

CRIMES SEXUAIS VIRTUAIS CONTRA CRIANÇAS E ADOLESCENTES: DESAFIOS PARA A LEGISLAÇÃO E APLICABILIDADE DA LEI

Sidyane Kelly Gonçalves de Araújo¹

Heloisa Bega Gonçalves²

Lucas Teixeira de Andrade³

Izabel Urani de Oliveira⁴

Virgílio Ricardo Coelho Meirelles⁵

RESUMO: A crescente dependência da sociedade da internet e das tecnologias digitais impulsionou avanços importantes, mas também propiciou o aumento de crimes cibernéticos, em especial aqueles relacionados à exploração sexual de crianças e adolescentes. Este objetivos do estudo como para ver comocomo as leis brasileiras mudaram ao longo do tempo para combater a pedofilia virtual, com foco nos problemas que surgem quando se tenta investigar e punir essas ações. As leis brasileiras mudaram ao longo do tempo para combater a pedofilia virtual, com foco nos problemas que surgem ao tentar investigar e punir essas ações. A a pesquisa se justifica porque o tema é importante social e legalmente, tanto social quanto legal, dado o aumento de casos de recrutamento, produção e compartilhamento de conteúdo sexual envolvendo menores em plataformas digitais .dado o aumento de casos de recrutamento, produção e compartilhamento de conteúdo sexual envolvendo menores em plataformas digitais. O o método utilizado foi uma análise qualitativa de dados relevantesanálise leis nacionais, de leis nacionais relevantes, como o Estatuto da Criança e do Adolescente, a Lei nº 12.737 /12, a Lei nº 12.965/14, a Lei nº 13.718/18 e a nova Lei nº 14.811/24. Como o Estatuto da Criança e do Adolescente, a Lei nº 12.737/12, a Lei nº 12.965 /14, a Lei nº 13.718/18 e a nova Lei nº 14.811/24, que ampliou a tipificação penal de condutas digitais contra menores. As evidências indicam que, mesmo com os progressos nas normas, ainda existem barreiras consideráveis para a identificação e punição dos infratores, incluindo o emprego de criptografia, utilização de identidades fictícias e o uso de moedas digitais. Além disso, há desafios técnicos e legais que afetam a cooperação a nível internacional. Assim, ressalta-se que, além das leis, é imprescindível o desenvolvimento de políticas públicas que priorizem a prevenção, a formação de profissionais especializados em investigações digitais e a provisão de um suporte humanizado para as vítimas

2652

Palavras-Chave: Pedofilia virtual. Crimes cibernéticos. Plataformas digitais. Legislação. contra crianças e adolescentes.

¹Discente do curso de Direito da Uninassau Palmas-TO.

²Discente do curso de Direito da Uninassau Palmas-TO.

³Discente do curso de Direito da Uninassau Palmas-TO.

⁴Docente orientadora no curso de Direito da Uninassau Palmas-TO. Especialização em Direito Civil, Direito Processual Civil e Direito do Consumidor pelo Centro Universitário Leonardo da Vinci. Mestranda em Sociedade, Tecnologia e Meio Ambiente pelo Centro Universitário UniEvangélica, na cidade de Anápolis-GO.

⁵Docente coorientador no curso de Direito da Uninassau Palmas-TO. Bacharel em Direito; Licenciado em Pedagogia; Especialista em direito e processo civil; Especialista em psicopedagogia; Mestre em Gestão do desenvolvimento Regional.

I INTRODUÇÃO

A integração da internet na rotina diária alterou de forma significativa a maneira como nos relacionamos, aprendemos, desempenhamos nossas funções profissionais e procuramos formas de lazer. Entretanto, juntamente com os diversos benefícios proporcionados pela conexão global, também apareceram novas formas de crimes que seriam inviáveis ou até impensáveis no mundo físico.

Dentre os vários delitos cibernéticos, a exploração sexual de crianças e adolescentes no meio digital se destaca como uma das formas mais preocupantes e destrutivas de abuso. Esses delitos se manifestam de diversas formas, incluindo a produção, compartilhamento e propagação de materiais relacionados ao abuso sexual infantil, bem como a manipulação de menores por meio de técnicas fraudulentas em contextos digitais.

Entre os diversos crimes cibernéticos, a exploração sexual de menores no ambiente digital é uma das formas de abuso mais alarmantes e prejudiciais. Esses crimes se apresentam de várias maneiras, incluindo a criação, disseminação e disseminação de materiais ligados ao abuso sexual de crianças, além da manipulação de menores através de métodos fraudulentos em ambientes digitais.

Neste cenário, o propósito deste estudo é examinar os crimes sexuais cometidos contra menores no meio digital, discutindo suas formas, a legislação em vigor e os obstáculos que as autoridades enfrentam na tentativa de prevenir tais condutas. A seleção deste assunto é motivada pela preocupação crescente com a vulnerabilidade dos menores na internet, impulsionada pela facilidade com que delinquentes conseguem acessar a internet podem acessar, explorar e abusar das vítimas, muitas vezes sem deixar vestígios. O progresso no uso de aparelhos móveis, computadores e outras tecnologias de comunicação criou um ambiente propício para que pessoas com intenções criminosas atuem sem as restrições físicas estabelecidas pelos limites territoriais. Este elemento aumenta consideravelmente a complexidade das investigações e complica a responsabilização dos infratores.

Este estudo foca principalmente em entender como os crimes sexuais contra crianças e adolescentes são realizados através de plataformas online. Adicionalmente, o objetivo é investigar as falhas nas ações legislativas e os desafios que os profissionais do direito e da segurança pública enfrentam para identificar e combater efetivamente tais práticas criminosas. Em um contexto de vertiginosa evolução tecnológica, surge a dúvida sobre a capacidade da legislação atual de acompanhar e combater essas ações criminosas, além de abordar os

obstáculos estruturais e operacionais que dificultam a luta eficaz contra esse tipo de violência, seja na prevenção ou na punição dos culpados.

