RGe
ISSN: 2177-3246

A EFICÁCIA DA LEGISLAÇÃO PENAL BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS

THE EFFECTIVENESS OF BRAZILIAN CRIMINAL LAW IN COMBATING CYBERCRIMES

LA EFICACIA DEL DERECHO PENAL BRASILEÑO EN LA LUCHA CONTRA LOS CIBERDELITOS

10.56238/revgeov17n4-173

Gustavo Almeida Silva
Graduando em Direito
Instituição: Unidade de Ensino Superior do Sul do Maranhão (UNISULMA)
E-mail: g.almeida17@icloud.com

Arisson Carneiro Franco
Professor orientador
Mestre em Direito
Instituição: Centro Universitário do Distrito Federal (UDF)
E-mail: arisson.franco@hotmail.com

RESUMO
O presente estudo analisa a eficácia do ordenamento jurídico brasileiro no enfrentamento aos crimes cibernéticos, diante do avanço exponencial das inovações tecnológicas e da sofisticação das práticas delitivas. A pergunta central que orienta a pesquisa é: em que medida a legislação penal brasileira é eficaz no combate aos crimes cibernéticos? A hipótese sustentada é a de que, embora o Brasil tenha consolidado um arcabouço jurídico relevante, as normas vigentes ainda são insuficientes para acompanhar a velocidade e a sofisticação dos delitos digitais. O objetivo geral é avaliar a efetividade das leis penais brasileiras, identificando avanços, lacunas normativas e os desafios práticos da persecução penal no ambiente digital. Por meio de pesquisa bibliográfica e documental, com abordagem qualitativa e exploratória, foram examinados marcos legais fundamentais, como a Lei n.º 12.737/2012 (Lei Carolina Dieckmann), o Marco Civil da Internet (Lei n.º 12.965/2014), a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), a Lei n.º 14.155/2021 e o Decreto n.º 11.419/2023, que promulgou a Convenção de Budapeste. A análise demonstra que, embora o Brasil tenha avançado na regulamentação do espaço digital, subsistem lacunas normativas relevantes, especialmente diante de condutas praticadas com inteligência artificial, deepfakes e técnicas sofisticadas de anonimato. Os resultados apontam que a complexidade da prova digital, a volatilidade dos vestígios eletrônicos e as dificuldades de identificação de autoria constituem os principais entraves à responsabilização criminal. Conclui-se pela necessidade urgente de reforma penal estrutural, investimento em capacitação técnico-pericial e fortalecimento da cooperação internacional para reduzir a impunidade no ciberespaço.

Palavras-chave: Crimes Cibernéticos. Direito Digital. Prova Eletrônica.

ABSTRACT
This study analyzes the effectiveness of the Brazilian legal system in combating cybercrimes, given the exponential advancement of technological innovations and the increasing sophistication of criminal practices. The central research question is: to what extent is Brazilian criminal legislation effective in combating cybercrimes? The hypothesis is that, although Brazil has consolidated an important legal framework, existing norms are still insufficient to keep pace with the speed and sophistication of digital offenses. Through bibliographic and documentary research with a qualitative and exploratory approach, fundamental legal milestones were examined, such as Law No. 12,737/2012 (Carolina Dieckmann Law), the Brazilian Internet Bill of Rights (Law No. 12,965/2014), the General Data Protection Law (Law No. 13,709/2018), Law No. 14,155/2021, and Decree No. 11,419/2023, which enacted the Budapest Convention. The analysis reveals persistent normative gaps, particularly regarding conduct carried out using artificial intelligence, deepfakes, and advanced anonymity techniques. The results indicate that the complexity of digital evidence, the volatility of electronic traces, and difficulties in identifying authorship are the main obstacles to criminal prosecution. The conclusion points to the urgent need for structural criminal reform, investment in forensic technical expertise, and strengthened international cooperation to reduce impunity in cyberspace.

Keywords: Cybercrimes. Brazilian Criminal Law. Digital Security. Digital Law. Electronic Evidence.

