CRIMES *CIBERNÉTICOS*: ANÁLISE EVOLUTIVA E LEGISLAÇÃO PENAL

CYBERCRIMES: EVOLUTIONARY ANALYSIS AND CRIMINAL LEGISLATION

Lôize Karolyne Vilarindo Tavares[1]
Antônio Carlos do Ó de Sousa[2]

RESUMO: O presente artigo tem como objeto de estudo a criminalidade cibernética por meio de uma análise evolutiva, sob a ótica da legislação penal brasileira aplicadas aos casos concretos. O objetivo consiste em discutir os crimes praticados por meios digitais, observando suas transformações ao longo do tempo e as implicações jurídicas decorrentes da aplicação das normas penais vigentes. Trata-se de um estudo de natureza bibliográfica, com abordagem qualitativa e método dedutivo, baseado na revisão de doutrina especializada, legislação atualizada e jurisprudência recente, além da análise de dados estatísticos relacionados às decisões judiciais em matéria de crimes virtuais. A pesquisa identificou os principais marcos legislativos, como a Lei nº 12.737/2012, o Marco Civil da Internet, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) e a Lei nº 14.155/2021, apontando avanços normativos, mas também limitações estruturais em sua aplicação. Os resultados indicam que, apesar do progresso legislativo, persistem desafios como a capacitação técnica dos operadores do direito, a uniformidade jurisprudencial e a cooperação internacional, evidenciando a necessidade de aperfeiçoamento contínuo das normas e de sua efetiva aplicação. As considerações finais do estudo evidenciam que, devido à volatilidade das provas digitais, a dificuldade de identificação de agente e a complexidade técnica das condutas praticadas no ambiente virtual, cada vez mais, os criminosos impõe desafios mais específicos às estruturas tradicionais do sistema penal, necessitando de atualização de legislação, investimento em tecnologia e capacitação profissional como forma de respeito.

Palavras-chave: crimes cibernéticos; legislação penal; Lei Geral de Proteção de Dados.

ABSTRACT: This article examines cybercrime through an evolutionary analysis, from the perspective of Brazilian criminal law applied to specific cases. The objective is to discuss crimes committed through digital means, observing their transformations over time and the legal implications arising from the application of current criminal laws. This is a bibliographic study with a qualitative approach and deductive method, based on a review of specialized doctrine, updated legislation, and recent case law, as well as an analysis of statistical data related to judicial decisions on cybercrimes. The research identified key legislative milestones, such as Law No. 12,737/2012, the Brazilian Internet Civil Rights Framework, Law No. 13,709/2018 (General Data Protection Law), and Law No. 14,155/2021, highlighting regulatory advances but also structural limitations in their application. The results indicate that, despite legislative progress, challenges remain, such as the technical training of legal professionals, uniformity in case law, and international cooperation, highlighting the need for continuous improvement of standards and their effective enforcement. The study's final considerations highlight that, due to the volatility of digital evidence, the difficulty in identifying perpetrators, and the technical complexity of conduct in the virtual environment, criminals increasingly pose more specific

[1] [1]Aluna concludente do Curso de Bacharelado em Direito, da Faculdade do Cerrado Piauiense-FCP. E-mail: Loizevilarindo@icloud.com

[2] Orientador de conteúdo desse artigo, da Faculdade do Cerrado Piauiense-FCP, formado em Bacharelado em Direito pela Universidade Estadual do Piauí. Especialista em Direito Processual Civil pela Faculdade do Cerrado Piauiense. E- mail: carlosousapm@hotmail.com.br

challenges to the traditional structures of the criminal justice system, necessitating updated legislation, investment in technology, and professional training as a means of ensuring respect.

Keywords: Cybercrimes; Criminal legislation; General Data Protection Law.

INTRODUÇÃO

Nas últimas décadas, a sociedade vivenciou uma verdadeira revolução tecnológica que transformou profundamente a forma como nos comunicamos, trabalhamos, consumimos informação e interagimos com o mundo ao nosso redor. A *internet* e os meios digitais passaram a ocupar um papel central nas relações humanas, aproximando distâncias, otimizando processos e abrindo espaço para inovações em praticamente todas as áreas do conhecimento. No entanto, junto com os inúmeros benefícios trazidos pela era digital, emergiram também novos desafios, especialmente no campo da segurança e do Direito Penal. Os crimes cibernéticos surgem nesse contexto como uma das principais preocupações do século XXI, desafiando legislações tradicionais e exigindo respostas rápidas e eficazes por parte do Estado.

O acelerado avanço das tecnologias e da diversidade de crimes praticados no ambiente virtual tem imposto ao Direito Penal o desafio de acompanhar a sofisticação das condutas ilícitas que surgem nesse cenário. Nesse contexto, torna-se fundamental compreender se o arcabouço jurídico existente é capaz de garantir uma resposta estatal eficiente e adequada à complexidade do ambiente digital. Diante desse cenário, questiona-se: em que medida a legislação penal brasileira tem sido eficaz no enfrentamento dos crimes cibernéticos?

Como hipótese inicial, parte-se da premissa de que a legislação penal brasileira ainda se mostra reativa e fragmentada frente à complexidade dos crimes cibernéticos, o que compromete a efetividade da persecução penal e a proteção de direitos fundamentais. Embora avanços importantes tenham ocorrido como a promulgação da Lei Carolina Dieckmann (Lei nº 12.737/2012), do Marco Civil da *Internet* (Lei nº 12.965/2014) e da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) , ainda existem lacunas normativas, dificuldades de aplicação prática e necessidade de cooperação internacional para enfrentar adequadamente esses delitos.

Dessa forma, a análise crítica dos crimes cibernéticos à luz da legislação penal brasileira torna-se essencial não apenas para compreender os limites atuais do sistema jurídico, mas também para apontar caminhos possíveis rumo a uma maior efetividade no enfrentamento dessas condutas. A constante evolução tecnológica exige do Direito Penal uma postura dinâmica, que alie rigor técnico, respeito aos direitos fundamentais e articulação com políticas públicas e cooperação internacional. É nesse contexto que o presente estudo se insere, buscando

oferecer uma contribuição relevante ao campo jurídico por meio de uma abordagem reflexiva, atualizada e propositiva.

A escolha do tema se justifica pela urgência de refletir criticamente sobre a capacidade do sistema penal brasileiro em lidar com práticas ilícitas digitais que afetam diretamente direitos como privacidade, honra, liberdade de expressão e segurança da informação, sem descurar dos limites constitucionais que resguardam o Estado Democrático de Direito. Nessa perspectiva, este estudo tem como objetivo geral analisar criticamente a eficácia e os limites da legislação penal brasileira no enfrentamento dos crimes cibernéticos. Identificar os principais marcos legislativos relacionados aos crimes cibernéticos no Brasil, examinar como a legislação penal tem sido aplicada em situações práticas e julgados recentes, analisar os desafios enfrentados pelas autoridades na investigação e repressão dos delitos virtuais e avaliar a eficácia da legislação penal frente aos avanços tecnológicos e às novas modalidades de crimes digitais, destacando eventuais lacunas normativas.

Assim, a presente pesquisa organiza-se em torno de três eixos principais: a análise da evolução histórica dos crimes cibernéticos e de sua consolidação na sociedade contemporânea; a investigação da legislação penal brasileira e seus limites frente às novas formas de criminalidade digital; e a avaliação da eficácia normativa e dos desafios práticos da aplicação da lei penal no combate aos delitos virtuais, delimitando-se o estudo de forma exclusiva ao ordenamento jurídico penal brasileiro, com foco na legislação e na jurisprudência nacional aplicáveis aos crimes cibernéticos.

1 A EVOLUÇÃO DOS CRIMES *CIBERNÉTICOS* NA SOCIEDADE CONTEMPORÂNEA

A sociedade atual é profundamente marcada pelo avanço tecnológico e pela integração da vida cotidiana ao meio digital. A transformação, apesar de positiva possibilitou o surgimento de novas formas de criminalidade. Os chamados crimes cibernéticos, ou delitos informáticos, representam um fenômeno contemporâneo que desafia os modelos tradicionais de prevenção, investigação e punição penal. A evolução desses crimes acompanha, de forma direta, a popularização e sofisticação dos recursos tecnológicos, exigindo atualização jurídica.