O objetivo principal deste estudo é examinar as diversas formas de crimes sexuais praticados contra menores em plataformas digitais, examinando as medidas legislativas implementadas para combatê-los e os desafios que profissionais dos campos jurídico e de segurança pública enfrentam ao investigar tais delitos. Adicionalmente, a meta é analisar o papel desempenhado pela legislação vigente e identificar os avanços necessários para uma resolução mais eficaz deste grave problema.

O estudo está relacionado à preocupação crescente com o crescimento dos crimes sexuais no ambiente digital e à necessidade premente de desenvolver métodos mais eficientes para sua prevenção e punição. A análise detalhada das especificidades dos crimes sexuais na internet, aliada à análise detalhada das ferramentas legais à disposição para combatê-los, é essencial para promover um ambiente virtual mais seguro para crianças e adolescentes. Além disso, busca garantir que as vítimas recebam proteção integral e adequada.

O propósito do estudo, ao abordar este assunto, não é somente enriquecer a discussão acadêmica, mas também chamar a atenção para a urgência de ações efetivas. Isso inclui uma maior participação da sociedade e medidas eficazes das instituições governamentais e judiciais, priorizando o desenvolvimento de estratégias robustas para prevenir e combater esse tipo de crime.

2 CRIMES SEXUAIS VIRTUAIS CONTRA CRIANÇAS E ADOLESCENTES

Recentemente, a tecnologia, particularmente a informática e a internet, tornou-se um componente crucial da vida em comunidade. As ferramentas digitais se tornaram essenciais em vários campos, incluindo compras online, mídias sociais, serviços bancários, educação e profissões.

Contudo, o mesmo espaço virtual que promove tantas interações e progressos também tem servido de palco para a emergência de diversas práticas ilegais. Entre eles, os crimes online que ressaltam-se pela frequência e pelo impacto que causa para a sociedade. Um dos casos mais preocupantes é a pedofilia na internet, cuja incidência tem aumentado significativamente e gradativamente, estimulada pelo avanço tecnológico e pela crescente exposição dos usuários no ambiente digital.

2.1 O IMPACTO DA INTERNET NA SOCIEDADE CONTEMPORÂNEA

Com o progresso tecnológico, a utilização da internet tornou-se um componente essencial do dia a dia das pessoas, afetando diretamente vários aspectos sociais, culturais e econômicos. A internet não só simplifica a comunicação, mas também várias tarefas diárias, tais como compras, transações bancárias, lazer e educação.

Segundo Pinheiro (2017), as tecnologias de comunicação e informação converteram o mundo digital num terreno diversificado de interações sociais, educativas, econômicas e delituosas. A internet, originalmente projetada para fomentar a interação e o aprendizado, evoluiu para um ambiente favorável para a realização de atividades ilegais, tais como o tráfico de informações, fraudes financeiras e delitos sexuais.

Além disso, o rápido avanço e a globalização da internet permitem que os crimes digitais ultrapassem fronteiras físicas, possibilitando que criminosos atuem em qualquer parte do mundo. Martins (2017) ressalta que a conexão entre sistemas, dispositivos e redes digitais cria um ambiente vulnerável, complicando a regulamentação, visto que os delitos digitais frequentemente ocorrem em jurisdições distintas.

2.2 A TIPIFICAÇÃO DOS CRIMES SEXUAIS CONTRA CRIANÇAS E ADOLESCENTES NO AMBIENTE VIRTUAL

2655

Diversos países têm implementado legislações específicas para combater a pedofilia virtual, diante do crescimento dos crimes sexuais contra crianças e adolescentes em ambientes digitais. Na União Europeia, por exemplo, a Diretiva 2011/93/EU estabelece normas claras sobre o combate ao abuso sexual infantil, exigindo que os Estados-membros tipifiquem penalmente condutas como aliciamento online, posse e distribuição de material de abuso (Martins, 2017).

Nos Estados Unidos, o *Protect Our Children Act* e o *Children's Online Privacy Protection Act* (COPPA) impõem obrigações às plataformas e reforçam a cooperação entre agências para rastreamento de abusadores. Na Itália, a infiltração é empregada em casos de criminalidade organizada, especialmente em investigações de narcotráfico, com autorização judicial. Já na Alemanha, a técnica é usada em crimes graves, como tráfico de drogas e segurança do Estado, sendo necessária a aprovação do Ministério Público e com restrições de tempo e escopo. Em todos os casos, o uso de agentes infiltrados visa colher informações valiosas para a captura de criminosos e desmantelamento de redes ilícitas (Sarlet, 2024).

Já países como o Canadá, Reino Unido e Austrália têm adotado políticas de vigilância, cooperação internacional e uso de inteligência artificial para detecção de material ilícito, além de campanhas de educação digital. Esses modelos evidenciam a importância de marcos regulatórios adaptados à realidade virtual e à atuação transnacional dos crimes (Jesus, 2025).

No Brasil, o combate à pedofilia virtual conta com legislações importantes, como o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.718/2018, que ampliou a tipificação de crimes sexuais. Mais recentemente, a Lei nº 14.811/2024 atualizou o Código Penal e o ECA para incluir condutas como o aliciamento online, o armazenamento e a divulgação de conteúdo de exploração sexual infantojuvenil com agravantes quando praticadas via internet. Apesar desses avanços, ainda há lacunas normativas, especialmente no que diz respeito à responsabilização de plataformas digitais. Atualmente, tramitam projetos de lei no Congresso Nacional que visam reforçar a regulação do ambiente virtual e impor medidas mais rígidas para proteger crianças e adolescentes da exposição a conteúdo abusivo *on line* (Greco, 2025).