RESUMEN
Este estudio analiza la eficacia del sistema jurídico brasileño en la lucha contra los ciberdelitos, considerando el avance exponencial de las innovaciones tecnológicas y la sofisticación de las prácticas delictivas. La pregunta central que guía la investigación es: ¿hasta qué punto es eficaz el derecho penal brasileño en la lucha contra los ciberdelitos? La hipótesis es que, si bien Brasil ha consolidado un marco jurídico pertinente, las normas vigentes aún resultan insuficientes para seguir el ritmo y la sofisticación de los delitos digitales. El objetivo general es evaluar la eficacia del derecho penal brasileño, identificando los avances, las deficiencias normativas y los desafíos prácticos de la persecución penal en el entorno digital. Mediante investigación bibliográfica y documental, con un enfoque cualitativo y exploratorio, se examinaron marcos jurídicos fundamentales, como la Ley N° 12.737/2012 (Ley Carolina Dieckmann), la Carta Brasileña de Derechos de Internet (Ley N° 12.965/2014), la Ley General de Protección de Datos (Ley N° 13.709/2018), la Ley N° 14.155/2021 y el Decreto N° 11.419/2023, que promulgó el Convenio de Budapest. El análisis demuestra que, si bien Brasil ha avanzado en la regulación del espacio digital, persisten importantes lagunas normativas, especialmente ante conductas realizadas con inteligencia artificial, deepfakes y sofisticadas técnicas de anonimato. Los resultados indican que la complejidad de la evidencia digital, la volatilidad de las huellas electrónicas y las dificultades para identificar la autoría constituyen los principales obstáculos para la rendición de cuentas penal. Se concluye que existe una necesidad urgente de reforma penal estructural, inversión en formación técnica y especializada, y fortalecimiento de la cooperación internacional para reducir la impunidad en el ciberespacio.

Palabras clave: Delitos Cibernéticos. Derecho Digital. Prueba Electrónica.

1 INTRODUÇÃO

A crescente digitalização das relações sociais, econômicas e jurídicas transformou profundamente o cotidiano das sociedades contemporâneas, abrindo espaço para a emergência de novas modalidades criminosas que desafiam os limites tradicionais do Direito Penal.

Os crimes cibernéticos, praticados com o auxílio de dispositivos informáticos e redes de comunicação, tornaram-se uma das principais ameaças à segurança jurídica, à privacidade e ao patrimônio de indivíduos, empresas e instituições públicas no Brasil e no mundo. Fenômenos como fraudes eletrônicas, ataques de *ransomware,* invasão de dispositivos, roubo de dados e estelionato virtual revelam não apenas a sofisticação dos agentes criminosos, mas também as limitações estruturais do ordenamento jurídico na resposta a tais condutas.

A expansão tecnológica, embora tenha proporcionado inegáveis benefícios à sociedade, como a facilitação do comércio eletrônico, a comunicação instantânea e a digitalização de serviços públicos e privados, também criou um ambiente propício ao surgimento de condutas ilícitas de elevada complexidade técnica.

A internet, ao possibilitar o anonimato, a transnacionalidade e a velocidade de ação, representa um desafio singular para os sistemas de investigação criminal e para a produção probatória, exigindo resposta normativa e operacional igualmente especializada.

Diante desse contexto, emerge o problema central que orienta a presente pesquisa: em que medida a legislação penal brasileira é eficaz no combate aos crimes cibernéticos? A hipótese sustentada é a de que, embora o Brasil tenha avançado significativamente na edificação de um arcabouço normativo voltado à tutela penal do ambiente digital, especialmente com a Lei n.º 12.737/2012, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a adesão à Convenção de Budapeste, as normas vigentes ainda são insuficientes para enfrentar a rapidez e a sofisticação com que os crimes cibernéticos evoluem, resultando em lacunas normativas, dificuldades probatórias e elevada impunidade.

O objetivo geral deste artigo é avaliar a efetividade das leis penais brasileiras no combate aos delitos cibernéticos, identificando os principais avanços normativos, as lacunas existentes e os desafios práticos enfrentados na investigação e responsabilização criminal. Para tanto, elencam-se os seguintes objetivos específicos: (a) analisar a evolução histórica e normativa do Direito Penal Digital no Brasil, com ênfase nos principais marcos legislativos; (b) examinar os conceitos doutrinários de crime cibernético e sua tipificação no ordenamento jurídico pátrio e (c) estudar as principais lacunas normativas e os obstáculos processuais que comprometem a eficácia da persecução penal no ambiente digital.

