integral de crianças e adolescentes, garantindo seus direitos fundamentais na era digital.

6. Referências

BARRA, Helena; LEÃO, Luan. Denúncia Felca: adultização afeta desenvolvimento, explica especialista. **CNN Brasil**, 16 ago. 2025. Disponível em: <https://tinyurl.com/3xe3suja>. Acesso em: 15 set. 2025.

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília-DF: Senado, 1988. Disponível em: <https://tinyurl.com/29ucwd3a>. Acesso em: 06 set. 2025

BRASIL. **Decreto-lei nº. 2.848 de 07 de dezembro de 1940**. Código penal. Rio de Janeiro: Catete, 1940. Disponível em: <https://tinyurl.com/3795f56t>. Acesso em: 06 set. 2025.

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: Senado, 1990. Disponível em: <https://tinyurl.com/2stc7ynw>. Acesso em: 06 set. 2025.

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: Senado, 2014. Disponível em: <https://tinyurl.com/2b9yz9wj>. Acesso em: 06 set. 2025.

BRASIL. **Lei nº. 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília-DF: Senado, 2018. Disponível em: <https://tinyurl.com/34u5u8ce>. Acesso em: 06 set. 2025.

CARBONIERI, Ana Luiza Bornia; SILVA, Maria Eloísa Benevides; PRADO, Thiago Silva. Adultização infantil no Brasil e o trabalho de menores nas redes sociais digitais. **Aurum Estudos em Ciências Humanas e Sociais**, 14 out. 2025. Disponível em: <https://tinyurl.com/e7z5z6he>. Acesso em: 20 out. 2025.

DISCORD. **Central familiar para pais e guardiões**, 09 jan. 2024. Disponível em: <https://tinyurl.com/bdfd7zd7>. Acesso em: 25 set. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

GRECO, Rogério. **Direito penal**: parte geral. 23. ed. Rio de Janeiro: Impetus, 2020.

LOPES JÚNIOR, Aury. **Direito processual penal**. 19. ed. São Paulo: Saraiva, 2022.

MARTINS, Jônatas. Em um dia, deputados apresentam mais de 20 projetos contra adultização. **CNN Brasil**, 12 ago. 2025. Disponível em: <https://tinyurl.com/4uf4kdew>. Acesso em: 25 set. 2025.

NASCIMENTO, Henrique. Após vídeo de Felca, senadores formalizam CPI contra exploração infantil nas redes. **Rádio Senado**, 12 ago. 2025. Disponível em: <https://tinyurl.com/y89pu9b2>. Acesso em: 25 set. 2025.

NUCCI, Guilherme de Souza. **Provas no processo penal**. Rio de Janeiro: Forense, 2015.

SAFERNET BRASIL. **Indicadores da central nacional de denúncias de crimes cibernéticos** [banco de dados], 2025. Disponível em: <https://tinyurl.com/868bw9ku>. Acesso em: 25 set. 2025.

STJ. Superior Tribunal de Justiça. **Habeas Corpus nº. 598.051-SP**. Quinta Turma. Relator: Ministro Rogério Schietti Cruz. Brasília-DF: DJe, 15 mar. 2021.