OS CRIMES DIGITAIS CONTRA MENORES E AS POSSIBILIDADES LEGAIS DE REPRESSÃO

Ana Luiza de Souza Mesquita[1]
Rafaela Stefany Carvalho Silva[2]
Leonardo Elias de Paiva[3]

RESUMO
O presente trabalho analisa os crimes digitais praticados contra menores e as possibilidades legais de repressão no ordenamento jurídico brasileiro, diante do avanço tecnológico e da crescente inserção de crianças e adolescentes no ambiente virtual. Embora a internet proporcione facilidades de comunicação, entretenimento e acesso à informação, também amplia significativamente a exposição desse público a riscos como aliciamento online, vazamento de dados pessoais, cyberbullying, fraudes virtuais e divulgação de conteúdos ilícitos. Nesse cenário, questiona-se em que medida o ordenamento jurídico brasileiro é eficaz na repressão dessas condutas, considerando as particularidades do ambiente virtual, a rapidez das interações digitais e a vulnerabilidade das vítimas. O estudo fundamenta-se na Constituição Federal de 1988, no Estatuto da Criança e do Adolescente e em normas voltadas à proteção digital e à responsabilização criminal. Objetiva-se compreender os crimes digitais contra menores, suas principais formas de ocorrência e a atuação do ordenamento jurídico na repressão dessas práticas. A metodologia adotada é qualitativa, com base em pesquisa bibliográfica, legislativa e jurisprudencial. Conclui-se que, apesar dos avanços normativos, ainda persistem dificuldades na efetividade da repressão, especialmente em razão da complexidade das investigações, do anonimato dos agentes, da transnacionalidade dos delitos e da insuficiência de mecanismos preventivos, o que evidencia a necessidade de maior atuação estatal preventiva, educativa e fiscalizatória.

PALAVRAS-CHAVE: Crimes digitais. Crianças e adolescentes. Vulnerabilidade. Repressão penal. Segurança digital.

ABSTRACT
This paper analyzes digital crimes committed against minors and the legal possibilities for repression within the Brazilian legal system, considering technological advances and the increasing presence of children and adolescents in the virtual environment. Although the internet provides facilities for communication, entertainment, and access to information, it also significantly increases the exposure of this group to risks such as online grooming, personal data leaks, cyberbullying, virtual fraud, and the dissemination of illegal content. In this context, the study questions the extent to which the Brazilian legal system is effective in repressing such conduct, considering the particularities of the virtual environment, the speed of digital interactions, and the vulnerability of victims. The study is based on the Federal Constitution of 1988, the Child and Adolescent Statute, and regulations aimed at digital protection and criminal accountability. Its objective is to understand digital crimes against minors, their main forms of occurrence, and the role of the legal system in repressing these practices. The methodology adopted is qualitative, based on bibliographic, legislative, and jurisprudential research. It is concluded that, despite legal advances, difficulties still persist regarding the effectiveness of repression, especially due to the complexity of investigations, the anonymity of offenders, the transnational nature of crimes, and the insufficiency of preventive mechanisms, highlighting the need for greater preventive, educational, and supervisory action by the State.

KEYWORDS: Digital crimes. Children and adolescents. Vulnerability. Criminal repression. Digital security.

INTRODUÇÃO

A expansão das tecnologias digitais e o acesso cada vez mais precoce à internet transformaram profundamente as formas de interação social, comunicação e construção de identidade, especialmente entre crianças e adolescentes. Nesse cenário, o ambiente

[1]Graduanda em Direito pela Faculdade Evangélica Raízes, Anápolis, Goiás, e-mail: naluh.09@gmail.com
[2]Graduanda em Direito pela Faculdade Evangélica Raízes, Anápolis, Goiás, e-mail: rafaela.carvalho333@outlook.com
[3] Especialista em Direito Penal, Processo Penal, Direito do Trabalho e Processo do Trabalho pelo Complexo Jurídico Damásio de Jesus. Mestrado (Universidade Evangélica de Goiás - UniEVANGÉLICA), professor, Faculdade Evangélica Raízes, Anápolis, Goiás, leonardo.paiva@docente.faculdaderaizes.edu.br

virtual, ao mesmo tempo em que amplia oportunidades de aprendizado e socialização, também se apresenta como espaço propício para a prática de condutas ilícitas, muitas vezes direcionadas a indivíduos em condição de vulnerabilidade. Dentre essas condutas, destacam-se os crimes digitais contra menores, que vêm crescendo em complexidade, alcance e impacto, exigindo respostas jurídicas cada vez mais eficazes.

A internet, por sua natureza descentralizada e transnacional, desafia os modelos tradicionais de repressão penal. Outro aspecto da realidade virtual também enfrenta problemas com a falta de normatização ou com a normatização falha já existente (Mitani, 2012). A facilidade de anonimato, a rapidez na disseminação de conteúdos e a dificuldade de rastreamento dos agentes tornam a persecução penal mais complexa, sobretudo quando as vítimas são menores de idade.

Nesse sentido, observa-se que os crimes digitais não apenas reproduzem práticas já conhecidas no mundo físico, mas também criam novas formas de violência, novos caminhos, bastante protegidos, para os Aliciamentos, Assédios Sexuais, Sedução, Grooming, Sexting, Sextortion, Pornografia e Estupro virtual, sem que a inteligência virtual seja acionada na forma e número suficiente a conter essas violências, com isso a integridade psicológica e o desenvolvimento saudável de crianças e adolescentes se encontra em um estado de vulnerabilidade (Pfeiffer, 2022).