É relevante destacar que a prática de crimes cibernéticos acarreta consequências significativas tanto no âmbito individual quanto coletivo. Esses delitos podem gerar impactos sociais profundos, além de comprometer a estabilidade psicológica e econômica das vítimas expostas a situações de constrangimento, perdas patrimoniais e abalos emocionais. A criminalidade digital transcende a mera violação de sistemas informáticos, pois interfere

diretamente na dignidade da humana e no equilíbrio das relações sociais contemporâneas.

1.1 O SURGIMENTO DA CRIMINALIDADE DIGITAL E SEUS PRIMEIROS REGISTROS

A criminalidade digital teve seus primeiros sinais ainda nas décadas de 1960 e 1970, nos Estados Unidos e Europa, quando sistemas computacionais começaram a ser utilizados em estruturas militares e universitárias. Nessa época, já ocorriam acessos não autorizados, manipulações indevidas de dados e sabotagens virtuais, que sinalizavam a emergência de uma nova tipologia de conduta delituosa. Entretanto, essas ações eram tratadas ainda como exceções, não recebendo atenção legal imediata.

No Brasil, o fenômeno dos crimes digitais começou a ganhar relevância na década de 1990, impulsionado pela ampliação do acesso à *internet*. A conectividade favoreceu tanto a democratização da informação quanto o surgimento de práticas ilícitas como fraudes bancárias online, disseminação de vírus e ataques a sistemas governamentais. Segundo Medeiros e Ugalde (2020), a evolução da tecnologia não foi acompanhada, à época, por uma normatização jurídica eficiente, o que tornou o combate a esses crimes mais difícil.

Durante os anos 2000, essa defasagem legislativa passou a representar um problema real no cenário penal brasileiro. Os crimes cometidos em ambientes virtuais eram, muitas vezes, enquadrados em tipos penais clássicos, como estelionato e dano, o que não refletia a complexidade dos fatos. Como destaca Ramos (2017), a ausência de normas específicas prejudicava a atuação das autoridades, sobretudo no que se referia à obtenção de provas técnicas e à tipificação exata dos delitos.

> No início da década de 2010, a pressão popular e os debates parlamentares em torno da proteção de dados e da privacidade digital culminaram na criação da Lei nº 12.737/2012. Essa norma visou, entre outros objetivos, criminalizar a invasão de dispositivos informáticos, permitindo ao ordenamento jurídico nacional um mínimo de adequação aos desafios impostos pelo avanço da tecnologia e pelo crescimento das práticas criminosas no ciberespaço (Ramos, 2017, p. 22).

Além da Lei nº 12.737/2012, o Marco Civil da *Internet* (Lei nº 12.965/2014) também representou um avanço importante, ao estabelecer princípios e diretrizes para o uso da *internet* no Brasil, com foco na proteção dos direitos dos usuários. Essa legislação incorporou os conceitos de neutralidade da rede, inviolabilidade da intimidade e da vida privada, bem como a responsabilidade dos provedores em relação à guarda e fornecimento de dados. Segundo Nascimento et al. (2017), o Marco Civil deu suporte normativo à atuação do Judiciário e do

Ministério Público no combate à criminalidade digital.

A tipificação dos crimes eletrônicos ainda foi ampliada com a promulgação da Lei nº 14.155/2021, que alterou o Código Penal para prever penas mais rígidas em casos de fraudes cometidas em ambientes eletrônicos. Conforme observa Gomes e Medrado (2023), as alterações legislativas foram uma resposta à intensificação dos golpes digitais, especialmente durante a pandemia, quando cresceu o número de vítimas de estelionato virtual em todo o país.

> A Lei 14.155/2021 surge em um contexto de adaptação e modernização do Código Penal. Ela representa uma tentativa do legislador brasileiro de adequar os dispositivos legais às novas formas de delinquência praticadas por meios informáticos, prevendo agravantes específicas e ampliando o rol de condutas consideradas criminosas no ambiente digital (Gomes; Medrado, 2023, p. 1886).

Apesar dos avanços legislativos, o Brasil ainda enfrenta desafios na repressão qualificada aos crimes cibernéticos, especialmente em relação à estrutura investigativa, à capacitação técnica dos operadores do Direito e à cooperação internacional. Conforme argumenta Dobler (2023), o enfrentamento eficaz da criminalidade digital exige a implementação de mecanismos de cooperação jurídica internacional, sobretudo diante da natureza transnacional dos delitos cometidos em rede.

Nesse contexto, é imprescindível que o Estado invista em políticas públicas voltadas à segurança digital, bem como na atualização constante de seu arcabouço normativo e institucional. A criminalidade virtual se reinventa constantemente, exigindo respostas jurídicas e tecnológicas igualmente dinâmicas e articuladas entre os poderes públicos, a sociedade civil e as empresas do setor tecnológico.

Observa-se, portanto, que o surgimento dos crimes digitais acompanha o desenvolvimento tecnológico global, refletindo a transição da sociedade para uma nova realidade comunicacional e informacional. Desde seus primeiros registros até os dias atuais, observa-se uma tentativa progressiva do ordenamento jurídico brasileiro de se adequar às demandas desse novo tipo de criminalidade, embora ainda persistam lacunas estruturais e operacionais que exigem atenção contínua.

1.2 A ASCENSÃO DA *CIBERCRIMINALIDADE* ORGANIZADA E O USO ESTRATÉGICO DA TECNOLOGIA

A criminalidade cibernética deixou de ser uma prática isolada e passou a constituir

redes criminosas transnacionais altamente organizadas. A estrutura dessas organizações assemelha-se a empresas, com funções específicas, hierarquia e operações que envolvem diversos países simultaneamente. Segundo Dobler (2023), o modus operandi das organizações digitais reflete a globalização do crime, que utiliza recursos tecnológicos de ponta para ocultar a identidade dos agentes e dificultar a atuação estatal.

A utilização estratégica de ferramentas tecnológicas como *ransomwares*, *phishing*, *spywares*, *bots*, *deepfakes* e criptografia de ponta tornou os crimes digitais mais lucrativos e praticamente indetectáveis. Conforme destaca Vieira (2023), os grupos cibercriminosos utilizam essas ferramentas para explorar vulnerabilidades em sistemas, capturar dados e extorquir vítimas, dificultando a responsabilização penal e o rastreamento da autoria.

O crescimento da criminalidade cibernética foi impulsionado, em grande parte, pela expansão da *deep web* e das criptomoedas. A *deep web*, ao permitir anonimato e descentralização, tornou-se o principal espaço para a comercialização de dados roubados e serviços ilícitos. Gomes e Medrado (2023) afirmam que a utilização de criptomoedas como meio de pagamento tem sido essencial para operações ilegais, pela ausência de controle e pela dificuldade de rastreabilidade das transações.

Além disso, a atuação descentralizada desses grupos criminosos representa um desafio real ao Direito Penal, que historicamente se fundamenta no princípio da territorialidade. A natureza transnacional dos delitos dificulta a cooperação jurídica entre países. Segundo Corrêa e Monteiro Neto (2023), a ausência de uma normativa internacional padronizada dificulta o enfrentamento efetivo da criminalidade digital, exigindo esforços conjuntos e adaptações legais.

> As organizações criminosas cibernéticas atuam de forma coordenada em diferentes países, valendo-se de ferramentas digitais para ocultar sua identidade, utilizar servidores em locais diversos e criptografar suas comunicações. essa atuação simultânea em múltiplos territórios impõe barreiras significativas à atuação estatal, exigindo uma reformulação das estratégias jurídicas convencionais (Dobler, 2023, p. 94).

Essa constatação exige uma análise crítica sobre a capacidade atual do Estado em oferecer respostas jurídicas efetivas. A atuação fragmentada das instituições públicas e a morosidade legislativa favorecem a impunidade. Para Medeiros e Ugalde (2020), a falta de infraestrutura tecnológica nas polícias judiciárias compromete a obtenção de provas e dificulta o mapeamento das redes criminosas virtuais.