O ordenamento jurídico brasileiro, ao longo dos últimos anos, tem buscado atualizar-se para enfrentar os desafios impostos pelos crimes virtuais, incluindo a pedofilia digital. O Estatuto da Criança e do Adolescente (ECA), instituído pela Lei nº 8.069 de 1990, foi uma das primeiras legislações a tratar de forma explícita da proteção das crianças e adolescentes no país. O artigo 241 do ECA estabelece que é crime produzir, reproduzir, publicar, distribuir ou compartilhar material pornográfico envolvendo crianças ou adolescentes, com penas que variam de reclusão de 3 a 6 anos, além de multa (Martins, 2017).

Em 2014, o Brasil deu um passo significativo ao aprovar o Marco Civil da Internet (Lei nº 12.965/2014), um marco regulatório que visa estabelecer direitos e deveres para os usuários da internet, garantindo a privacidade e a liberdade na rede. O Marco Civil da Internet prevê, no artigo 7º, a proteção da privacidade dos usuários, assegurando o sigilo das comunicações privadas, sem que haja necessidade de ordem judicial para o monitoramento de dados, exceto em casos excepcionais (Sarlet, 2024).

Além disso, a Lei nº 13.718/2018 foi uma atualização importante da legislação, tratando de crimes como a divulgação de cenas de estupro e assédio sexual. Ela tipifica crimes digitais relacionados à pornografia e à violência sexual, tornando mais rigorosa a punição para a produção e divulgação de conteúdo pornográfico envolvendo menores. De acordo com o artigo 218-C do Código Penal, a pena para quem divulgar ou distribuir material envolvendo a

exploração sexual infantil é de 3 a 6 anos de reclusão (Jesus, 2025).

Embora o Brasil tenha adotado leis importantes para combater a pedofilia virtual, o problema continua crescente, e muitos criminosos se utilizam de novas tecnologias para burlarem as barreiras da legislação. A falta de regulamentação eficaz das plataformas digitais e o anonimato proporcionado pela internet dificultam a identificação dos criminosos (Greco, 2025).

A pedofilia, conforme definida pela Organização Mundial da Saúde (OMS), é um transtorno psicológico caracterizado pela atração sexual por crianças e adolescentes. No ambiente digital, esse crime assume novas formas, principalmente por meio da produção, distribuição e compartilhamento de imagens e vídeos de abuso infantil. A internet tem se mostrado uma poderosa ferramenta para a atuação de pedófilos, pois permite a disseminação de conteúdo pornográfico envolvendo menores de idade de maneira rápida, quase anônima, e muitas vezes sem grandes riscos de detecção (Santos, 2019).

Em um estudo sobre os avanços dos crimes cibernéticos, Rios (2020) destaca que a pedofilia virtual ocorre principalmente por meio do compartilhamento de conteúdo ilícito, como imagens e vídeos de crianças em situações explícitas de abuso sexual. Além disso, a utilização de plataformas digitais, como redes sociais e aplicativos de mensagens, tem sido uma prática comum entre pedófilos. Esses criminosos criam perfis falsos, muitas vezes se passando por pessoas da mesma faixa etária das crianças e adolescentes, para ganhar sua confiança e aliciar as vítimas (Jesus, 2025).

2657

O uso de dispositivos eletrônicos, como smartphones e webcams, tornou-se uma ferramenta amplamente utilizada para que menores compartilhem imagens e vídeos íntimos sem perceberem os riscos envolvidos. Segundo Martins (2017), essa vulnerabilidade aumenta o número de casos de pedofilia virtual, pois muitas crianças e adolescentes não têm plena consciência dos riscos de suas ações no ambiente digital.

O aumento da pedofilia digital tem se mostrado um problema crescente em diversas partes do mundo, incluindo o Brasil. O crescente acesso à tecnologia, a popularização de dispositivos como smartphones e webcams, e a maior exposição de crianças e adolescentes ao ambiente digital tornam esse público ainda mais vulnerável. A pedofilia digital é um crime multifacetado que não apenas envolve a produção de conteúdo ilícito, mas também a troca e o compartilhamento desse material por meio de plataformas digitais, muitas vezes protegidas por criptografia e anonimato (Martins, 2017).

Santos (2021) salienta que os criminosos digitais frequentemente utilizam plataformas protegidas por criptografia e redes privadas para compartilhar e distribuir material pornográfico infantil, o que dificulta o trabalho de rastreamento e detecção das autoridades. A utilização de criptomoedas, que garantem transações anônimas, também tem sido uma ferramenta comum entre os pedófilos digitais. Isso cria um grande obstáculo para a investigação e a punibilidade dos crimes, uma vez que os criminosos podem operar com maior liberdade e segurança, sem o risco imediato de serem identificados.

3 ASPECTOS LEGAIS E NORMATIVOS NO COMBATE AOS CRIMES SEXUAIS VIRTUAIS

No Brasil, a defesa de jovens e crianças contra a exploração sexual é embasada na Lei nº 8.069/90, conhecida como Estatuto da Criança e do Adolescente, ou ECA. Embora tenha sido criada antes da popularização da internet, o ECA estabeleceu os princípios de proteção total e os direitos essenciais dos menores, funcionando como fundamento para a responsabilização em contextos de violência, incluindo a sexual.