A justificativa para a realização deste estudo decorre tanto da relevância social do tema quanto de sua urgência jurídica. Dados do Centro de Estudos, Resposta e Tratamento de Incidentes de

Segurança no Brasil (CERT.br) apontam para um crescimento exponencial de incidentes cibernéticos nos últimos anos, cenário que expõe a insuficiência das respostas institucionais e normativas disponíveis. Do ponto de vista acadêmico, a pesquisa contribui para o aprofundamento do debate jurídico sobre o Direito Penal Digital, um campo em constante expansão e ainda carente de sistematização doutrinária no Brasil. Do ponto de vista prático, pretende oferecer subsídios para a formulação de políticas legislativas e investigativas mais eficientes, em consonância com os padrões internacionais de combate ao cibercrime.

Quanto à metodologia, a presente pesquisa é de natureza qualitativa e exploratória, desenvolvida por meio de revisão bibliográfica e documental. Foram consultadas fontes primárias, legislação nacional e internacional, jurisprudência do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF), além de tratados internacionais e fontes secundárias, como doutrina especializada em Direito Penal, Direito Digital e segurança da informação, artigos científicos indexados nas plataformas CAPES e Google Acadêmico, dissertações e monografias. A análise foi realizada de forma sistemática e crítica, visando não apenas descrever o arcabouço normativo existente, mas também identificar suas insuficiências e propor perspectivas de aperfeiçoamento.

2 A EVOLUÇÃO DA INTERNET E O SURGIMENTO DA CRIMINALIDADE NO AMBIENTE DIGITAL

Para compreender a dimensão do fenômeno criminoso no ambiente digital, é indispensável analisar o processo histórico de desenvolvimento da internet e a forma como sua expansão criou as condições propícias ao surgimento de novas modalidades delitivas.

O ponto de partida dessa trajetória remonta à Guerra Fria e ao interesse militar norte-americano no desenvolvimento de sistemas de comunicação descentralizados e resistentes a ataques. A partir do lançamento do satélite soviético Sputnik, em outubro de 1957, os Estados Unidos estimularam a criação da ARPANET, rede precursora da internet, cuja finalidade era garantir a comunicação entre centros estratégicos mesmo após um eventual ataque nuclear (Corrêa; Monteiro Neto, 2023).

A Agência de Projetos de Pesquisa Avançada (ARPA) desenvolveu a infraestrutura que permitia o compartilhamento de arquivos e a comunicação entre computadores geograficamente distantes. Em 1969, foi estabelecida a primeira conexão entre a Universidade da Califórnia e o Instituto de Pesquisa de Stanford, marco inaugural da comunicação em rede (Barreto; Silva, 2022). Ao longo das décadas seguintes, a rede expandiu-se progressivamente do ambiente militar para os centros acadêmicos e, na década de 1990, para o uso comercial e doméstico, com o surgimento de navegadores como o Internet Explorer, Mozilla Firefox e Google Chrome, que tornaram a internet acessível ao grande público.

No Brasil, as primeiras conexões à internet ocorreram nos anos 1980, restritas inicialmente ao Laboratório Nacional de Computação Científica (LNCC) e a universidades públicas. Em meados de

1994, a EMBRATEL iniciou a distribuição de acesso experimental, e em 1995 o serviço foi liberado comercialmente, impulsionando o crescimento exponencial de usuários e, consequentemente, das atividades realizadas no ambiente digital. Em 1996, a internet já estava amplamente difundida na sociedade brasileira, alterando de forma substancial os padrões de comunicação, consumo e relações sociais.

Esse processo de digitalização acelerada, todavia, não foi acompanhado por respostas normativas adequadas. Como observam Barreto e Silva (2022), a evolução tecnológica criou um ambiente fértil para a prática criminosa em rede, ao passo que o ordenamento jurídico permaneceu estruturado em bases concebidas para a criminalidade convencional, centrada na materialidade física dos bens jurídicos tutelados. Essa defasagem entre inovação tecnológica e resposta normativa constitui o núcleo do problema analisado neste estudo.