A sofisticação das ações criminosas também envolve o uso de inteligência artificial e automação. Segundo Nascimento et al. (2017), os cibercriminosos têm adotado modelos

preditivos para atacar sistemas financeiros e redes públicas, selecionando alvos com base em padrões de comportamento e vulnerabilidades detectadas por algoritmos.

A atuação do Estado também precisa ser acompanhada por medidas preventivas e educativas. Vieira (2023) observa que o combate à cibercriminalidade exige a criação de políticas públicas de segurança digital que envolvam não apenas repressão, mas também conscientização da população sobre os riscos e modos de prevenção.

Portanto, a ascensão da cibercriminalidade organizada é um fenômeno complexo, que exige ações coordenadas, tanto no plano interno quanto internacional. A modernização legislativa, a capacitação técnica de agentes públicos e a consolidação de redes de cooperação entre países são medidas fundamentais para conter a expansão do crime digital e garantir a efetividade da proteção jurídica no ambiente virtual.

1.3 IMPACTOS SOCIAIS, ECONÔMICOS E SUBJETIVOS DOS CRIMES VIRTUAIS

A criminalidade cibernética tem repercussões que extrapolam os danos patrimoniais. O vazamento de dados sensíveis, a usurpação de identidade digital, a disseminação de conteúdos íntimos sem consentimento e os golpes aplicados por meio de aplicativos de mensagens produzem efeitos diretos na dignidade da pessoa humana. Esses crimes afetam valores fundamentais como a privacidade, a honra e a integridade psíquica das vítimas, exigindo respostas jurídicas adequadas e proporcionais.

Além disso, os danos psicológicos decorrentes da exposição pública e da violação de dados são severos, especialmente quando as vítimas se tornam alvo de humilhação, perseguição ou constrangimento no ambiente virtual. Segundo Vieira (2023), a vulnerabilidade das pessoas em meios digitais tem gerado um aumento nos casos de depressão, ansiedade e isolamento social, configurando uma nova forma de violência que necessita ser juridicamente reconhecida e combatida.

No ambiente corporativo, os ataques cibernéticos provocam perdas substanciais tanto no aspecto financeiro quanto na credibilidade institucional. Empresas que sofrem invasões de sistemas ou se tornam alvo de sequestros de dados enfrentam consequências que incluem sanções legais, perda de contratos e desvalorização no mercado. De acordo com Medeiros e Ugalde (2020), a preocupação com a proteção de dados e com os investimentos em segurança digital se tornou uma prioridade estratégica nas organizações.

A responsabilização das empresas por falhas na proteção dos dados pessoais também passou a ser regulada por legislações como a Lei Geral de Proteção de Dados Pessoais (Lei nº

13.709/2018). Conforme Gomes e Medrado (2023), a legislação brasileira avançou ao impor obrigações concretas aos controladores de dados, prevendo sanções administrativas e judiciais, além de reconhecer o dano moral decorrente da exposição indevida de informações sensíveis.

> Os crimes cibernéticos, especialmente os que envolvem a exposição de informações privadas ou ataques direcionados à integridade moral das vítimas, demandam um tratamento jurídico que vá além da reparação econômica, pois envolvem a proteção da intimidade, da vida privada e da honra, valores constitucionalmente assegurados no ordenamento brasileiro (Gomes; Medrado, 2023, p. 1889).

Essa citação evidencia a necessidade de compreender os crimes digitais sob uma ótica que transcenda a esfera patrimonial, incorporando princípios constitucionais como a dignidade da pessoa humana e a inviolabilidade da intimidade. O sistema jurídico precisa adotar uma postura mais sensível diante dessas novas modalidades delitivas, estabelecendo mecanismos céleres e eficazes de reparação.

Do ponto de vista coletivo, os crimes digitais geram um sentimento generalizado de insegurança. O medo de ter dados pessoais violados ou de ser vítima de fraudes eletrônicas prejudica a confiança dos usuários em plataformas digitais, impactando diretamente o uso das tecnologias na vida cotidiana. Conforme destaca Dobler (2023), o enfraquecimento da segurança digital compromete o pleno exercício da cidadania digital e o acesso igualitário aos meios de informação e comunicação.

A desinformação, aliada ao uso estratégico de dados roubados e perfis falsos, representa uma ameaça ao próprio funcionamento das democracias modernas. Corrêa e Monteiro Neto (2023) argumentam que a criminalidade cibernética deve ser enfrentada com instrumentos de cooperação jurídica internacional, dada a complexidade dos fluxos transnacionais envolvidos na disseminação dos delitos digitais.

Embora o Brasil tenha avançado com a adesão à Convenção de Budapeste e com as recentes alterações legislativas promovidas pela Lei nº 14.155/2021, os desafios permanecem expressivos. As estruturas de investigação, o Judiciário e o Ministério Público carecem de qualificação técnica específica para lidar com os elementos de prova oriundos do ambiente digital, o que compromete a efetividade das decisões judiciais, como apontado por Nascimento *et al*. (2017).

Diante disso, é indispensável que o enfrentamento dos crimes cibernéticos seja pautado por uma abordagem jurídica multidisciplinar, combinando direito penal, direito digital, proteção de dados e garantias fundamentais. O avanço tecnológico não pode ser dissociado da responsabilidade estatal em proteger o cidadão diante das novas formas de violência que

emergem no ciberespaço.

2 LEGISLAÇÃO PENAL BRASILEIRA E OS DESAFIOS FRENTE AOS CRIMES DIGITAIS

A legislação penal brasileira tem evoluído de forma gradual frente à crescente complexidade dos crimes cibernéticos. Os avanços tecnológicos, ao transformarem as dinâmicas sociais e econômicas, também impuseram novos desafios à aplicação do direito penal. Segundo Gomes e Medrado (2023), a modernização legislativa foi impulsionada pela necessidade de combater práticas delituosas que ultrapassam fronteiras e exigem respostas mais dinâmicas do ordenamento jurídico.

O primeiro marco legislativo relevante foi a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipificou a invasão de dispositivos informáticos. Esta norma foi uma resposta direta a um caso concreto que expôs a fragilidade da legislação brasileira frente à violação de dados pessoais. Conforme observa Vieira (2023), a edição da lei evidenciou a lacuna normativa até então existente sobre crimes digitais e estimulou a formulação de novos instrumentos legislativos.

Outro avanço significativo foi a promulgação da Lei nº 12.965/2014, o Marco Civil da *Internet*. Esta lei estabeleceu princípios, garantias e deveres para o uso da *internet* no Brasil, com destaque para a proteção da privacidade e dos dados pessoais. Segundo Corrêa e Monteiro Neto (2023), o Marco Civil foi essencial para delimitar responsabilidades civis e criar fundamentos legais que contribuíram para a futura construção da Lei Geral de Proteção de Dados.

A Lei nº 14.155/2021, por sua vez, reformulou dispositivos do Código Penal, aumentando as penas para crimes cometidos por meio de fraudes eletrônicas, especialmente quando há uso de informações indevidamente obtidas ou transferências bancárias. Como afirmam Medeiros e Ugalde (2020), essas alterações demonstram um reconhecimento legislativo da gravidade e da sofisticação dos crimes cibernéticos, que exigem respostas mais severas e eficientes por parte do Estado.

Apesar dos avanços legislativos, persistem lacunas normativas e conceituais que comprometem a eficácia da repressão penal. A legislação ainda não acompanha, em sua integralidade, a velocidade com que surgem novas modalidades de delitos no ciberespaço. Conforme destacam Nascimento *et al*. (2017), o ritmo acelerado da inovação tecnológica cria

situações delituosas não previstas em lei, dificultando a tipificação penal adequada e enfraquecendo a segurança jurídica.