3.1. A LEGISLAÇÃO BRASILEIRA SOBRE CRIMES CIBERNÉTICOS E SEXUAIS

Com o passar do tempo, o Estatuto da Criança e do Adolescente sofreu várias mudanças para se ajustar às novas circunstâncias do dia a dia, incluindo a introduzida pela Lei no 13.431/17. Esta reforçou o sistema que assegura os direitos de crianças e adolescentes que são vítimas ou testemunhas de atos de violência, incluindo a violência digital, estabelecendo procedimentos específicos para seu acolhimento e escuta (Greco, 2025).

Com o aumento do uso da internet e o aparecimento de novas modalidades de crimes, a Lei nº 12.737/12 (Lei Carolina Dieckmann) se destacou ao classificar delitos cibernéticos no Código Penal. Embora não tenha sido criada especificamente para combater a exploração sexual infantil, essa legislação foi fundamental para afirmar a peculiaridade do ambiente online como um local de ações criminosas, punindo invasões de dispositivos, fraudes eletrônicas e a divulgação de dados pessoais, ferramentas essenciais para a investigação e responsabilização de autores de crimes sexuais virtuais contra crianças e adolescentes (Jesus, 2025).

Com nova redação, veio a Lei no 12.965/14, o Marco Civil da Internet, que estabelece um conjunto de normas para o uso da internet no Brasil, disciplinando direitos e deveres dos usuários e dos provedores de serviços. No que diz respeito à proteção de crianças e adolescentes, é especialmente relevante, por impor obrigações aos provedores de registros de acesso de

usuários no Brasil.⁸⁹⁰ A referida lei obriga ainda a eliminação de conteúdo indicado por decisão judicial como ilícito, fosse imagem ou vídeo de abuso sexual de menores a ser eliminado. Isso simplifica a detecção de infratores e a eliminação de conteúdos danosos da internet (Greco, 2025).

A Lei no 13.718/18, também conhecida como Lei de Importunação Sexual, apesar de não focar especificamente em crianças e adolescentes ou no contexto digital, alterou o Código Penal para estabelecer o delito de importunação sexual e modificar outras regras ligadas a crimes sexuais. No ambiente digital, essa legislação pode ser empregada em situações de interações sexuais dirigidas a menores que representem tal assédio, expandindo a proteção jurídica contra condutas abusivas (Moraes, 2024). O mais recente e específico avanço legislativo para o enfrentamento dos crimes sexuais contra crianças e adolescentes no ambiente virtual é a Lei nº 14.811/24. Essa lei promoveu alterações significativas no Código Penal, no ECA e na Lei nº 14.155/21, com o objetivo de tipificar novas condutas criminosas praticadas online contra menores e aumentar as penas para crimes já existentes quando cometidos por meio da internet.

Decidiu-se, com a edição da Lei nº 14.811/24, criminalizar, de forma expressa, o aliciamento online para fins sexuais, a produção, divulgação e transmissão de conteúdo de exploração sexual infantil e o armazenamento do mesmo tipo material, bem como agravar a pena de crimes como o estupro de vulnerável no caso de sua prática ser realizada por meio do ambiente digital. Isso pode ser considerado um esforço para adaptar a ordem legal à ameaça crescente do delito sexual online contra a infância e a adolescência, mas é insuficiente para a solução do cenário e impunidade dos criminosos.

2659

3.2. O MARCO CIVIL DA INTERNET: PROTEÇÃO DE DADOS E PRIVACIDADE

A Lei no 13.718/18, também conhecida como Lei de Importunação Sexual, apesar de não focar especificamente em crianças e adolescentes ou no contexto digital, alterou o Código Penal para estabelecer o delito de importunação sexual e modificar outras regras ligadas a crimes sexuais. No ambiente digital, essa legislação pode ser empregada em situações de interações sexuais dirigidas a menores que representem tal assédio, expandindo a proteção jurídica contra condutas abusivas (Moraes, 2024).

Do ponto de vista do Direito Penal, a doutrina tem se concentrado na análise dos delitos cibernéticos e na aplicação das leis penais vigentes às ações realizadas no meio digital. Isso destaca a importância de interpretar as leis penais de maneira a incorporar as novas formas de

delitos que surgiram com a tecnologia, incluindo as ligadas à exploração sexual infantil na internet (Jesus, 2025).

Obter registros de conexão e acesso, permitido pelo MCI sob ordem judicial (arts. 10 e 11), é considerado um recurso essencial para identificar a autoria e a materialidade desses delitos. No entanto, deve-se respeitar as garantias individuais e o devido processo legal. A doutrina penal também discute a responsabilidade dos provedores de aplicações pela não remoção de conteúdo ilegal após notificação judicial (art. 19). A omissão é vista como uma forma de participação em delitos recorrentes ou como negligência em situações de disseminação de material prejudicial (Greco, 2024).

No contexto do Direito Constitucional, é crucial entender a tensão entre os direitos de privacidade e intimidade (art. 50, X, CF) e o interesse público na segurança e na investigação de delitos. O Marco Civil é examinado como um esforço para regular o ambiente digital de acordo com os princípios constitucionais, impondo restrições à intervenção do estado na esfera privada dos usuários de internet. A obrigatoriedade de uma ordem judicial fundamentada para a obtenção de dados e remoção de conteúdo, estabelecida no MCI, espelha a salvaguarda constitucional do sigilo das comunicações (art. 50, XII, CF), que só pode ser violado em circunstâncias específicas e mediante autorização judicial (Moraes, 2024).