Para o Estudo da Criança e Adolescente lei 8.069, de 13 de julho de 1990, em seu artigo 2º traz que é considerado criança, pessoas de 0 a 12 anos de idade incompletos e os adolescentes são aqueles entre doze e dezoito anos de idade. A referida lei também deixa claro que o ordenamento, a família e a sociedade têm o dever de assegurar os direitos fundamentais inerentes a pessoas humanas, mesmo com todo esse aparato legislativo ainda se encontra lacunas para o acontecimento desses crimes.

Conforme destaca Capez (2023), o Direito Penal (1940) deve acompanhar as transformações sociais, adaptando-se às novas formas de criminalidade sem perder de vista seus princípios fundamentais. Nessa linha, a evolução tecnológica impõe ao ordenamento jurídico o desafio de equilibrar a proteção dos direitos fundamentais com a necessidade de responsabilização dos agentes que utilizam o meio digital para práticas ilícitas. Ainda, segundo Greco (2022), a tutela penal deve ser orientada pela proteção dos bens jurídicos mais relevantes, entre os quais se insere, de forma prioritária, a dignidade da pessoa humana, especialmente quando se trata de menores.

No ordenamento jurídico brasileiro, diversas normas buscam enfrentar essa problemática, como o Estatuto da Criança e do Adolescente (1990), o Marco Civil da Internet (2014) e a Lei nº 12.737/2012 (Lei Carolina Dieckmann). Tais diplomas normativos representam avanços relevantes na tutela jurídica do ambiente digital; contudo, ainda enfrentam limitações práticas diante da rapidez das transformações

tecnológicas e da crescente sofisticação dos meios utilizados para a prática de crimes virtuais. Nesse sentido, Postai (2023) destaca que o enfrentamento eficaz da criminalidade cibernética depende não apenas do aprimoramento legislativo interno, mas também do fortalecimento dos mecanismos de cooperação internacional.

Diante desse contexto, surge o seguinte problema de pesquisa: em que medida o ordenamento jurídico brasileiro é eficaz na repressão dos crimes digitais praticados contra menores, considerando as particularidades do ambiente virtual e a condição de vulnerabilidade das vítimas?

A relevância do tema justifica-se tanto do ponto de vista jurídico quanto social. Do ponto de vista jurídico, há a necessidade de aprofundar a compreensão sobre a adequação das normas existentes frente às novas modalidades de crime digital. Sob a perspectiva social, a proteção de crianças e adolescentes constitui prioridade absoluta, conforme estabelece o artigo 227 da Constituição Federal de 1988, o que reforça a urgência de mecanismos eficazes de prevenção e repressão dessas condutas. Além disso, o aumento significativo de casos envolvendo violência digital contra menores evidencia a necessidade de reflexão crítica sobre a atuação estatal e os instrumentos legais disponíveis.

O objetivo geral deste trabalho é analisar os crimes digitais praticados contra menores e as possibilidades legais de sua repressão no ordenamento jurídico brasileiro. Como objetivos específicos, pretende-se: (i) compreender o conceito e a evolução dos crimes digitais; (ii) identificar as principais tipologias de crimes digitais que atingem menores, bem como suas características; e (iii) examinar os mecanismos legais de repressão existentes no Brasil, avaliando sua eficácia e eventuais lacunas.

Para a consecução desses objetivos, será adotada uma metodologia de natureza qualitativa, baseada em pesquisa bibliográfica e documental. Serão analisadas obras doutrinárias relevantes no campo do Direito Penal (1940) e do Direito Digital, bem como a legislação vigente e decisões jurisprudenciais pertinentes ao tema. A abordagem será dedutiva, partindo da análise geral dos crimes digitais para, posteriormente, focar nas especificidades relacionadas à proteção de menores.

Por fim, destaca-se que o presente trabalho será estruturado em três tópicos principais, além desta introdução e das considerações finais. O primeiro tópico abordará o conceito e a evolução dos crimes digitais; o segundo tratará especificamente dos crimes digitais contra menores, suas tipologias e características; e o terceiro analisará os mecanismos legais de repressão no Brasil, incluindo legislação, jurisprudência e atuação estatal.

1. CONCEITO E EVOLUÇÃO DOS CRIMES DIGITAIS

A consolidação da sociedade da informação trouxe consigo novas dinâmicas sociais, econômicas e comunicacionais, impactando diretamente a forma como o Direito compreende e enfrenta a criminalidade. Nesse contexto, surgem os chamados crimes digitais, também denominados crimes cibernéticos ou informáticos, cuja definição não é unívoca na doutrina, mas que, em linhas gerais, referem-se às condutas ilícitas praticadas por meio de sistemas informáticos ou contra eles.

De acordo com Pinheiro (2021, p.45), os crimes digitais podem ser compreendidos como "todas as condutas típicas, ilícitas e culpáveis que envolvem, direta ou indiretamente, o uso de tecnologia da informação, seja como meio ou como fim da prática criminosa". Essa conceituação amplia o espectro de análise ao considerar tanto os delitos que têm como alvo os sistemas informáticos quanto aqueles em que tais sistemas são utilizados como instrumento para a prática de crimes tradicionais.

Nessa mesma linha, Capez (2023) ressalta que o Direito Penal (1940) contemporâneo não pode se limitar a categorias clássicas de criminalidade, devendo adaptar-se às novas formas de lesão a bens jurídicos. Segundo o autor, os crimes digitais representam uma evolução das práticas delitivas, exigindo releitura dos tipos penais existentes e, em alguns casos, a criação de novas figuras típicas. Tal compreensão reforça a ideia de que o fenômeno não se restringe a uma nova categoria isolada, mas integra uma transformação mais ampla da criminalidade.