> A legislação brasileira, apesar de conter avanços pontuais, ainda é insuficiente para lidar com a amplitude dos crimes digitais. a ausência de uma estrutura normativa sólida, que considere a transnacionalidade dos delitos e a complexidade técnica das condutas, prejudica o combate eficaz à criminalidade cibernética, além de comprometer a proteção dos direitos fundamentais no ambiente virtual. a defasagem legislativa, somada à falta de uniformidade nos procedimentos investigativos, evidencia a urgência de reformas mais abrangentes e especializadas (Dobler, 2023, p. 98).

Além das limitações normativas, a investigação e a persecução penal dos crimes digitais enfrentam obstáculos operacionais expressivos. O ambiente virtual permite a atuação anônima e descentralizada dos agentes, dificultando a identificação e responsabilização dos autores. Para Gomes e Medrado (2023), a efetividade da lei penal depende da capacidade do Estado em produzir provas técnicas robustas, o que nem sempre é possível sem cooperação internacional.

A fragilidade estrutural das instituições de segurança pública também compromete o combate efetivo à criminalidade digital. A falta de capacitação especializada, aliada à carência de ferramentas tecnológicas apropriadas, impacta negativamente na apuração dos crimes. Conforme aponta Corrêa e Monteiro Neto (2023), o combate ao cibercrime exige a formação continuada dos operadores do Direito, bem como o investimento em inteligência cibernética.

> A persecução penal dos crimes informáticos esbarra não apenas na fragilidade das normas, mas também na limitação dos meios técnicos das autoridades encarregadas da investigação. é comum que provas digitais sejam perdidas, adulteradas ou sequer coletadas, o que compromete a responsabilização dos infratores e favorece a impunidade (Medeiros; Ugalde, 2020, p. 7).

Diante da realidade da criminalidade transnacional, destaca-se a importância da adesão do Brasil à Convenção de Budapeste sobre o *Cibercrime*. Essa convenção, conforme defendem Corrêa e Monteiro Neto (2023), fortalece a cooperação internacional e a harmonização de procedimentos entre países, permitindo respostas mais efetivas a condutas que ultrapassam as fronteiras nacionais.

Diante disso, embora o ordenamento jurídico brasileiro tenha dado passos relevantes no combate aos crimes cibernéticos, ainda são necessários avanços legislativos e estruturais. A legislação penal precisa ser continuamente atualizada para acompanhar a inovação tecnológica

e garantir a proteção eficaz dos direitos fundamentais no ambiente digital. A superação desses desafios depende de uma articulação entre legislação, investigação técnica, capacitação institucional e cooperação internacional.

2.1 MARCOS LEGAIS RELEVANTES NO COMBATE À CRIMINALIDADE DIGITAL

A legislação penal brasileira tem buscado se adequar, ainda que de forma gradual, às demandas surgidas com a expansão da criminalidade digital. Os primeiros esforços normativos voltaram-se para a criminalização de condutas que violam a privacidade e a integridade de dados pessoais, refletindo a preocupação do Estado com a proteção do indivíduo em ambiente virtual. Conforme afirmam Medeiros e Ugalde (2020), os crimes informáticos passaram a demandar tratamento jurídico específico diante da dificuldade de enquadramento nas normas penais clássicas.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, marcou o início de uma abordagem mais direta sobre crimes *cibernéticos*, introduzindo no Código Penal o artigo 154-A, que trata da invasão de dispositivos eletrônicos. A promulgação da norma ocorreu após um episódio de divulgação de fotos íntimas da atriz Carolina Dieckmann, o que demonstrou a fragilidade da legislação até então vigente. Segundo Nascimento *et al*. (2017), esse episódio evidenciou a urgência de um marco normativo que contemplasse condutas ilícitas no ambiente digital.

A referida lei passou a criminalizar a invasão de dispositivos informáticos com o intuito de obter, adulterar ou destruir dados sem autorização do titular, além da instalação de programas maliciosos com a mesma finalidade. Ainda que limitada em sua abrangência, a norma representou um passo importante para a proteção da privacidade digital. Vieira (2023) aponta que a lei trouxe visibilidade à necessidade de tipificação penal de práticas que afetam diretamente os direitos fundamentais no ciberespaço.

Posteriormente, a promulgação do Marco Civil da *Internet*, por meio da Lei nº 12.965/2014, consolidou princípios fundamentais para a utilização da *internet* no Brasil. A norma abordou a neutralidade da rede, a proteção da privacidade e a guarda de registros de acesso e conexão. Corrêa e Monteiro Neto (2023) ressaltam que essa legislação não visava criar tipos penais, mas sim estabelecer bases normativas para o funcionamento da *internet* e a responsabilização dos agentes envolvidos.

Ainda que o Marco Civil da *Internet* não tenha se destinado ao combate direto à

criminalidade, ele proporcionou avanços na regulamentação da atuação de provedores e no controle sobre a disseminação indevida de dados. Segundo Gomes e Medrado (2023), a obrigatoriedade de autorização judicial para fornecimento de dados fortaleceu o respeito aos direitos fundamentais e contribuiu para a construção de um ambiente digital mais seguro e transparente.

A promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), representou uma nova etapa na evolução legislativa voltada à proteção da privacidade e dos dados pessoais. A Lei Geral de Proteção de Dados (LGPD) estabeleceu princípios para o tratamento de dados por entidades públicas e privadas, fixando responsabilidades, direitos dos titulares e sanções em caso de descumprimento. Conforme destacado por Medeiros e Ugalde (2020), a Lei Geral de Proteção de Dados (LGPD) foi influenciada por normativas internacionais e buscou harmonizar a legislação brasileira aos padrões globais de proteção da privacidade.

A criação da Autoridade Nacional de Proteção de Dados (ANPD) pela Lei Geral de Proteção de Dados (LGPD) reforçou o compromisso institucional com a fiscalização e regulamentação do uso de dados pessoais. Gomes e Medrado (2023) explicam que a Autoridade Nacional de Proteção de Dados (ANPD) exerce papel estratégico na consolidação de uma cultura de proteção de dados no país, sendo responsável por editar normas complementares e aplicar sanções administrativas em caso de infrações.

Outro marco relevante foi a promulgação da Lei nº 14.155/2021, que alterou o Código Penal para prever penas mais severas para delitos praticados por meio eletrônico. A norma ampliou a pena do furto qualificado quando cometido mediante fraude eletrônica, especialmente nos casos em que há uso de informações obtidas indevidamente para transferências bancárias. Corrêa e Monteiro Neto (2023) destacam que essa mudança legislativa foi impulsionada pelo crescimento dos golpes virtuais durante a pandemia.

A referida lei também trouxe um agravante específico para casos de fraudes cometidas contra idosos ou pessoas em situação de vulnerabilidade, reconhecendo a especial proteção que essas populações merecem no contexto digital. Conforme Vieira (2023), a modernização do Código Penal representa um esforço do legislador para tornar a repressão aos crimes cibernéticos mais eficaz e proporcional à gravidade das condutas.

Como ressaltam Corrêa e Monteiro Neto (2023), a legislação nacional precisa de constante atualização para acompanhar a evolução tecnológica e os desafios transnacionais que caracterizam os crimes virtuais. A consolidação de uma estrutura normativa coerente, aliada à capacitação dos operadores do Direito e à cooperação internacional, é fundamental para a

construção de um sistema penal digitalmente eficiente. Essa construção, no entanto, ainda enfrenta entraves estruturais e práticos, exigindo um esforço conjunto entre o Estado, a sociedade civil e as instituições jurídicas para garantir maior efetividade na repressão e prevenção desses delitos.

2.2 LIMITAÇÕES LEGISLATIVAS E OS DESAFIOS DA TIPIFICAÇÃO PENAL

Apesar dos avanços observados na legislação penal brasileira, o ordenamento jurídico ainda apresenta lacunas significativas quando se trata da criminalidade digital. Diversas condutas praticadas no ciberespaço, embora socialmente reprováveis, não possuem previsão legal clara ou adequada. A criação de perfis falsos, por exemplo, nem sempre se enquadra de forma precisa nas figuras penais tradicionais, dificultando a responsabilização dos agentes e gerando insegurança jurídica para as vítimas.