2660

Por outro lado, a dificuldade em categorizar e avaliar a questão, juntamente com a internacionalidade do problema e a instabilidade da propriedade em termos de informações digitais, é vital para o relacionamento jurídico. Nesse sentido, o Marco Civil da Internet se destina a ser de ajuda para todos os órgãos do aparato judicial e policial, uma vez que cria direitos e obrigações de um lado dos provedores de serviços de internet, localizados no Brasil, upesadamente de um de propriedade e estrutura que é possível de ser conseguido, e, de outra, implica na base de dados, o processamento dos dados abertos e no apontamento criminal do acusado que executa a atividade criminosa no território do país, entre outras dimensões, que exercem influência, (Bitencourt, 2024).

Do ponto de vista do Direito Constitucional e dos direitos fundamentais na era digital, discute-se a relevância de uma abordagem progressiva para os direitos de privacidade e proteção de dados diante de novas tecnologias. O MCI se alinha com as preocupações constitucionais sobre a dignidade humana e o pleno desenvolvimento da personalidade no ambiente digital ao garantir a proteção de dados pessoais e estabelecer limites para sua coleta e tratamento (Jesus, 2025).

Dessa forma, a aplicação do MCI na luta contra a exploração sexual infantil online deve considerar a necessidade de equilibrar a proteção de crianças e adolescentes com a defesa dos direitos fundamentais dos usuários da internet, conforme determina a Constituição Federal (Sarlet, 2024).

Em suma, a análise do Marco Civil da Internet pela ótica do Direito Penal e Constitucional revela sua importância como ferramenta legal que busca regular o espaço digital em conformidade com os princípios fundamentais da República. Coletar dados para investigações, responsabilizar prestadores de serviço e preservar a privacidade dos usuários são aspectos interconectados que exigem uma avaliação cuidadosa e equilibrada, visando ser eficaz no combate à exploração sexual infantil na internet, sem infringir os direitos e garantias individuais assegurados pela Constituição Federal (Moraes, 2024).

3.3. DESAFIOS NA INVESTIGAÇÃO DE CRIMES SEXUAIS VIRTUAIS

A apuração de infrações sexuais virtuais direcionadas à infância e juventude configura um território multifacetado e complexo, atravessado por desafios que extrapolam fronteiras físicas e demandam das autoridades policiais e judiciais uma perícia singular. A própria essência da internet, marcada pela sua característica transnacional e pela habilidade de proporcionar um véu de anonimato, ergue obstáculos consideráveis para a identificação, o rastreamento e a consequente responsabilização dos perpetradores desses delitos (Greco, 2025).

2661

Um dos entraves primordiais reside na natureza global e descentralizada da rede mundial de computadores. A facilidade com que criminosos podem operar a partir de qualquer ponto do planeta, valendo-se de servidores e plataformas hospedadas em jurisdições diversas, complexifica sobremaneira a aplicação da legislação nacional e a determinação da competência jurisdicional. A obtenção de informações cruciais para a investigação, frequentemente armazenadas por provedores de serviços de internet e de aplicações sediados em outros países, esbarra em intrincados mecanismos de cooperação jurídica internacional, caracterizados por procedimentos morosos e entraves burocráticos (Bitencourt, 2025).

O anonimato e a disseminação de identidades fictícias representam outro obstáculo de monta. A maleabilidade do ambiente online permite a criação de perfis falsos com notável facilidade, aliada ao uso de ferramentas que mascaram o endereço IP e outras informações de rastreamento. Essa capacidade de ocultação dificulta a vinculação da atividade delituosa à identidade real do agente, exigindo das equipes de investigação o emprego de técnicas

avanzadas de cibernética forense para tentar desvelar a verdadeira identidade por trás do rastro digital (Capez, 2025).

A evolução tecnológica impõe um ritmo de atualização constante para as autoridades encarregadas da investigação. Novas plataformas de comunicação, aplicativos com recursos de criptografia robusta e a efemeridade de mensagens desafiam as metodologias tradicionais de coleta de evidências digitais. A agilidade com que os criminosos se adaptam a essas inovações, explorando novas ferramentas para ocultar suas ações, demanda um investimento contínuo em treinamento especializado e no desenvolvimento de soluções tecnológicas forenses capazes de acompanhar esse dinamismo (Jesus, 2025).

A necessidade de um corpo de conhecimento técnico altamente especializado é inegável para a condução eficaz dessas investigações. Peritos e policiais precisam dominar áreas como informática forense, análise de tráfego de dados, recuperação de informações deletadas, rastreamento de endereços IP e a interpretação de metadados. A escassez de profissionais com essa expertise específica e a dificuldade em manter esses talentos nas instituições policiais constituem um fator limitante para a capacidade de resposta do Estado frente a essa modalidade criminosa (Mirabete, 2025).

A garantia da integridade e da autenticidade das provas digitais, ou seja, a preservação da cadeia de custódia, emerge como um desafio crítico. A natureza volátil e facilmente manipulável das evidências digitais exige a implementação de protocolos rigorosos desde o momento da coleta até a sua apresentação em juízo. Qualquer falha nesse processo pode comprometer a validade da prova e a responsabilização do acusado (Moraes, 2024).

2662

As questões de jurisdição e a complexidade da legislação aplicável em um contexto transnacional também representam um entrave significativo. Em casos que envolvem autores e vítimas localizados em diferentes países, a determinação de qual ordenamento jurídico deve prevalecer e qual autoridade possui competência para julgar o delito pode ser um processo complexo e demorado. A ausência de uma harmonização global das leis cibernéticas e as dificuldades inerentes à cooperação jurídica internacional podem, em muitos casos, culminar na impunidade.

Por fim, a proteção das vítimas, especialmente crianças e adolescentes, e a obtenção de seus depoimentos no ambiente virtual exigem uma abordagem particularmente sensível e a aplicação de técnicas especializadas. O trauma vivenciado pelas vítimas e sua vulnerabilidade demandam que a coleta de seus relatos seja conduzida por profissionais devidamente

capacitados, em um ambiente que promova a segurança e o acolhimento, evitando a revitimização. A análise dos dispositivos eletrônicos das vítimas para a obtenção de provas também deve ser realizada com o máximo de cuidado, respeitando sua privacidade e garantindo a integridade dos dados (Greco, 2025).