A evolução dos crimes digitais está diretamente ligada ao desenvolvimento tecnológico e à popularização da internet. Em sua fase inicial, ainda nas décadas de 1970 e 1980, os delitos informáticos estavam restritos a ambientes corporativos e acadêmicos, sendo praticados, em sua maioria, por indivíduos com elevado conhecimento técnico. Nessa etapa, predominavam condutas como invasão de sistemas e manipulação de dados, muitas vezes sem finalidade econômica direta (Masini Neto, 2025).

Com a expansão da internet a partir da década de 1990, observa-se uma significativa mudança no perfil dos agentes e na natureza dos crimes. O acesso facilitado às tecnologias digitais ampliou o alcance das práticas ilícitas, permitindo que indivíduos sem conhecimento técnico aprofundado também passassem a praticar crimes no ambiente virtual. Conforme leciona Castells (2003), a sociedade em rede potencializa tanto as relações sociais quanto os riscos associados à circulação de informações, criando um ambiente propício à disseminação de condutas ilícitas.

Nesse período, surgem novas modalidades criminosas, como fraudes eletrônicas, estelionatos virtuais e a disseminação de conteúdos ilícitos. A partir dos anos 2000, com o advento das redes sociais e da chamada Web 2.0, há uma intensificação da interação

entre usuários, o que, por sua vez, amplia as possibilidades de ocorrência de crimes que atingem diretamente a honra, a imagem e a dignidade das pessoas, com o desenvolvimento desse espaço de múltiplas relações virtuais, surgiu o novo gênero de criminalidade que é impulsionada pelas sensações de anonimato e de liberdade que a internet proporciona (Masini Neto, 2025).

Mais recentemente, com o avanço da tecnologia móvel, da computação em nuvem e da inteligência artificial, os crimes digitais tornaram-se progressivamente mais sofisticados e difíceis de rastrear. A utilização de ferramentas de anonimização, como criptografia, redes privadas virtuais (VPNs) e ambientes ocultos da internet (dark web), eleva a complexidade investigativa e exige atuação técnica especializada por parte das autoridades públicas.

Nesse sentido, Pinheiro (2021) destaca que a evolução tecnológica, ao mesmo tempo em que amplia as possibilidades de comunicação e circulação de informações, também potencializa novas formas de prática criminosa, impondo obstáculos relevantes à identificação de autores e à persecução penal. Ademais, relatórios da Europol (2024) apontam que o uso crescente de mecanismos de anonimização e anti-forense representa um dos principais entraves à investigação de crimes cibernéticos contemporâneos

No que se refere à classificação dos crimes digitais, a doutrina apresenta diferentes critérios. Uma das classificações mais aceitas distingue os crimes próprios (ou puros) dos crimes impróprios ou mistos (Masini Neto, 2025). Os crimes digitais próprios são aqueles que têm como objeto direto os sistemas informáticos, como ocorre nas hipóteses de invasão de dispositivo informático, tipificada no artigo 154-A do Código Penal de 1940, incluído pela Lei nº 12.737/2012. Nesses casos, o bem jurídico protegido está diretamente relacionado à segurança da informação e à integridade dos sistemas.

Por outro lado, os crimes digitais impróprios são aqueles em que a tecnologia é utilizada como meio para a prática de crimes já previstos no ordenamento jurídico, como estelionato, ameaça, difamação e crimes contra a dignidade sexual. Nesse caso, o ambiente digital funciona como instrumento facilitador da conduta criminosa, sem alterar, em essência, o tipo penal já existente. Segundo Greco (2022), essa distinção é fundamental para compreender que nem toda inovação tecnológica exige, necessariamente, a criação de novos tipos penais, sendo possível, em muitos casos, a aplicação das normas já existentes.

Há, ainda, classificações que levam em conta o bem jurídico tutelado, abrangendo crimes contra a honra, o patrimônio, a dignidade sexual e a administração pública, todos passíveis de ocorrência no ambiente digital. Nessa perspectiva, os crimes digitais não configuram categoria homogênea, mas conjunto plural de condutas

ofensivas a distintos bens jurídicos penalmente protegidos, revelando a complexidade da tutela penal no ciberespaço, conforme lecionam Vladimir Aras (2001) e Amanda Silvestre Patrus *et al.* (2017).

Importante destacar que a transnacionalidade é uma das características mais marcantes dos crimes digitais. Diferentemente dos crimes tradicionais, que, em regra, possuem delimitação territorial mais clara, os delitos praticados na internet frequentemente ultrapassam fronteiras, envolvendo agentes, vítimas e servidores localizados em diferentes países. Tal característica impõe desafios adicionais à aplicação da lei penal no espaço, bem como à cooperação jurídica internacional (Pinheiro,2021).

Nesse sentido, a Convenção de Budapeste sobre o Crime Cibernético (2001), embora não tenha sido inicialmente ratificada pelo Brasil, influenciou significativamente a formulação de normas internas voltadas ao enfrentamento da criminalidade digital. Com a adesão formal do país e sua promulgação pelo Decreto nº 11.491, de 12 de abril de 2023, a convenção passou a integrar o ordenamento jurídico brasileiro, reforçando a necessidade de harmonização legislativa e de cooperação internacional no combate aos crimes cibernéticos.

Diante desse panorama, verifica-se que os crimes digitais representam uma realidade complexa e em constante transformação, exigindo do Direito Penal (1940) não apenas atualização normativa, mas também interpretação sistemática e integrada com outros ramos do Direito. A compreensão de seu conceito, evolução e classificação constitui etapa fundamental para a análise específica dos crimes praticados contra menores, tema que será aprofundado no tópico seguinte.