2.1 CONCEITO E CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A definição de crime cibernético não é unívoca na doutrina, reflexo da própria pluralidade de condutas que o fenômeno abrange. Em sentido amplo, pode-se compreendê-lo como toda atividade criminosa na qual o computador, a rede de computadores ou um dispositivo conectado é utilizado como instrumento ou alvo da conduta delitiva.

Para Roque (2007, p. 33), crimes de informática são "todas as condutas, definidas pela lei como crime, em que o computador é utilizado como instrumento de sua perpetração". Ferreira (2005) amplia essa perspectiva ao identificar, além das condutas tradicionais praticadas por meio digital, novas condutas típicas do ambiente cibernético, sem correspondência nos delitos convencionais, como a invasão de sistemas e a interceptação ilegal de dados.

A doutrina especializada costuma classificar os crimes cibernéticos em duas grandes categorias. Os crimes cibernéticos próprios são aqueles em que o sistema informático constitui tanto o meio quanto o objeto da conduta, como a invasão de dispositivo informático e o ataque a infraestruturas digitais. Já os crimes cibernéticos impróprios correspondem a delitos já tipificados no ordenamento penal tradicional, como o estelionato, a calúnia e a injúria, praticados com o auxílio de meios eletrônicos. Essa distinção é relevante para a análise das lacunas normativas, pois a ausência de tipos penais específicos para condutas próprias do ciberespaço representa uma das fragilidades centrais da legislação brasileira (Daoun, 2001).

Conforme aponta Castro (2003), a internet tornou-se o principal meio de cometimento de delitos informáticos, não apenas pela capilaridade de seu alcance, mas também pela possibilidade de atuação anônima, transnacional e de baixo custo para o criminoso. Condutas como fraudes eletrônicas, roubo de identidade, ataques de *ransomware, phishing, cyberbullying* e disseminação de desinformação, para citar apenas algumas das modalidades mais recorrentes, exigem respostas

normativas específicas que o Código Penal de 1940, elaborado em um contexto de total ausência de tecnologia digital, não tem condições de oferecer de forma satisfatória.

2.2 A EVOLUÇÃO NORMATIVA DOS CRIMES CIBERNÉTICOS NO BRASIL E SUAS LIMITAÇÕES

A evolução normativa brasileira em matéria de crimes cibernéticos caracterizou-se, historicamente, por um caráter reativo: as leis foram editadas em resposta a episódios de grande repercussão pública, sem que houvesse um planejamento legislativo sistemático voltado à tutela do ambiente digital. Esse padrão resultou em uma regulação fragmentada, com lacunas significativas que comprometem a eficácia da persecução penal.

A Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, representou o primeiro grande marco normativo na tipificação dos crimes cibernéticos próprios no Brasil. A norma inseriu o art. 154-A no Código Penal, criminalizando a invasão de dispositivo informático alheio. No entanto, a doutrina identificou desde sua promulgação uma limitação estrutural relevante: a exigência, em sua redação original, de que a invasão fosse praticada mediante violação de "mecanismo de segurança", o que excluía da proteção penal os dispositivos desprovidos de medidas de segurança ou com proteções insuficientes (Corrêa; Monteiro Neto, 2023). Tal lacuna somente foi parcialmente sanada pela Lei n.º 14.155/2021.

A Lei n.º 12.965/2014, denominada Marco Civil da Internet, representou avanço qualitativo na regulação do espaço digital brasileiro. Inspirada em princípios de direitos humanos aplicados ao ambiente online, a norma estabeleceu a neutralidade da rede, a liberdade de expressão, a proteção de dados pessoais e as regras de guarda e disponibilização de registros de conexão e acesso a aplicações, fundamentais para a viabilização de investigações criminais mediante ordem judicial (Barreto; Silva, 2022). Embora seu caráter seja predominantemente civil, a Lei n.º 12.965/2014 impactou diretamente a persecução penal ao disciplinar as obrigações dos provedores de conexão e de aplicações na cooperação com autoridades.