O uso de tecnologias como *deepfakes* — vídeos ou áudios manipulados com a ajuda de inteligência artificial (IA) — agrava ainda mais esse cenário. Quando utilizados com o propósito de difamar, fraudar ou manipular a opinião pública, esses recursos configuram condutas graves, mas muitas vezes não são contempladas pela legislação vigente. Corrêa e Monteiro Neto (2023) observam que o Direito Penal brasileiro ainda carece de tipificações específicas para lidar com tais práticas, o que compromete a efetividade da repressão penal.

Outro exemplo de limitação legislativa está relacionado ao vazamento de dados em grupos fechados de aplicativos de mensagens. Embora essas ações possam gerar danos consideráveis, não há uma previsão normativa clara que abranja a totalidade da conduta, especialmente quando não há intenção explícita de extorsão ou chantagem. Gomes e Medrado (2023) apontam que, nesses casos, o enquadramento jurídico depende de interpretações extensivas, o que nem sempre é aceito pelo Judiciário por ferir o princípio da legalidade.

A ausência de atualização contínua da legislação penal contribui para a impunidade e para a sensação de insegurança no meio digital. A morosidade do processo legislativo impede que as normas acompanhem a velocidade das transformações tecnológicas. Conforme afirmam Medeiros e Ugalde (2020), enquanto o crime cibernético se reinventa em tempo real, a resposta estatal permanece atrasada, burocrática e limitada, o que enfraquece o sistema de justiça penal.

Além da lacuna normativa, existe o desafio de manter o equilíbrio entre a repressão penal e o respeito aos direitos fundamentais. O combate à criminalidade digital não pode ser utilizado como justificativa para violações à privacidade, à liberdade de expressão e ao devido

processo legal. Corrêa e Monteiro Neto (2023) ressaltam que o Estado deve agir com cautela ao ampliar seus poderes investigativos, assegurando que a proteção da sociedade não comprometa as bases democráticas.

A atuação do poder público deve se dar dentro dos limites constitucionais, especialmente em relação ao tratamento de dados pessoais e à interceptação de comunicações eletrônicas. Gomes e Medrado (2023) destacam que medidas invasivas precisam ser acompanhadas de autorização judicial fundamentada, sob pena de nulidade e responsabilização do Estado. O controle jurisdicional sobre ações repressivas é essencial para evitar abusos e garantir o equilíbrio entre segurança e liberdade.

A complexidade dos crimes digitais também impõe dificuldades na produção de provas. A volatilidade das evidências eletrônicas, associada à atuação transnacional de muitos criminosos, exige mecanismos de cooperação internacional mais eficazes. Medeiros e Ugalde (2020) afirmam que o Brasil ainda enfrenta limitações na integração com organismos estrangeiros, o que prejudica a efetiva responsabilização de autores de crimes transfronteiriços.

Além disso, a falta de uniformidade na interpretação e aplicação das normas contribui para decisões divergentes no âmbito judicial. Essa inconsistência compromete a previsibilidade do Direito Penal e dificulta a consolidação de jurisprudência específica para crimes cibernéticos. Vieira (2023) observa que a ausência de uma doutrina consolidada sobre os delitos informáticos também limita a atuação dos operadores do direito.

2.3 DIFICULDADES PRÁTICAS DE INVESTIGAÇÃO E APLICAÇÃO DA LEI PENAL

A aplicação prática da lei penal aos crimes cibernéticos enfrenta diversos entraves operacionais e estruturais. A atuação das autoridades responsáveis pela repressão penal é frequentemente prejudicada pela escassez de conhecimentos técnicos específicos. Delegados, promotores e peritos, em muitos casos, não possuem domínio aprofundado sobre linguagens de programação, redes criptografadas ou arquitetura de sistemas digitais. Segundo Medeiros e Ugalde (2020), essa lacuna dificulta a coleta de provas válidas e compromete o andamento de inquéritos envolvendo crimes digitais.

Além disso, a cadeia de custódia da prova digital exige procedimentos rigorosos que nem sempre são observados pelas autoridades. Arquivos eletrônicos, por sua natureza volátil, podem ser facilmente alterados, apagados ou perdidos. Gomes e Medrado (2023) destacam que, para garantir a validade da prova, é necessário preservar metadados, registros de acesso *(logs)* e históricos de navegação, que comprovem a autenticidade e integridade do conteúdo.

Outro obstáculo recorrente está na própria estrutura tecnológica das instituições públicas encarregadas da persecução penal. Muitas delegacias ainda carecem de equipamentos adequados, softwares forenses atualizados e servidores seguros para o armazenamento das provas digitais. Vieira (2023) aponta que a falta de investimento em infraestrutura cibernética compromete diretamente a eficiência das investigações criminais e a proteção da cadeia de custódia digital.

A cooperação internacional também se apresenta como uma das principais dificuldades enfrentadas no combate ao crime cibernético. Como muitos delitos digitais ocorrem entre países distintos — com autores, servidores e vítimas localizados em diferentes jurisdições — torna-se imprescindível a atuação coordenada entre Estados. Conforme explicam Corrêa e Monteiro Neto (2023), a inexistência de uma legislação penal internacional unificada e a lentidão na resposta de autoridades estrangeiras dificultam o acesso a dados em servidores externos e a responsabilização dos agentes.

A adesão do Brasil à Convenção de Budapeste sobre o *Cibercrime* representou um passo importante, mas a implementação plena dos seus dispositivos ainda encontra barreiras internas. A falta de articulação entre o Judiciário, o Ministério Público e a Polícia Civil ou Federal em pedidos de cooperação pode atrasar medidas urgentes. Gomes e Medrado (2023) observam que, mesmo com tratados vigentes, a burocracia envolvida em pedidos de auxílio internacional compromete a obtenção célere de provas.

Além disso, há um desafio metodológico quanto à distinção entre condutas lícitas e ilícitas no ambiente virtual. Atos como sátiras, perfis anônimos ou expressões ácidas, por vezes, são confundidos com práticas criminosas, o que leva a investigações indevidas ou imputações sem respaldo técnico-jurídico. Medeiros e Ugalde (2020) ressaltam a importância de formação ética e técnica dos investigadores para evitar excessos e respeitar os limites da liberdade de expressão.

A ausência de uniformização de procedimentos entre os Estados brasileiros também é uma dificuldade. Há divergência sobre os meios válidos de obtenção de provas, formas de perícia e prazos processuais, o que compromete a isonomia e a previsibilidade na aplicação da lei penal. Vieira (2023) aponta que a criação de delegacias especializadas em crimes digitais em apenas alguns estados do país contribuem para a desigualdade na repressão penal desses delitos.

O despreparo técnico das equipes de investigação impacta não apenas a fase de apuração, mas também a judicialização dos casos. Em muitos processos, há dificuldades na tradução dos elementos técnicos em provas juridicamente válidas. Corrêa e Monteiro Neto

(2023) afirmam que a ausência de uma atuação integrada entre peritos, promotores e magistrados resulta em decisões inconsistentes, com provas desconsideradas ou nulidades processuais.

Desse modo, as dificuldades práticas para a investigação e aplicação da lei penal aos crimes cibernéticos exigem ações estruturais urgentes. É imprescindível investir na capacitação dos operadores do direito, padronizar os protocolos de coleta e preservação de provas digitais, e ampliar a cooperação internacional. Somente assim será possível garantir a efetividade da repressão penal sem comprometer os princípios fundamentais do Estado Democrático de Direito.

3 A EFICÁCIA DA NORMA JURÍDICA NO COMBATE À CRIMINALIDADE DIGITAL

A crescente sofisticação dos crimes cibernéticos exige do Estado brasileiro uma resposta normativa eficaz e atualizada. Como garantidor da segurança jurídica e da ordem pública, compete ao Estado promover a criação de instrumentos legais que possibilitem o enfrentamento dessas condutas. Para Araújo (2021), a eficácia da norma penal depende diretamente da sua adequação à realidade tecnológica e da sua aplicação coerente por parte das instituições responsáveis.