2. PROTEÇÃO JURÍDICA DA CRIANÇA E DO ADOLESCENTE NO BRASIL.

A lei da proteção à criança e do adolescente do Brasil está previsto no artigo 227 da Constituição Federal de 1988 que diz

> É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Brasil, *online*)

Ele estabelece o dever da família, da sociedade e do Estado a assegurar, com absoluta prioridade, a efetivação dos direitos fundamentais. No artigo citado, proporciona grande clareza de que, as crianças e os adolescentes são sujeitos também a direitos como o restante da sociedade. Eles têm direito à vida, saúde, educação, lar,

dignidade, respeito e convivência familiar. Além da proteção de toda forma de negligência, violência, discriminação e opressão.

Diante desse contexto de proteção integral prevista na Constituição Federal de 1988 e regulamentada pelo Estatuto da Criança e do Adolescente Lei nº 8.069 do ano de 1990, verifica-se a necessidade de sua aplicação também no ambiente digital. A promulgação da Constituição Federal de 1988 representou uma verdadeira mudança de paradigmas no ordenamento jurídico brasileiro, ao substituir o modelo de menoridade pela doutrina da proteção integral. Anteriormente, o menor era visto como um problema, a doutrina era irregular, hoje a criança é vista como um sujeito de direitos, segundo Dias (2021), a criança não deve ser tratada como objeto de propriedade da família, mas como sujeito de direitos, em consonância com a evolução do Direito de Família. Segundo levantamento realizado pelo UNICEF, aproximadamente uma em cada cinco crianças e adolescentes no Brasil já foi exposta a situações de violência sexual facilitada pela tecnologia, o que demonstra a gravidade do problema.

A crescente incidência de crimes digitais contra crianças e adolescentes no Brasil evidencia a gravidade do problema no ambiente virtual. Dados recentes apontam que, em 2024, o país registrou aproximadamente 593 mil denúncias de exploração e abuso sexual infantil online, com média superior a uma denúncia por minuto. Em 2025, esse cenário se agravou, alcançando mais de 2.500 denúncias diárias, o que reforça a urgência de políticas públicas e mecanismos jurídicos eficazes de prevenção e repressão a tais condutas (Poder360, 2025).

Com essa evolução significativa, a criança e o adolescente possuem atendimento preferencial, a Lei traz consigo os princípios fundamentais e o Estatuto da Criança e do Adolescente Lei nº 8.069 do ano de 1990 coloca em prática, sabe-se que é na prática que é visto a diferença. Cumpre ressaltar que de acordo com o artigo 227 da Constituição Federal de 1988, não é somente a família, em seu convívio que necessita praticar essas prerrogativas, mas a lei dispõe também da sociedade e do Estado, que requer prioridade nessa proteção integral (Brasil, 1988).

O Estatuto da Criança e do Adolescente foi instituído em 13 de julho de 1990, no contexto posterior à redemocratização do Brasil, surgindo assim, à necessidade de regulamentar o artigo 227 da Constituição Federal de 1988. O Estatuto da Criança e do Adolescente de 1990, em sua forma total, garante que os direitos da criança e o adolescente serão colocados em prática, conforme diz a Constituição Federal de 1988. Conforme já mencionado, a criança possui os mesmos direitos fundamentais que qualquer outro indivíduo, ressaltando que, o Estatuto depende da atuação do Sistema de órgãos como Ministério Público, Conselho Tutelar e o Poder Judiciário como enfatiza Nucci (2021), a proteção dos direitos fundamentais exige mecanismos institucionais

eficazes e a atuação concreta do Estado.

Pode-se ter sucesso em construções de leis para amenizar o impacto do descaso com os direitos das crianças, porém, isso vai muito além de apenas uma criação de lei específica, ou agravante dela, mas como, e de que forma essa lei é aplicada. Já ressaltado neste trabalho que, o sucesso de tal lei depende mais do compromisso do que da própria lei, por vezes que nem sempre é aplicada corretamente.

Embora a Constituição Federal de 1988 deixa a plena certeza que existem três pilares para o direito ser estabelecido e por quem eles virão, o primeiro lugar de proteção é a família, é na formação de valores e crenças, no acolhimento e no afeto. Conforme leciona Farias (2021), é na família que nasce a proteção e a formação da pessoa.

Tem-se observado que, a proteção infantojuvenil não se limita ao ambiente familiar, estendendo-se também à atuação da sociedade e do Estado. Nesse cenário, o avanço das tecnologias digitais passou a integrar a realidade de crianças e adolescentes, criando novos espaços de convivência e, consequentemente, novos riscos. A proteção agora sai do mundo físico e entra no virtual ou digital, pelo uso excessivo de internet e meios digitais.

Constatam-se, grandes exposições de menores nas redes o que traz consequência como o, cyberbullying, crimes virtuais, vazamento de dados, mesmo que, as plataformas criem regras, punem usuários a internet vai muito além do que isso, evitar crimes, não é algo tão fácil ou mais acessível, somente isso não resolve. Logo, foi sancionado em 2018, e está em vigor desde 2020 A Lei Geral de Proteção de Dados Lei nº 13.709 do ano de 2018 que representa um importante marco na proteção de dados pessoais no Brasil, especialmente no que se refere à tutela de crianças e adolescentes no ambiente digital.

O artigo 14 da Lei Geral de Proteção de Dados de 2018 estabelece regras específicas para o tratamento de dados pessoais de crianças e adolescentes, determinando que tal tratamento deve ocorrer em seu melhor interesse. Dessa forma, a legislação reconhece a vulnerabilidade desse grupo no ambiente digital, exigindo maior rigor na proteção de suas informações pessoais.