4 PREVENÇÃO, INVESTIGAÇÃO E SOLUÇÕES PARA O ENFRENTAMENTO DA PEDOFILIA VIRTUAL

O enfrentamento à pedofilia virtual exige, além da repressão penal, um forte compromisso com a prevenção, sendo a educação digital e a conscientização pública instrumentos indispensáveis nesse processo. O direito penal, como última ratio, deve ser acionado apenas quando os mecanismos de prevenção e controle social falham, conforme orientam Capez (2025) e Mirabete (2025), sendo fundamental que o Estado atue de maneira preventiva por meio de políticas públicas educativas que esclareçam a população, sobretudo crianças, adolescentes e responsáveis legais, acerca dos riscos existentes no ambiente virtual.

4.1 A IMPORTÂNCIA DA EDUCAÇÃO DIGITAL E DA CONSCIENTIZAÇÃO PÚBLICA

A vulnerabilidade de crianças e adolescentes em redes sociais, jogos on-line e aplicativos de mensagens decorre, em grande parte, da ausência de conhecimento sobre os perigos e as condutas típicas utilizadas por aliciadores. Martins (2017) observa que o desconhecimento das formas de abordagem utilizadas por criminosos digitais favorece o sucesso das ações delitivas. Dessa forma, a educação digital deve ser inserida nos currículos escolares e nas campanhas institucionais, possibilitando que menores desenvolvam um senso crítico e habilidades para reconhecer situações de risco.

Rogério Bretan (2012) destaca que a função preventiva do direito penal se fortalece quando há atuação coordenada entre o poder público, instituições educacionais e meios de comunicação, no sentido de promover o esclarecimento da sociedade sobre os delitos praticados no ambiente digital. Segundo o autor, a prevenção geral positiva busca dissuadir a prática delituosa por meio da informação e da formação da consciência social quanto à gravidade do crime.

A educação digital deve ser entendida como uma política pública de proteção infantojuvenil, em consonância com o princípio da proteção integral previsto no artigo 227 da Constituição Federal e no Estatuto da Criança e do Adolescente (Lei nº 8.069/90). Trata-se de

um dever compartilhado entre Estado, família e sociedade, que deve orientar a criança quanto ao uso seguro da internet, à preservação de sua intimidade e à rejeição de abordagens inapropriadas (Lowenkron, 2013).

Damásio de Jesus (2025) afirma que o direito penal não possui eficácia isolada para conter comportamentos delitivos, especialmente no ambiente digital, onde a atuação dos criminosos é contínua, dinâmica e camuflada por tecnologias que dificultam a repressão. Nesse contexto, a prevenção assume papel central, sendo a informação um dos meios mais eficazes para inibir condutas ilícitas e fortalecer a proteção de bens jurídicos fundamentais, como a dignidade sexual de menores.

A doutrina penal contemporânea entende que a prevenção primária, voltada à formação ética e digital dos cidadãos, é uma etapa indispensável na contenção de crimes sexuais virtuais. Mirabete e Mirabete (2025) ressaltam que o direito penal deve caminhar em paralelo com políticas educativas que promovam a responsabilização dos indivíduos e a construção de uma cultura de respeito às normas jurídicas no ambiente digital.

A promoção de campanhas públicas e escolares sobre segurança on-line, identificação de situações suspeitas e denúncia de condutas abusivas representa uma forma concreta de prevenção. Além disso, a capacitação de professores, servidores públicos e familiares para lidar

2664

com as novas tecnologias é essencial para a eficácia da rede de proteção (Martins, 2017). O papel da família também é destacado como núcleo de formação inicial. A ausência de diálogo entre pais e filhos sobre o uso da internet e seus perigos cria um espaço permissivo à atuação de abusadores. Assim, políticas de conscientização devem incluir orientações práticas para os responsáveis legais, de modo que estes possam exercer adequadamente sua função de supervisão. Além disso, a mídia deve ser aliada no processo de conscientização. Utilizar rádio, televisão, redes sociais e influenciadores digitais para difundir informações sobre segurança virtual e prevenção à pedofilia digital amplia o alcance da mensagem preventiva e fortalece a cultura de proteção dos direitos infantojuvenis (Moraes, 2024)

O desconhecimento técnico por parte da população sobre o funcionamento de algoritmos, redes privadas e plataformas digitais torna ainda mais urgente a inserção da educação digital em todos os níveis de ensino. Essa medida colabora não só para a prevenção de crimes, mas também para a autonomia digital responsável de crianças e adolescentes (Pnheiro, 2017).

Martins (2017) salienta que a desinformação favorece o anonimato e o encobrimento das práticas delitivas no ciberespaço, sendo a educação a principal barreira a esse avanço. Por isso, investir em programas permanentes de orientação digital é uma forma eficaz de dificultar a ação de redes criminosas que se valem da ingenuidade de menores para a obtenção de conteúdo ilícito.

A ausência de políticas públicas de conscientização contribui para a manutenção de altos índices de subnotificação desses crimes, como alerta Greco (2025), pois muitas vítimas sequer reconhecem que foram alvos de abuso ou têm receio de relatar os fatos. A educação digital, portanto, também contribui para a desnaturalização da violência sexual e para o fortalecimento da confiança institucional.