A eficácia da legislação penal está intrinsicamente vinculada à capacidade do sistema de justiça de responder de forma célere e proporcional aos delitos digitais. Não basta que a norma exista; é essencial que sua aplicação seja eficaz, com operadores do Direito capacitados para lidar com as especificidades dos crimes informáticos. Nesse sentido, Castro (2021) observa que a complexidade técnica dessas infrações exige especialização e estrutura compatível com os desafios contemporâneos.

Casos concretos demonstram a importância da atualização normativa. A promulgação da Lei nº 14.155/2021, que agravou penas para fraudes eletrônicas, representa uma tentativa do legislador de acompanhar o avanço da criminalidade digital. Segundo Ferreira (2021), tal iniciativa reflete o esforço do poder público em ajustar o ordenamento jurídico à realidade dos delitos praticados por meio de tecnologias digitais, especialmente durante a pandemia.

No entanto, apenas a existência da norma não garante sua efetividade. Sanches (2018) destaca que a lentidão dos processos judiciais e a falta de estrutura tecnológica no sistema de justiça comprometem os efeitos práticos da legislação penal. Para que a norma seja eficaz, é

necessário que sua aplicação seja técnica, rápida e compatível com as particularidades do ambiente virtual.

O caráter preventivo da norma penal também é fundamental para sua eficácia. Quando bem estruturada e aplicada de forma regular, a lei atua como elemento de dissuasão, desestimulando a prática delituosa. Britto e Freitas (2017) ressaltam que a previsibilidade da punição e a percepção de risco jurídico são fatores determinantes para que potenciais infratores reconsiderem suas ações.

O dinamismo dos crimes virtuais impõe a constante revisão da legislação. Como afirma Kilian (2020), o Direito Penal precisa ser adaptado periodicamente para responder às transformações tecnológicas, evitando que condutas lesivas escapem à tipificação penal. Isso reforça a necessidade de um sistema jurídico flexível e atento às novas formas de criminalidade. A eficácia da norma também se amplia quando associada a políticas públicas de educação digital. Alves (2024) defende que o combate aos crimes cibernéticos deve incluir estratégias pedagógicas que promovam a cidadania digital, a segurança nas redes e a conscientização sobre o uso ético das tecnologias. Assim, a norma penal deixa de ser apenas repressiva e passa a integrar um sistema preventivo de proteção.

Outro elemento crucial é a estabilidade da jurisprudência. Decisões judiciais divergentes reduzem a segurança jurídica e comprometem a confiança dos cidadãos na aplicação da lei. Silva (2022) argumenta que a uniformização das decisões judiciais sobre crimes digitais é essencial para garantir a eficácia normativa e a isonomia na aplicação da justiça penal.

O fortalecimento das instituições responsáveis pela repressão penal é igualmente indispensável. Cunha (2019) afirma que a eficácia da norma jurídica depende da existência de polícias, ministérios públicos e magistrados capacitados, além de infraestrutura tecnológica apropriada. Sem tais elementos, mesmo uma legislação moderna pode se tornar ineficaz. Nesse sentido, torna-se evidente que o investimento na estrutura estatal é condição essencial para transformar o conteúdo jurídico em resultados concretos no combate aos crimes cibernéticos.

3.1 CAPACIDADE DE RESPOSTA AOS CRIMES CIBERNÉTICOS

A capacidade de resposta do ordenamento jurídico penal aos crimes cibernéticos está diretamente relacionada à suficiência e à efetividade das leis existentes. Com o aumento de práticas ilícitas no ambiente virtual, como fraudes eletrônicas, invasões de dispositivos e

disseminação de conteúdos ilícitos, tornou-se imperativo que o Estado reagisse com instrumentos normativos proporcionais. Para Araújo (2021), as legislações mais recentes ampliaram o alcance repressivo do Direito Penal, mas ainda carecem de harmonização com os aspectos tecnológicos que envolvem a dinâmica dos crimes virtuais.

As penas previstas na Lei nº 14.155/2021, por exemplo, evidenciam um avanço ao prever aumento de pena para fraudes cometidas com uso de dados de dispositivos móveis, especialmente em prejuízo de idosos. No entanto, autores como Ferreira (2021) sustentam que o endurecimento penal, embora necessário, não resolve por si só a questão da impunidade, pois a dificuldade investigativa e a lentidão processual acabam por fragilizar os efeitos práticos da lei.

Além disso, há divergências jurisprudenciais quanto à interpretação de condutas cibernéticas, o que compromete a resposta uniforme do Estado. Silva (2022) pontua que a ausência de um entendimento consolidado entre os tribunais contribui para decisões contraditórias, afetando diretamente a credibilidade da lei penal enquanto ferramenta de controle social no ambiente digital.

A eficácia da resposta penal depende, ainda, da atuação técnica e célere do sistema de justiça. Sanches (2018) afirma que a ausência de especialização nos quadros do Judiciário e do Ministério Público compromete o tempo de resposta estatal, permitindo que muitos crimes fiquem impunes ou sejam julgados sob tipos penais genéricos. Isso enfraquece o caráter preventivo e repressivo da norma. Assim, percebe-se que, embora o arcabouço jurídico tenha evoluído para responder aos crimes cibernéticos, sua eficácia está condicionada não apenas ao conteúdo normativo, mas à capacidade do Estado de aplicá-lo de forma técnica, uniforme e tempestiva.

3.2 APRIMORAMENTO E APLICAÇÃO DA LEI PENAL AOS CASOS CONCRETOS

O aprimoramento da aplicação da lei penal no enfrentamento dos crimes digitais exige uma abordagem estratégica que considere os avanços tecnológicos e a complexidade dos delitos praticados no ciberespaço. Segundo Kilian (2020), a simples positivação de normas não basta; é preciso garantir que sua aplicação seja adequada aos casos concretos, com operadores do direito qualificados e procedimentos atualizados.

Muitas vezes, condutas graves acabam sendo desqualificadas ou arquivadas por ausência de provas técnicas válidas. Britto e Freitas (2017) observam que isso decorre da fragilidade da estrutura pericial e da falta de formação específica dos agentes públicos

envolvidos na persecução penal.

A especialização de delegacias e promotorias tem contribuído para melhorar a aplicação da lei penal nos crimes cibernéticos. Alves (2024) ressalta que a atuação de núcleos especializados permite uma leitura mais técnica dos fatos, promovendo decisões mais adequadas à realidade digital e à complexidade das condutas envolvidas. Essa especialização também facilita a coleta de provas eletrônicas com rigor e segurança.

O aprimoramento da aplicação penal exige parcerias entre órgãos nacionais e internacionais. Santos e Martins (2017) destacam que a cooperação interinstitucional é essencial para viabilizar o acesso a provas que muitas vezes estão armazenadas em servidores estrangeiros. A efetivação dessas parcerias depende de acordos jurídicos internacionais e de uma legislação interna que seja compatível com os padrões globais.

Isso mostra que exige mais do que reformas legislativas. É necessário investir na qualificação institucional, na padronização de procedimentos e na integração entre os diversos órgãos envolvidos na repressão penal, garantindo que a resposta estatal seja efetiva e proporcional ao dano causado.

3.3 A LEI PENAL COMO FERRAMENTA DE PREVENÇÃO E REPRESSÃO APLICADA AOS CRIMES CIBERNÉTICOS.

A lei penal possui função preventiva no controle da criminalidade, inclusive no ambiente digital. A previsibilidade da sanção e a sua aplicação coerente são fundamentais para inibir a prática de delitos cibernéticos. Conforme aponta Castro (2021), a prevenção geral positiva da pena se realiza quando o cidadão reconhece que o Estado é capaz de punir de maneira justa e eficaz os comportamentos lesivos à ordem digital.

A utilização da lei penal como instrumento de prevenção é mais eficaz quando está aliada a ações educativas e de conscientização. Cunha (2019) ressalta que o Direito Penal, isoladamente, tem eficácia limitada na prevenção de condutas criminosas complexas e que a educação digital pode atuar como um mecanismo complementar essencial. A combinação entre repressão penal e programas pedagógicos voltados à ética digital é vista como uma estratégia de longo prazo.