A Autoridade Nacional de Proteção de Dados (ANPD) de 2018, destaca que o tratamento de dados de crianças e adolescentes impõe atenção redobrada e observa o princípio do melhor interesse. A utilização dos dados precisa ser feita de forma transparente, clara e acessível, especialmente aos responsáveis legais considerando que, mesmo com a Lei Geral de Proteção de Dados, é necessário ações voltadas no sentido de uma efetiva fiscalização e aplicação prática das normas, sendo assunto do próximo tópico.

3. OS CRIMES DIGITAIS COMETIDOS CONTRA MENORES

O enfrentamento dos crimes digitais contra menores no Brasil demanda uma atuação articulada entre legislação penal, normas de direito digital, políticas públicas e mecanismos de cooperação institucional. Diante da complexidade e da constante evolução dessas práticas ilícitas, o ordenamento jurídico brasileiro tem buscado adaptar-se por meio da criação de leis específicas e da interpretação extensiva de normas já existentes, com o objetivo de garantir proteção efetiva às vítimas e responsabilização dos agentes.

Inicialmente, destaca-se o papel central do Estatuto da Criança e do Adolescente Lei nº 8.069 de 1990, que constitui um dos principais instrumentos normativos de proteção aos direitos de menores no Brasil. No âmbito dos crimes digitais, o ECA ganhou especial relevância após as alterações promovidas pela Lei nº 11.829/2008, que passou a tipificar de forma mais abrangente condutas relacionadas à pornografia infantil.

Os artigos 240 a 241-E do ECA (1990) contemplam desde a produção até o armazenamento e compartilhamento de material ilícito, evidenciando a preocupação do legislador em atingir toda a cadeia criminosa. Nesse sentido, Nucci (2023) afirma que a legislação brasileira evoluiu significativamente ao criminalizar não apenas a produção, mas também a posse e a disseminação de material pornográfico envolvendo menores, ampliando o alcance da tutela penal.

Além do ECA (1990), o Código Penal brasileiro (1940) também desempenha papel relevante na repressão de condutas praticadas no ambiente digital. Crimes como estelionato (art. 171), ameaça (art. 147), extorsão (art. 158) e os crimes contra a honra (arts. 138 a 140) são frequentemente praticados por meio da internet, inclusive contra menores. Ademais, o artigo 218-C, introduzido pela Lei nº 13.718/2018, tipifica a divulgação de cena de sexo, nudez ou pornografia sem consentimento, podendo ser aplicado em situações que envolvam adolescentes.

Outro marco importante é a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que introduziu no Código Penal (1940) em seu artigo 154-A, a criminalização da condutas de invasão de dispositivo informático. Embora a previsão incursa no artigo 154-A do CP (1940) não seja voltada exclusivamente à proteção de menores, essa norma possui relevância indireta, especialmente em casos em que dispositivos de crianças e adolescentes são invadidos para obtenção de imagens ou dados pessoais.

No campo do direito digital, destaca-se o Marco Civil da Internet Lei nº 12.965 do ano de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da

internet no Brasil. Embora não tenha natureza penal, o Marco Civil desempenha papel fundamental na repressão de crimes digitais ao disciplinar a responsabilidade dos provedores de aplicação e de conexão. O artigo 19, por exemplo, prevê que os provedores somente podem ser responsabilizados civilmente por conteúdos gerados por terceiros após o descumprimento de ordem judicial de remoção.

Todavia, há exceção relevante no que se refere à pornografia de vingança, em que a retirada de conteúdo pode ocorrer mediante simples notificação do ofendido, conforme previsto no artigo 21 da referida lei. Tal dispositivo revela uma tentativa do legislador de conferir maior celeridade à proteção de direitos fundamentais, especialmente em situações de grande impacto à dignidade da vítima.

Segundo Pinheiro (2021), o Marco Civil da Internet representa um avanço ao estabelecer regras claras para a responsabilização no ambiente digital, mas ainda enfrenta desafios quanto à efetividade, sobretudo diante da velocidade de propagação dos conteúdos ilícitos.

Um novo marco se evidencia em relação a proteção da criança e do adolescente no meio digital, o Estatuto Digital da Criança e do adolescente lei n° 15.211 do ano de 2025, em suas disposições preliminares a referida lei dispõe sobre a proteção da criança no meio digital e vai ser aplicado a todos produto que é direcionado a crianças ou ao acessos que podem recair na timeline dos menores. Conforme dispõe a previsão do artigo primeiro da lei 15.211(2025).

> Art. 1º Esta Lei dispõe sobre a proteção de crianças e de adolescentes em ambientes digitais e aplica-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no País ou de acesso provável por eles, independentemente de sua localização, desenvolvimento, fabricação, oferta, comercialização e operação. (Brasil, *online*)

Na mesma normativa do ECA digital de 2025 o artigo 7 traz uma das medidas que protege os dados dos jovens, essa lei é especifica para os fornecedores de produto e serviço, onde o controle fica direcionado a um padrão de modelo que tem como prioridade o cuidado com o menor de idade.

> Art. 7º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão, desde a concepção de seus produtos e serviços, garantir, por padrão, a configuração no modelo mais protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerados a autonomia e o desenvolvimento progressivo do indivíduo e justificado o melhor interesse da criança e do adolescente. (Brasil, *online*)

No âmbito jurisprudencial, o Superior Tribunal de Justiça consolidou entendimento segundo o qual, nos termos do art. 19 do Marco Civil da Internet, os provedores de aplicação somente respondem civilmente por conteúdo ofensivo gerado

por terceiros quando, após ordem judicial específica, deixam de promover sua indisponibilização (STJ, 2025).Além disso, a jurisprudência pátria tem reconhecido a elevada gravidade dos crimes digitais praticados contra crianças e adolescentes, sobretudo em hipóteses de exploração sexual e disseminação de material ilícito, legitimando a adoção de respostas penais mais severas e medidas protetivas voltadas à tutela integral da infância (STF, 2025).