4.2 ESTRATÉGIAS DE INVESTIGAÇÃO E AÇÕES DE PREVENÇÃO NO AMBIENTE VIRTUAL

O enfrentamento à pedofilia virtual exige uma atuação articulada entre órgãos de segurança pública, Ministério Público, Judiciário e sociedade civil, sendo essencial o desenvolvimento de estratégias de investigação que sejam compatíveis com as particularidades do ambiente digital. A investigação de crimes cibernéticos, como a produção e o compartilhamento de material pornográfico infantil, exige técnicas especializadas e previsão legal que permita a atuação eficiente e legítima do Estado. Martins (2017) ressalta que o ciberespaço é dinâmico, anônimo e transnacional, o que impõe à persecução penal novos desafios metodológicos e legais.

A legislação brasileira vem se aperfeiçoando gradualmente no enfrentamento desse tipo de delito. A Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente - ECA) dispõe, em seu artigo 241-A, que é crime oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemática, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, com pena de reclusão de 3 a 6 anos e multa (Moraes, 2024). A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi um marco na tipificação dos crimes informáticos. Embora tenha caráter mais geral, seu art. 154-A do Código Penal passou a tipificar a invasão de dispositivo informático como crime, com pena de detenção de 3 meses a 1 ano e multa. Essa previsão é relevante na investigação de delitos sexuais virtuais, pois muitos aliciadores acessam conteúdos íntimos de vítimas por meio de invasões e engenharia

social (Jesus, 2025).

A Lei nº 14.811/2024 representa um avanço mais específico no combate à pedofilia digital. Ela inseriu no Código Penal o artigo 218-E, que tipifica o crime de aliciamento ou induzimento de criança ou adolescente, por meio da internet, com o fim de praticar crime contra a dignidade sexual, com pena de reclusão de 1 a 3 anos. Essa medida visa inibir o chamado "grooming", prática comum entre predadores digitais (Brasil, 2024).

No aspecto investigativo, uma das estratégias fundamentais é a rastreabilidade de dados. O Marco Civil da Internet (Lei nº 12.965/2014), em seu artigo 15, obriga os provedores de aplicações a manterem os registros de acesso a aplicações de internet, sob sigilo, pelo prazo de seis meses, o que permite a identificação de usuários em casos de abuso. Ainda, o art. 10 exige ordem judicial para o fornecimento de dados cadastrais e registros de conexão, reforçando o equilíbrio entre segurança pública e direitos fundamentais (Brasil, 2014).

A criptografia e o anonimato são entraves recorrentes nas investigações, sendo amplamente utilizados para dificultar a identificação dos infratores. Conforme Rios (2020), os criminosos utilizam redes privadas virtuais (VPNs), browsers como Tor e criptomoedas para encobrir sua identidade. Assim, o investimento em perícia forense digital e em equipes técnicas especializadas é indispensável para o rastreamento das condutas delitivas.

2666

Segundo Damásio de Jesus (2025), a atuação policial no ambiente digital deve ser precedida por autorização judicial específica, nos termos do art. 5º, inciso XII, da Constituição Federal, que protege o sigilo das comunicações, salvo, nas hipóteses e na forma previstas em lei, por ordem judicial. A garantia constitucional impõe limites e obrigações para a produção da prova, garantindo sua licitude e validade processual.

Greco (2025), afirma que a efetividade do Direito Penal depende de um processo penal eficiente e compatível com as transformações tecnológicas. Nesse sentido, defende o uso de medidas cautelares digitais, como a interceptação de comunicações eletrônicas (com autorização judicial, nos termos da Lei nº 9.296/1996) e o bloqueio de perfis em redes sociais, como forma de evitar a continuidade da prática delitiva e proteger vítimas em potencial.

O controle do conteúdo online deve ser acompanhado de mecanismos de denúncia e remoção de material ilegal. A Lei nº 12.965/2014, em seu artigo 19, estabelece que os provedores de aplicações de internet somente serão responsabilizados por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomarem as providências para a sua retirada. Isso obriga plataformas digitais a colaborar com o Judiciário na remoção de conteúdo

de abuso infantil.

Moraes (2024) observa que o direito à intimidade e à privacidade deve ser equilibrado com o interesse público na repressão a condutas gravíssimas como a exploração sexual infantil. A interpretação constitucional deve ser feita à luz da dignidade da pessoa humana (art. 1º, III, CF), com prevalência da proteção à infância quando houver conflito entre direitos fundamentais.

A prevenção também deve envolver o monitoramento das redes sociais e fóruns suspeitos por parte das autoridades policiais. Martins (2017) enfatiza que grupos organizados operam em plataformas fechadas e encriptadas, exigindo da investigação técnicas de infiltração e cooperação com entidades internacionais, uma vez que os dados muitas vezes estão em servidores estrangeiros.

Pinheiro (2017) destaca a importância de protocolos de cibersegurança nas escolas e instituições públicas como meio preventivo. A implementação de filtros, controle parental e programas educativos que ensinem boas práticas no uso da internet são essenciais para reduzir o número de vítimas e dificultar a ação de criminosos.

Sarlet (2024) ressalta que o princípio da efetividade dos direitos fundamentais deve orientar as políticas públicas voltadas à proteção de crianças e adolescentes no meio digital. Isso implica não apenas em repressão criminal, mas também em ações de capacitação técnica de profissionais da segurança pública, da educação e da saúde.

2667

O sucesso da repressão penal aos crimes de pedofilia virtual depende de uma cadeia de custódia rígida, que assegure a integridade das provas digitais. Qualquer falha na preservação dos dados pode comprometer a investigação e gerar impunidade, sendo necessário o aperfeiçoamento constante de protocolos periciais.