A Lei n.º 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), inspirada no Regulamento Geral de Proteção de Dados europeu (GDPR), estabeleceu um regime abrangente de proteção de dados pessoais no Brasil. Embora sua natureza seja predominantemente civil e administrativa, a LGPD impacta a esfera penal ao definir o conceito de dados pessoais sensíveis e os limites de sua coleta, tratamento e compartilhamento, influenciando diretamente as condições de obtenção de provas em investigações criminais que envolvam dados de usuários (Corrêa; Monteiro Neto, 2023).

A Lei n.º 14.155/2021 representou um endurecimento necessário das penas para crimes de furto mediante fraude eletrônica e estelionato virtual, modalidades que haviam se tornado endêmicas no contexto da pandemia de COVID-19 e da acelerada digitalização dos serviços bancários. A norma

também corrigiu parcialmente a lacuna da Lei Carolina Dieckmann, excluindo a exigência de violação de mecanismo de segurança para a configuração do delito de invasão de dispositivo informático, ampliando o alcance da tutela penal (Barreto; Silva, 2022).

O marco mais recente e estratégico da legislação brasileira sobre crimes cibernéticos é o Decreto n.º 11.419/2023, que promulgou a Convenção de Budapeste sobre o Crime Cibernético. Trata-se do principal tratado internacional em matéria de cibercrime, ao qual o Brasil aderiu após longo processo de aprovação parlamentar. A Convenção harmoniza a legislação nacional com padrões globais, facilita a obtenção de provas em servidores localizados em países signatários e fortalece os mecanismos de cooperação jurídica internacional para a extradição e a assistência mútua em investigações transnacionais (Corrêa; Monteiro Neto, 2023).

Mais recentemente, a Lei n.º 14.811/2024 instituiu medidas de proteção à convivência escolar, tipificando o crime de intimidação sistemática (bullying e cyberbullying) no Código Penal, com agravantes quando praticado por meio de redes sociais ou plataformas de jogos online, ampliando a proteção penal a vítimas em contextos digitais de especial vulnerabilidade (Brasil, 2024).

3 ANÁLISE CRÍTICA DA EFICÁCIA DA LEGISLAÇÃO PENAL BRASILEIRA

A avaliação da eficácia da legislação penal brasileira no combate aos crimes cibernéticos exige que se vá além da mera descrição normativa, adentrando a análise de sua aplicabilidade prática, de suas limitações estruturais e dos efeitos concretos sobre a persecução penal. Essa perspectiva crítica é indispensável para identificar os pontos de ruptura entre a norma e a realidade, contribuindo para a formulação de propostas de aperfeiçoamento legislativo e institucional.

3.1 LACUNAS NORMATIVAS E DEFASAGEM DO CÓDIGO PENAL

A principal limitação estrutural da legislação penal brasileira em matéria digital reside na defasagem conceitual do Código Penal de 1940, elaborado em um contexto histórico de total ausência de tecnologia informática. Os tipos penais tradicionais foram concebidos a partir de conceitos de materialidade física, bens corpóreos, documentos em papel, espaços físicos — que dificultam, e por vezes inviabilizam, a subsunção de condutas praticadas no ambiente digital, especialmente aquelas que envolvem ativos imateriais como criptoativos, dados digitais e identidades virtuais (Silva, 2025).

A Lei n.º 14.155/2021, embora tenha representado avanço ao agravar as penas para o estelionato e o furto eletrônicos, não criou um tipo penal autônomo para o "furto eletrônico", mantendo a necessidade de enquadramento das condutas nos tipos do Código Penal mediante interpretação analógica. Essa situação gera oscilação jurisprudencial sobre o enquadramento correto das condutas e, consequentemente, insegurança jurídica para operadores do Direito e jurisdicionados (Silva, 2025).

Novos delitos que se valem de inteligência artificial, como a geração de *deepfakes* para fraudes e extorsões e de técnicas avançadas de anonimato em redes criptografadas frequentemente não encontram correspondência nos tipos penais vigentes, resultando em zonas de atipicidade que comprometem a resposta estatal.