A atuação estatal também se materializa por meio de órgãos especializados, como as Delegacias de Repressão a Crimes Cibernéticos e núcleos especializados do Ministério Público, os quais vêm intensificando ações investigativas, medidas cautelares e denúncias voltadas à repressão de ilícitos praticados no ambiente digital (Ministério Público do Estado de São Paulo, 2025). Ademais, iniciativas da sociedade civil, como a SaferNet Brasil, desempenham papel relevante no recebimento de denúncias, na produção de dados estatísticos e na conscientização da população acerca dos riscos e formas de proteção no ambiente virtual (Safernet Brasil, 2026).

No entanto, apesar dos avanços normativos e institucionais, persistem desafios significativos na repressão dos crimes digitais contra menores. Um dos principais obstáculos reside na dificuldade de identificação dos autores, em razão da utilização de tecnologias que proporcionam anonimato relativo, como redes privadas virtuais (VPNs), criptografia e mecanismos de ocultação de identidade digital. Tal cenário dificulta a rastreabilidade das condutas ilícitas, compromete a coleta de provas e reduz a eficácia da persecução penal (Pinheiro, 2021; Blum; Abrusio; Uema, 2020; Europol, 2024).

Outro ponto crítico reside na morosidade na obtenção de dados junto a provedores de aplicação, especialmente quando estes se encontram sediados no exterior. A necessidade de acionamento de mecanismos de cooperação jurídica internacional, frequentemente marcados por formalidades procedimentais e tramitação prolongada, contrasta com a velocidade com que os crimes digitais são praticados e os conteúdos ilícitos disseminados. Nesse sentido, Postai (2023) destaca que a natureza transnacional da criminalidade cibernética exige instrumentos de cooperação internacional mais céleres e eficazes, aptos a viabilizar a obtenção tempestiva de provas digitais e a assegurar maior efetividade à persecução penal.

Além disso, há críticas quanto à insuficiência de estrutura estatal, tanto em termos de recursos tecnológicos quanto de capacitação de agentes públicos. A investigação de crimes digitais exige conhecimento técnico especializado em rastreamento digital, preservação de provas eletrônicas e inteligência cibernética, capacidades que ainda não se encontram uniformemente distribuídas no território nacional, gerando desigualdades na efetividade da persecução penal (Polícia Federal, 2024; safernet brasil, 2024).

Outro aspecto relevante diz respeito à prevenção, que ainda se mostra incipiente. Embora existam campanhas educativas e iniciativas institucionais voltadas à cidadania digital, tais medidas ainda não alcançam de forma efetiva toda a população, especialmente crianças e adolescentes em situação de vulnerabilidade social. Nesse contexto, a repressão penal isoladamente não se mostra suficiente, sendo imprescindível a formulação de políticas públicas integradas que envolvam educação digital, conscientização social e participação ativa da família, da escola e das instituições públicas (Safernet Brasil, 2024; universidade federal do Rio de Janeiro, 2025).

Por fim, destaca-se a recente adesão do Brasil à Convenção de Budapeste (2001) sobre o Crime Cibernético, que representa um avanço significativo na cooperação internacional. A convenção estabelece diretrizes para harmonização legislativa e facilitação da troca de informações entre países, contribuindo para o enfrentamento mais eficaz da criminalidade digital transnacional.

Diante do exposto, verifica-se que o Brasil possui um arcabouço jurídico relevante para a repressão dos crimes digitais contra menores, composto por normas penais, civis e administrativas. Contudo, a efetividade desses mecanismos ainda enfrenta limitações práticas, especialmente no que se refere à investigação, cooperação internacional e prevenção. Assim, torna-se evidente a necessidade de constante atualização legislativa e fortalecimento das instituições responsáveis pela proteção de crianças e adolescentes no ambiente digital.

CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo analisar os crimes digitais praticados contra menores e as possibilidades legais de sua repressão no ordenamento jurídico brasileiro, partindo da compreensão do fenômeno dos crimes cibernéticos, sua evolução e suas principais manifestações no contexto da sociedade da informação. Ao longo da pesquisa, evidenciou-se que o avanço tecnológico, embora tenha proporcionado inúmeros benefícios sociais, também ampliou significativamente os riscos e vulnerabilidades, especialmente no que se refere à proteção de crianças e adolescentes no ambiente digital.

A partir da análise desenvolvida, verificou-se que os crimes digitais contra menores apresentam características próprias que os tornam particularmente graves, como a amplitude do dano, a dificuldade de remoção de conteúdos ilícitos, o anonimato relativo dos agentes e a transnacionalidade das condutas. Além disso, a condição peculiar de desenvolvimento dos menores agrava os impactos dessas práticas, exigindo do Estado e da sociedade uma atuação mais rigorosa e efetiva.

No que se refere ao problema de pesquisa consistente em verificar em que medida o ordenamento jurídico brasileiro é eficaz na repressão dos crimes digitais praticados contra menores conclui-se que, embora exista um arcabouço normativo relevante e em constante evolução, sua efetividade ainda é limitada diante das particularidades do ambiente virtual.

De um lado, é inegável que o Brasil possui instrumentos jurídicos importantes, como o Estatuto da Criança e do Adolescente (1990), o Código Penal (1940), o Marco Civil da Internet (2014) e legislações específicas como a Lei nº 12.737/2012. Tais normas demonstram um esforço do legislador em acompanhar as transformações sociais e tecnológicas, ampliando a proteção jurídica e responsabilizando condutas ilícitas no meio digital.