No aspecto repressivo, a legislação atual tem tentado acompanhar os novos modelos de criminalidade digital com penas mais severas e previsões específicas. Araújo (2021) observa que a ampliação das penas e a inclusão de condutas típicas relativas à invasão de sistemas e fraudes bancárias reforçam a função repressiva do Direito Penal. No entanto, sua eficácia

depende do fortalecimento da estrutura de aplicação da norma.

A atuação coordenada entre Judiciário, Ministério Público e forças de segurança pública potencializa o uso da lei penal como ferramenta de contenção dos crimes cibernéticos. Alves (2024) argumenta que somente com uma rede institucional funcional e integrada é possível garantir a efetividade da norma penal. A ausência de diálogo entre esses agentes enfraquece a capacidade de atuação preventiva e repressiva do Estado.

Assim, a eficácia preventiva e repressiva da lei penal no combate à criminalidade digital está condicionada à sua aplicação eficiente, à formação técnica dos operadores jurídicos e à articulação de políticas públicas complementares. Quando bem estruturada, a legislação penal se mostra um instrumento indispensável para assegurar um ambiente digital seguro e juridicamente protegido.

METODOLOGIA

A presente pesquisa adota como base lógica a abordagem dedutiva, que parte de premissas gerais para alcançar conclusões específicas relacionadas ao tema da criminalidade cibernética e à eficácia da norma jurídica na sua repressão. Esse método é considerado apropriado para investigações jurídicas, uma vez que permite a análise de normas legais a partir de teorias consolidadas e dados extraídos da doutrina e da jurisprudência. Segundo Creswell (2024), a abordagem dedutiva é amplamente utilizada em estudos jurídicos por possibilitar a estruturação de hipóteses a partir de princípios teóricos gerais, os quais são posteriormente confrontados com os dados levantados.

Optou-se por uma pesquisa de natureza exploratória, pois se busca aprofundar o conhecimento sobre as limitações e potencialidades da legislação penal brasileira frente aos crimes praticados no ambiente digital. Esse tipo de investigação é recomendado quando se pretende obter maior familiaridade com um problema ainda pouco delimitado ou em constante transformação, como é o caso da criminalidade virtual. De acordo com Gil (2023), a pesquisa exploratória visa oferecer uma compreensão inicial do fenômeno estudado, sendo ideal para temas cuja complexidade exige análise teórica prévia antes de estudos empíricos.

Além disso, foi adotado um procedimento metodológico de cunho bibliográfico, tendo como finalidade compreender a estrutura normativa e os desafios de sua aplicação à luz da literatura especializada. O estudo se baseia na revisão de fontes primárias, como a Constituição Federal de 1988, o Código Penal Brasileiro (Decreto-Lei nº 2.848/1940), a Lei nº 12.737/2012, o Marco Civil da *Internet* (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº

13.709/2018) e a Lei nº 14.155/2021, além de fontes secundárias como artigos científicos extraídos de bases reconhecidas, tais como *SciELO*, Periódicos *CAPES*, *LexML* e Biblioteca Digital da Câmara dos Deputados. Conforme Lakatos e Marconi (2020), a pesquisa bibliográfica consiste na análise de contribuições teóricas publicadas por diversos autores com o objetivo de examinar e discutir um tema de forma sistematizada e fundamentada.

A coleta de dados será realizada por meio da seleção criteriosa de publicações acadêmicas, livros, legislações e relatórios técnicos e análise crítica excluindo-se duplicidades e trabalhos com baixo rigor metodológico ou excessiva semelhança entre si, garantindo-se, assim, a originalidade da análise e a relevância do conteúdo incluído. Segundo Severino (2018), a filtragem criteriosa do material bibliográfico é essencial para assegurar a qualidade e a profundidade das inferências teóricas em uma investigação de natureza jurídica.

Portanto, o percurso metodológico adotado neste trabalho busca garantir uma análise robusta e fundamentada sobre a eficácia das normas penais brasileiras no enfrentamento dos crimes cibernéticos, mediante uma revisão teórica ampla, atualizada e alinhada com os parâmetros científicos contemporâneos.

DISCUSSÃO E RESULTADOS

A partir da análise da produção doutrinária e legislativa recente, constatou-se que o Brasil tem promovido avanços significativos na normatização dos crimes cibernéticos, especialmente com a promulgação da Lei nº 14.155/2021. No entanto, os resultados indicam que tais avanços ainda não se traduzem em uma repressão penal plenamente eficaz, sobretudo devido à velocidade com que novas práticas delituosas surgem no ambiente virtual.

Verificou-se também que a legislação penal, apesar de atualizações pontuais, permanece reativa e fragmentada, o que dificulta sua aplicação uniforme. A ausência de um sistema penal digital estruturado, aliado à carência de recursos técnicos e humanos nas instituições de repressão penal, compromete o enfrentamento adequado desses crimes. Esse cenário é agravado pela insuficiência de capacitação técnica de juízes, promotores e agentes de segurança no trato com crimes de alta complexidade digital.

A construção do referencial teórico teve como finalidade compreender os principais conceitos envolvidos, como criminalidade digital, eficácia penal, cooperação jurídica internacional e segurança cibernética. A fundamentação foi necessária para contextualizar o tema e permitir um diálogo crítico entre os dispositivos legais e a doutrina jurídica. Segundo Cunha (2019), o referencial teórico deve ser usado não apenas como base de sustentação, mas

como instrumento de análise.

Dentre os principais resultados, constatou-se que o ordenamento jurídico brasileiro evoluiu com a edição de leis específicas, como a Lei nº 12.737/2012, o Marco Civil da *Internet* e a Lei nº 14.155/2021, que ampliaram a tipificação penal de condutas digitais. No entanto, como observam Corrêa e Monteiro Neto (2023), a existência da norma por si só não garante eficácia, sendo necessário o desenvolvimento de mecanismos adequados para sua aplicação.

A discussão desses resultados revelou que, embora as normas estejam presentes, muitas vezes não são efetivamente aplicadas, seja por lacunas técnicas na investigação, seja por desconhecimento das autoridades sobre aspectos tecnológicos envolvidos nos crimes. Gomes e Medrado (2023) ressaltam que a ausência de capacitação compromete o processo penal e pode resultar na impunidade dos agentes.

A jurisprudência brasileira ainda não é unificada quanto à aplicação dessas leis, o que prejudica a segurança jurídica e dificulta a previsibilidade das decisões judiciais. Silva (2022) aponta que a fragmentação interpretativa nos tribunais gera insegurança e compromete a eficácia repressiva da norma penal no meio digital.

Outro dado relevante diz respeito à ausência de uma política pública coordenada de prevenção à criminalidade cibernética. Embora a norma penal tenha caráter repressivo, sua aplicação isolada não é suficiente para conter o avanço dos delitos digitais. Santos e Martins (2017) sugerem que a lei penal deve ser acompanhada por medidas educativas e campanhas de conscientização voltadas à segurança digital da população.

Adicionalmente, observou-se que o uso da tecnologia como instrumento do crime exige atualização constante dos mecanismos legais. A introdução de novas formas de golpe, como *phishing*, *ransomware* e manipulação de identidade digital, demanda respostas legislativas rápidas. Alves (2024) defende que o legislador deve agir de forma proativa, antecipando-se aos riscos emergentes.

Apesar das contribuições, algumas limitações foram identificadas na pesquisa. Por ser um estudo de natureza bibliográfica, não foi possível realizar análises empíricas ou coleta de dados primários. Essa restrição, no entanto, não compromete os resultados, mas aponta para a necessidade de futuras investigações de cunho quantitativo, como propõe Britto e Freitas (2017).

No plano comparativo, verificou-se que o Brasil ainda está atrasado em relação a países que possuem estruturas jurídicas e tecnológicas mais integradas. Ferreira (2021) observa que sistemas jurídicos como o dos Estados Unidos e do Reino Unido apresentam maior sinergia entre normas e instituições, o que favorece a celeridade e a eficácia penal.

A pesquisa também revelou que a baixa taxa de denúncia e a subnotificação de crimes digitais são obstáculos para a atuação penal. Muitas vítimas desconhecem seus direitos ou não acreditam que o sistema jurídico será capaz de oferecer proteção efetiva. Vieira (2023) destaca que o acesso à justiça digital precisa ser democratizado e desburocratizado.