Kunrath (2017) aponta a existência de posições doutrinárias divergentes sobre a suficiência do arcabouço normativo: enquanto parte da doutrina sustenta que as Leis n.º 12.735/2012 e n.º 12.737/2012 preencheram as lacunas mais relevantes, outra corrente entende que a tipificação criminal vigente deixa fora do alcance da lei penal importantes categorias de ataques cibernéticos.

Ferreira (2010) observa que, em linhas gerais, o Brasil já dispõe de arcabouço normativo razoavelmente compatível com as diretrizes da Convenção de Budapeste, o que viabilizaria a persecução penal. Todavia, a mera existência formal da norma não garante sua efetividade, que depende igualmente da capacidade investigativa do Estado e da adequação dos instrumentos processuais.

3.2 COMPLEXIDADE DA PROVA DIGITAL E DESAFIOS PROCESSUAIS

A eficácia da norma penal no combate ao cibercrime depende não apenas da qualidade da tipificação, mas também da capacidade do Estado de produzir prova válida e suficiente para sustentar a condenação em juízo. Nesse ponto, a realidade brasileira apresenta deficiências críticas. A natureza volátil das provas eletrônicas, facilmente alteradas, destruídas ou ocultadas exige uma cadeia de custódia rigorosa, disciplinada pelo art. 158-A do Código de Processo Penal, introduzido pela Lei n.º 13.964/2019 (Pacote Anticrime).

A jurisprudência do Superior Tribunal de Justiça ilustra de forma contundente os riscos decorrentes da inobservância das regras de cadeia de custódia digital. No julgamento do HC 828.054, a Quinta Turma do STJ, sob a relatoria do Min. Joel Ilan Paciornik (2024), reconheceu a ilicitude de prova obtida por meio de prints de conversas de WhatsApp colhidos sem a adoção de metodologia técnica adequada, determinando a anulação da condenação. Esse precedente evidencia um paradoxo central: a lei tipifica a conduta, mas o Estado frequentemente falha na produção da prova válida necessária para sustentar a punição, resultando em impunidade não por ausência de norma, mas por déficit de capacidade técnica e processual.

Agrava essa realidade a sofisticação crescente dos criminosos digitais, que se valem de criptografia de ponta a ponta, redes de anonimato como o Tor e servidores localizados em jurisdições com baixa cooperação internacional, tornando extremamente difícil a identificação da autoria e a obtenção de provas admissíveis. A volatilidade dos vestígios eletrônicos, aliada à dificuldade de acesso a dados armazenados por provedores estrangeiros, representa um dos maiores entraves à persecução penal eficaz no ambiente digital (Rocha et al., 2025).

3.3 TENSÃO ENTRE PRIVACIDADE E SEGURANÇA PÚBLICA

A tutela da privacidade individual e a necessidade de acesso a dados para fins de investigação criminal constituem polos em tensão permanente no ordenamento jurídico brasileiro. A LGPD, ao estabelecer restrições rigorosas ao tratamento de dados pessoais, cria obstáculos ao acesso célere a informações essenciais em investigações de urgência, gerando conflito normativo entre a proteção do direito individual à privacidade e o interesse público na segurança e na persecução penal (Brasil, 2019).

O Marco Civil da Internet, embora disciplinando a guarda obrigatória de registros de conexão e acesso a aplicações, subordina o fornecimento dessas informações à ordem judicial, o que, em situações de urgência investigativa, pode implicar perda irreversível de vestígios. Essa tensão revela a necessidade de construção de marcos normativos que harmonizem, de forma proporcional e fundamentada, a proteção à privacidade com as exigências da segurança pública no ambiente digital, sem que nenhum dos dois valores seja sacrificado em favor do outro.

3.4 INSUFICIÊNCIA ESTRUTURAL DAS INSTITUIÇÕES DE PERSECUÇÃO PENAL

A eficácia normativa depende, em última análise, da capacidade institucional do Estado de investigar, reunir provas, processar e julgar os agentes criminosos. Nesse aspecto, a realidade brasileira apresenta déficits expressivos. Embora existam delegacias especializadas em crimes cibernéticos em alguns estados da federação, a distribuição geográfica dessas unidades é desigual, e os recursos humanos e tecnológicos disponíveis são, em geral, insuficientes para fazer frente ao volume e à complexidade dos delitos digitais (Souza; Lima, 2022).