Por outro lado, a pesquisa evidenciou-se que a existência de normas, por si só, não garante a efetividade da repressão penal. Persistem entraves significativos, como a dificuldade de identificação dos autores, a morosidade na obtenção de provas digitais, a dependência de cooperação internacional e a insuficiência de estrutura estatal para lidar com a complexidade dos crimes cibernéticos. Esses fatores contribuem para a sensação de impunidade e fragilizam a proteção dos menores no ambiente digital.

Além disso, observou-se que a atuação estatal ainda é predominantemente reativa, centrada na repressão após a ocorrência do dano, havendo lacunas importantes no campo da prevenção. A ausência de políticas públicas amplas e contínuas de educação digital e conscientização limita a capacidade de reduzir a incidência desses crimes, especialmente entre populações mais vulneráveis.

Diante desse cenário, torna-se evidente que o enfrentamento dos crimes digitais contra menores exige uma abordagem multidimensional, que vá além da simples aplicação do Direito Penal (1940). É necessário integrar esforços entre o Estado, a sociedade, as instituições de ensino, as famílias e as próprias plataformas digitais, de modo a construir um ambiente virtual mais seguro.

Como sugestões para o aprimoramento do sistema de repressão e prevenção, destacam-se: (i) o fortalecimento das estruturas de investigação, com investimento em tecnologia e capacitação de profissionais especializados; (ii) a ampliação e agilização dos mecanismos de cooperação jurídica internacional; (iii) a revisão e atualização constante da legislação, de modo a acompanhar a evolução tecnológica; (iv) a implementação de políticas públicas eficazes de educação digital, voltadas especialmente a crianças e adolescentes.

Por fim, é necessário a responsabilização mais efetiva das plataformas digitais na prevenção e remoção de conteúdos ilícitos. Ressalta-se que a proteção de crianças e adolescentes no ambiente digital não constitui apenas uma questão jurídica, mas um

compromisso ético e social. A construção de um espaço virtual seguro depende da atuação conjunta e consciente de todos os atores envolvidos, sendo o Direito instrumento essencial, mas não exclusivo, nesse processo.

Dessa forma, conclui-se que, embora o ordenamento jurídico brasileiro apresente avanços significativos no enfrentamento dos crimes digitais contra menores, ainda há um longo caminho a ser percorrido para garantir uma proteção efetiva, compatível com os desafios impostos pela era digital. Isso se deve, sobretudo, à constante evolução das tecnologias, que cria novas formas de prática delitiva e dificulta a atuação dos órgãos de investigação e repressão. Além disso, fatores como a insuficiência de recursos estatais, a necessidade de capacitação técnica especializada e a limitada cooperação internacional contribuem para a fragilidade na aplicação das normas existentes.

Por fim, torna-se fundamental o fortalecimento de políticas públicas voltadas à prevenção, à educação digital e à conscientização de crianças, adolescentes, famílias e educadores. Igualmente relevante é a promoção de uma atuação integrada entre Estado, sociedade e setor privado, especialmente as plataformas digitais, a fim de criar mecanismos mais eficazes de identificação, denúncia e remoção de conteúdos ilícitos. Assim, a construção de um ambiente virtual mais seguro depende não apenas do aprimoramento legislativo, mas também de ações coordenadas e contínuas que acompanhem as transformações tecnológicas e sociais contemporâneas.

REFERÊNCIAS

ANANIAS, Amanda Silvestre Patrus; MOURA, Anna Beatriz de Oliveira; FIGUEIREDO, Joana Nascimento Rennó de; RAGONESI, Vinicius Bretas. **O bem jurídico nos crimes informáticos**. *Revista do CAAP*, Belo Horizonte, v. 22, n. 1, p. 1-15, 2017. Disponível em: Revista do CAAP – O bem jurídico nos crimes informáticos. Acesso em: 20 maio 2026.

ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. *Jus Navigandi*, Teresina, ano 6, n. 53, 1 out. 2001. Disponível em: Jus Navigandi – Crimes de informática: uma nova criminalidade. Acesso em: 20 maio 2026.

BLUM, Renato Opice Blum; ABRUSIO, Juliana Canha; UEMA, Marcelo. **Manual de direito digital e compliance**. Rio de Janeiro: Forense, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes**. Brasília, DF, 24 maio 2023. Disponível em: ANPD – Enunciado sobre o tratamento de dados pessoais de crianças e adolescentes. Acesso em: 20 maio 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: Constituição da República Federativa do Brasil de 1988. Acesso em: 20 maio 2026.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001. *Diário Oficial da União: seção 1*, Brasília, DF, 13 abr. 2023. Disponível em: Decreto nº 11.491, de 12 de abril de 2023. Acesso em: 20 maio 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente. *Diário Oficial da União: seção 1*, Brasília, DF, 16 jul. 1990. Disponível em: Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente. Acesso em: 20 maio 2026.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a Lei nº 8.069/1990 para aprimorar o combate à produção, venda e divulgação de pornografia infantil. *Diário Oficial da União: seção 1*, Brasília, DF, 26 nov. 2008. Disponível em: Lei nº 11.829, de 25 de novembro de 2008. Acesso em: 20 maio 2026.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. *Diário Oficial da União: seção 1*, Brasília, DF, 3 dez. 2012. Disponível em: Lei nº 12.737, de 30 de novembro de 2012. Acesso em: 20 maio 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Marco Civil da Internet). *Diário Oficial da União: seção 1*, Brasília, DF, 24 abr. 2014. Disponível em: Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet. Acesso em: 20 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018. Disponível em: Lei nº 13.709, de 14 de agosto de 2018 – LGPD. Acesso em: 20 maio 2026.