5 CONSIDERAÇÕES FINAIS

O combate à pedofilia virtual representa um dos maiores desafios da contemporaneidade no campo do Direito Penal e da proteção infantojuvenil. Embora o ordenamento jurídico brasileiro conte com um conjunto de leis que tipificam, reprimem e penalizam condutas relacionadas à exploração sexual de crianças e adolescentes na internet — como o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei de Crimes Informáticos (Lei nº 12.737/2012), e mais recentemente a Lei nº 14.811/2024 — essas normas, embora fundamentais, não são suficientes para o

enfrentamento pleno do problema.

Esta pesquisa contribuiu no sentido de oferecer uma análise crítica sobre os limites e avanços da legislação brasileira voltada à repressão da pedofilia online, destacando os obstáculos práticos enfrentados pelos órgãos de investigação e pela Justiça. A título de ilustração cite-se a transnacionalidade dos delitos, o anonimato proporcionado pela tecnologia e a carência de infraestrutura técnica e humana. Ao reunir e sistematizar essas informações, o estudo evidenciou a urgência de uma abordagem mais abrangente e integrada.

A legislação atual proporciona instrumentos para a responsabilização penal dos autores, para a cooperação com provedores de internet, e para a proteção dos direitos fundamentais das vítimas. No entanto, a efetividade dessas normas esbarra em dificuldades práticas como a transnacionalidade dos crimes, o anonimato proporcionado pelas tecnologias, a limitação de recursos técnicos e humanos nas polícias e a burocracia nos processos de cooperação internacional. Como apontam autores como Martins (2017) e Rios (2020), a complexidade do ambiente virtual exige constante atualização técnica, jurídica e institucional.

Dessa forma, torna-se indispensável a formulação e implementação de políticas públicas integradas, voltadas não apenas à repressão, mas, principalmente, à prevenção e educação digital. Ações de conscientização voltadas a pais, educadores e crianças sobre os riscos da internet, além do investimento na formação de profissionais especializados em crimes cibernéticos, são elementos fundamentais para mitigar a vulnerabilidade infantojuvenil no meio digital.

2668

É essencial também a ampliação de canais de denúncia acessíveis, o fortalecimento de órgãos especializados e o estímulo à cooperação interinstitucional e internacional. Políticas públicas que incentivem parcerias entre poder público, sociedade civil e setor privado são necessárias para criar um ecossistema digital mais seguro.

Apesar dos avanços legislativos no Brasil, o enfrentamento da pedofilia virtual demanda uma abordagem mais ampla, que articule direito penal, políticas públicas, educação digital e cooperação global. A proteção integral da infância e adolescência, prevista no artigo 227 da Constituição Federal, só será efetivamente garantida se houver vontade política, mobilização social e investimento contínuo na prevenção e combate a esses crimes tão graves e danosos à dignidade humana.

REFERÊNCIAS

BRETAN, M. E. A. N. **Violência sexual contra crianças e adolescentes mediada pela tecnologia da informação e comunicação: elementos para a prevenção vitimal**. 2012. Tese (Doutorado em Direito) - Curso de Direito - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal, Volume 1: Parte Geral**. 30. ed. São Paulo: Saraiva Educação, 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, Seção 1, p. 1, 3 dez.2012. www2.camara.leg.br

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, Seção 1, p. 1,24 abr. 2014.

BRASIL. **Lei nº 13.431, de 4 de abril de 2017**. Estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência. Diário Oficial da União, Brasília, DF, Seção 1, p. 1, 5 abr. 2017.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Diário Oficial da União, Brasília, DF, Seção 1, p. 1, 25 set. 2018.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal para agravar penas de crimes cometidos por meio da internet. Diário Oficial da União, Brasília, DF, Seção 1, p. 1, 28 mai. 2021.

BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Diário Oficial da União, Brasília, DF, Seção 1, p. 1, 15 jan. 2024.

CAPEZ, Fernando. **Curso de Direito Penal, Volume 1: Parte Geral**. São Paulo: Saraiva Educação, 2025.

GRECO, Rogério. **Curso de Direito Penal: Parte Geral**. Rio de Janeiro: Forense, 2025. JESUS, Damásio de. **Direito Penal, Volume 1: Parte Geral**. São Paulo: Saraiva Educação, 2025.

LOWENKRON, Laura. **O monstro contemporâneo: notas sobre a construção da pedofilia como "causa política" e "caso de polícia"**. Cadernos Pagu. 2013, n. 41, pp. 303-337. Disponível em: <https://doi.org/10.1590/S0104-83332013000200016>. Acesso em 14 abr. 2025. MARTINS, Guilherme Magalhães. **Crimes Cibernéticos**. São Paulo: Atlas, 2017.

MIRABETE, Julio Fabbrini; FABBRINI MIRABETE, Renato N. **Manual de Direito Penal, Volume 1: Parte Geral**. São Paulo: Atlas, 2025.

MORAES, Alexandre de. **Direito Constitucional**. São Paulo: Atlas, 2024.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Classificação Estatística Internacional de Doenças e Problemas Relacionados à Saúde - CID-10**. São Paulo: EDUSP, 2018.

PINHEIRO, Patricia Peck. **Direito Digital**. São Paulo: Saraiva Educação, 2017.

RIOS, Aurélio Wander Bastos. **Crimes Cibernéticos: Teoria e Prática**. 3. ed. Salvador: uspodivm, 2020.

SANTOS, Emerson Wendt dos. **Crimes Informáticos: Aspectos da Lei nº 12.737/2012**. 4. ed. Curitiba: Juruá, 2019.

SANTOS, Emerson Wendt dos. **Direito Penal Informático: Crimes Cibernéticos**. 6. ed. Curitiba: Juruá, 2021.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**. 13. ed. Porto Alegre: Livraria do Advogado Editora, 2024.