Quanto ao significado das descobertas, fica claro que a norma penal, sozinha, não é suficiente para garantir a segurança cibernética. É necessário integrar as ações legislativas com medidas administrativas, educacionais e tecnológicas. Sanches (2018) afirma que a eficácia do Direito Penal se amplia quando há atuação conjunta entre os Poderes e a sociedade civil.

Alguns resultados inesperados também surgiram, como a constatação de que, em certas regiões, os crimes cibernéticos ainda são tratados como delitos de menor relevância, o que compromete sua apuração. Araújo (2021) adverte que o preconceito institucional contra temas digitais precisa ser superado com formação técnica e humanização do atendimento às vítimas.

As descobertas aqui discutidas reafirmam a importância de se investir na formação técnica dos operadores do Direito, no fortalecimento das estruturas institucionais e na produção contínua de conhecimento sobre o tema. Castro (2021) propõe que universidades e centros de pesquisa atuem como aliados estratégicos na formulação de políticas públicas para o enfrentamento da criminalidade digital. Essa colaboração entre o meio acadêmico e o poder público pode ser decisiva para desenvolver soluções sustentáveis e eficazes, capazes de acompanhar a velocidade das transformações tecnológicas e proteger os direitos fundamentais no ambiente digital.

CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo principal analisar a eficácia da norma penal brasileira frente ao crescente fenômeno da criminalidade cibernética, considerando os desafios impostos pelas novas tecnologias e pela natureza transnacional dos delitos digitais. A partir de uma abordagem dedutiva, exploratória e bibliográfica, foi possível examinar criticamente o conjunto normativo vigente, bem como identificar as limitações e potencialidades do sistema penal no enfrentamento desse tipo de criminalidade.

A pesquisa demonstrou que, embora o ordenamento jurídico brasileiro tenha evoluído nas últimas décadas com a edição de leis específicas, como a Lei nº 12.737/2012, o Marco Civil da *Internet* (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e, mais recentemente, a Lei nº 14.155/2021, ainda há importantes lacunas que comprometem a

efetividade do Direito Penal na repressão aos crimes digitais. A ausência de uniformidade jurisprudencial, a carência de capacitação técnica dos operadores do direito e a limitada estrutura institucional foram fatores recorrentes apontados ao longo do estudo.

O referencial teórico analisado permitiu compreender que a eficácia da norma penal não depende exclusivamente de sua previsão legal, mas também de sua correta aplicação, interpretação uniforme e integração com outras políticas públicas. A literatura consultada revelou, de forma unânime, a importância de articular ações repressivas com medidas preventivas, como a educação digital, campanhas de conscientização e fortalecimento dos mecanismos de cooperação internacional.

Além disso, constatou-se que a criminalidade cibernética impõe desafios específicos às estruturas tradicionais do sistema penal, especialmente em razão da volatilidade das provas digitais, da dificuldade de identificação dos agentes e da complexidade técnica das condutas praticadas. A atuação repressiva, portanto, exige atualização constante da legislação, investimento em tecnologia e capacitação dos profissionais envolvidos na persecução penal.

As descobertas deste trabalho reforçam a hipótese de que, apesar dos avanços legislativos, a eficácia da norma penal ainda está aquém do necessário para enfrentar, de forma ampla e eficiente, os crimes praticados no ciberespaço. A resposta do Estado, muitas vezes, é reativa e pontual, sendo necessário desenvolver uma política penal mais integrada, preventiva e orientada para a realidade digital.

Diante do exposto, sugere-se que futuras investigações explorem o impacto da cooperação jurídica internacional na persecução de crimes cibernéticos, bem como o papel das autoridades administrativas, como a Autoridade Nacional de Proteção de Dados (ANPD), no aprimoramento das medidas de prevenção e repressão. O aprofundamento dessas temáticas poderá contribuir significativamente para o aperfeiçoamento do sistema penal brasileiro frente aos desafios do século XXI.

Dessa forma, pode se afirmar que a norma penal constitui um importante instrumento de enfrentamento à criminalidade digital, mas seu êxito depende de uma atuação coordenada, técnica e proativa por parte do Estado e da sociedade. A eficácia normativa, nesse contexto, não pode ser pensada de forma isolada, mas como resultado de uma política pública ampla, orientada pela proteção dos direitos fundamentais e pela promoção da justiça digital.

REFERÊNCIAS

ALVES, Leonardo Barreto Moreira. **Processo penal parte geral**. 14. ed. São Paulo: JusPODIVM, 2024.

ARAÚJO, Claudio Rodrigues. **Análise da aplicação do direito penal nos crimes virtuais**. Belo Horizonte: Expert, 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 20 12. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 03 set. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 set. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 ago. 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal e a Lei nº 7.492/1986 para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 17 set. 2025.

BRITTO, Gladstone Avelino; FREITAS, Maristella Barros. Ciberataques em massa e os limites do poder punitivo na tipificação de crimes informáticos. **Revista de Direito Penal, Processo Penal e Constituição**, v. 3, n. 2, p. 1–16, 2017.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2021.

CORRÊA, Isadora Donza; MONTEIRO NETO, João Araújo. A adesão do Brasil à Convenção de Budapeste e o enfrentamento do cibercrime: entre a cooperação internacional e a expansão do direito penal. **Revista Eletrônica Direito & TI**, v. 1, n. 16, p. 32–60, 2023.

CUNHA, Rogério Sanches. **Código penal para concursos**. 12. ed. Salvador: JusPODIVM, 2 019.

CRESWELL, John W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 6. e d. Porto Alegre: Penso, 2024.

DOBLER,Débora Terezinha.**Crimes cibernéticos e a proteção de dados pessoais no Brasil: desafios e perspectivas**. Curitiba: Appris, 2023.

FERREIRA, Sarah Pereira. **Crimes cibernéticos: a ineficácia da legislação brasileira**.2021. 31 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2023.

GOMES, Walyson Milhomem Souza de; MEDRADO, Lucas Cavalcante.Crimes cibernéticos: uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 9, p. 1870–1894, 2023.

KILIAN, Jean. **Crimes cibernéticos: uma abordagem jurídica diante da eficácia na legislação brasileira**. 2020. 65 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2020.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 9. ed. São Paulo: Atlas, 2020.

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes cibernéticos: considerações sobre a criminalidade na Internet**. **Âmbito Jurídico**, 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/. Acesso em: 6 mai. 2025.

NASCIMENTO, Cláudia Rufino do; SOUZA, Maria; LIMA, Pedro. Crimes Cibernéticos à Luz Da Lei 12.737/2012: Avanços e Retrocessos. **Revista de Trabalhos Acadêmicos – Universo Recife**, v. 4, n. 2, 2017. Disponível em: https://ri.ucsal.br/bitstreams/c08c600f-2a5e-413f-8e15-45cfa56959aa/download. Acesso em: 10 de maio 2025.

RAMOS, Eduardo Dulcetti. **Crimes cibernéticos: análise evolutiva e legislação penal brasileira**. 2017. 64 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017. Disponível em: https://pantheon.ufrj.br/handle/11422/6911. Acesso em: 29 set. 2025.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso. **Os crimes cibernéticos e o direito à segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo**. In: IV Congresso Internacional de Direito e Contemporaneidade**,** Santa Maria, RS, 2017.

SANCHES, Ademir Gasques. A insuficiência das leis em relação aos crimes cibernéticos no Brasil. **Revista Jus Navigandi**, Teresina, maio 2018.
Disponível em: https://jus.com.br/artigos/66527. Acesso em: 22 set. 2025.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 27. ed. São Paulo: Cortez, 2018.

SILVA, Matheus Giboski Moreira da. **A Convenção de Budapeste e a cooperação jurídica internacional como ferramentas essenciais na repressão aos crimes cibernéticos no Brasil.** 2022. 84 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2022.

VIEIRA, Edinilson Santos. **Crimes cibernéticos**. São Paulo: Viseu, 2023.