BRASIL. Polícia Federal. **PF e SaferNet assinam memorando de entendimento para prevenção a crimes cibernéticos relacionados ao abuso sexual infantojuvenil**. Brasília, DF, 14 maio 2024. Disponível em: Polícia Federal – Memorando de entendimento com a SaferNet para prevenção a crimes cibernéticos relacionados ao abuso sexual infantojuvenil. Acesso em: 20 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Responsabilidade civil de provedores por conteúdo gerado por terceiros na internet**. Brasília, DF, 2025. Disponível em: Superior Tribunal de Justiça – Notícias e Comunicados. Acesso em: 20 maio 2026.

BRASIL. Supremo Tribunal Federal. **Jurisprudência relativa à responsabilização de plataformas digitais e proteção de direitos fundamentais no ambiente virtual**. Brasília, DF, 2025. Disponível em: Supremo Tribunal Federal – Portal Oficial. Acesso em: 20 maio 2026.

CAPEZ, Fernando Capez. **Curso de direito penal: parte geral**. 28. ed. São Paulo: Saraiva, 2023.

CASTELLS, Manuel Castells. **A sociedade em rede.** 6. ed. São Paulo: Paz e Terra, 2003.

CRESPO, Marcelo Xavier de Freitas. **Cibercrimes e direito penal.** São Paulo: Revista dos Tribunais, 2015.

DIAS, Maria Berenice Dias. **Manual de direito das famílias.** 14. ed. São Paulo:

Revista dos Tribunais, 2021.

EUROPOL. ***Internet Organised Crime Threat Assessment (IOCTA) 2024***. Haia, 2024. Disponível em: EUROPOL – Internet Organised Crime Threat Assessment (IOCTA) 2024. Acesso em: 20 maio 2026.

FARIAS, Cristiano Chaves de Farias; ROSENVALD, Nelson Rosenvald. **Curso de direito civil: famílias.** 13. ed. Salvador: JusPodivm, 2021.

GRECO, Rogério Greco. **Curso de direito penal**. 11. ed. Rio de Janeiro: Impetus, 2022.

MASINI NETO, Ameleto (org.). **Crimes cibernéticos**. Indaiatuba: Editora Foco, 2025. E-book.

MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. **Atuação institucional no enfrentamento aos crimes cibernéticos**. São Paulo, 2025. Disponível em: Ministério Público do Estado de São Paulo – Portal Oficial. Acesso em: 20 maio 2026.

NUCCI, Guilherme de Souza Nucci. **Estatuto da Criança e do Adolescente comentado**. Rio de Janeiro: Forense, 2021.

NUCCI, Guilherme de Souza Nucci. **Leis penais e processuais penais comentadas**. 17. ed. Rio de Janeiro: Forense, 2023.

PFEIFFER, Luci. **O desamparo da infância e adolescência: violências do mundo real e do mundo virtual**. *Revista do Observatório Proteca*, v. 1, n. 1, p. 1-21, 2022. Disponível em: Revista do Observatório Proteca – O desamparo da infância e adolescência: violências do mundo real e do mundo virtual. Acesso em: 20 maio 2026.

PINHEIRO, Patrícia Peck Pinheiro. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

POSTAI, Rogério. **Convenção sobre o crime cibernético: impactos da internalização no ordenamento jurídico brasileiro e na cooperação internacional**. *Boletim Científico da Escola Superior do Ministério Público da União*, Brasília, n. 60, p. 220-236, 2023. Disponível em: Boletim Científico da Escola Superior do Ministério Público da União. Acesso em: 20 maio 2026.

PODER360. **Brasil tem 593 mil denúncias de abuso infantil on-line. Brasília, 22 dez. 2025**. Disponível em: PODER360 – Brasil tem 593 mil denúncias de abuso infantil on-line. Acesso em: 20 maio 2026.

SAFERNET BRASIL. **Central Nacional de Denúncias de Crimes Cibernéticos**. Salvador, 2026. Disponível em: SaferNet Brasil – Central Nacional de Denúncias de Crimes Cibernéticos. Acesso em: 20 maio 2026.

SaferNet Brasil. **Cidadania digital deve ser prioridade na formação de professores que lidarão com TICs na educação**. Salvador, 4 jun. 2024.

SAFERNET BRASIL. **Segurança e cidadania digital em sala de aula**. Salvador, 2025. Disponível em: SaferNet Brasil – Portal Oficial. Acesso em: 20 maio 2026.

UNICEF. **Uma a cada cinco crianças e adolescentes no Brasil sofreu violência sexual facilitada pela tecnologia em um ano, revela estudo**. 2025. Disponível em: UNICEF Brasil – Comunicados de imprensa. Acesso em: 20 maio 2026.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. **Sobre cidadania digital e educação digital. Rio de Janeiro, 2025**. Disponível em: Universidade Federal do Rio de Janeiro – Portal Oficial. Acesso em: 20 maio 2026.

WENDT MITANI, Amanda. **A imprecisão da linguagem da lei e a dificuldade de comunicação entre delegados e peritos nos crimes de pornografia infantil pela internet**. *Revista Brasileira de Segurança Pública*, São Paulo, v. 6, n. 1, p. 118-131, 2012. Disponível em: Revista Brasileira de Segurança Pública – A imprecisão da linguagem da lei e a dificuldade de comunicação entre delegados e peritos nos crimes de pornografia infantil pela internet. Acesso em: 20 maio 2026.