Souza e Lima (2022) enfatizam que a eficácia da lei penal depende diretamente da existência de policiais, peritos e magistrados com profundo conhecimento técnico em forense digital, criptografia e análise de redes. A carência de profissionais especializados compromete não apenas a qualidade das investigações, mas também a produção de laudos periciais capazes de resistir ao contraditório judicial. O investimento em ferramentas de forense digital, na criação de núcleos especializados em cibercrimes e na formação continuada de operadores do Direito configura, portanto, condição necessária, ainda que não suficiente para a efetividade da tutela penal no ciberespaço.

Além disso, a morosidade do Poder Judiciário, combinada com a celeridade característica dos crimes digitais, amplifica o risco de perecimento de provas e de prescrição das pretensões punitivas, revelando que o problema da ineficácia não é exclusivamente normativo, mas também estrutural e institucional.

4 PERSPECTIVAS DE APERFEIÇOAMENTO LEGISLATIVO E INSTITUCIONAL

Diante das lacunas e insuficiências identificadas, a literatura especializada aponta caminhos concretos para o aperfeiçoamento da tutela penal no ambiente digital. Essas perspectivas envolvem

reformas normativas, investimentos institucionais e o fortalecimento da cooperação nacional e internacional.

No plano normativo, Jesus e Milagres (2016) propugnam uma reforma estrutural do Código Penal que migre do foco na ferramenta tecnológica para o foco na conduta e no bem jurídico tutelado. Normas mais flexíveis e perenes, que permitam a subsunção de condutas praticadas por meio de inteligência artificial ou em ambientes de realidade virtual, mostram-se mais adequadas ao ritmo da inovação tecnológica do que a edição de tipos penais específicos para cada nova ferramenta estratégia normativa que inevitavelmente resulta em defasagem.

No plano probatório, sugere-se a adoção de tecnologias de blockchain para o registro e validação da cadeia de custódia de provas digitais, garantindo a integridade do material coletado desde a fase investigativa até o julgamento. Essa solução tecnológica, já adotada em experiências internacionais, confere maior segurança e credibilidade às provas eletrônicas em juízo (Juvêncio, 2023).

No plano institucional, o fortalecimento das delegacias especializadas em crimes cibernéticos, com dotação orçamentária adequada e programas permanentes de capacitação técnica, é condição essencial para a efetividade da persecução penal. O investimento em ferramentas de forense digital de última geração e na formação de peritos com elevado nível de especialização técnica deve ser tratado como política pública prioritária (Souza; Lima, 2022).

No plano da cooperação internacional, a plena implementação dos mecanismos previstos na Convenção de Budapeste especialmente os acordos de assistência jurídica mútua, é fundamental para superar a barreira da extraterritorialidade e viabilizar o acesso a dados armazenados em servidores localizados fora do território nacional. Colli (2010) aponta que a cooperação internacional representa um dos pilares insubstituíveis de qualquer estratégia eficaz de combate ao cibercrime, dado o caráter intrinsecamente transnacional da maior parte dessas condutas.

Por fim, o combate ao cibercrime não deve ser concebido apenas como resposta punitiva. A prevenção, por meio de programas de letramento digital para a população, fomento ao compliance digital nas empresas e campanhas de conscientização sobre segurança da informação, reduz a vulnerabilidade do sistema como um todo, diminuindo a exposição de potenciais vítimas e restringindo as oportunidades de atuação criminosa (Juvêncio, 2023).

5 CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar a eficácia da legislação penal brasileira no combate aos crimes cibernéticos, respondendo à pergunta central que o orientou: em que medida o ordenamento jurídico pátrio é eficaz na contenção e responsabilização dos delitos praticados no ambiente digital? A análise empreendida permite afirmar que a hipótese inicial se confirmou: o Brasil

avançou de forma significativa na construção de um arcabouço normativo voltado ao Direito Penal Digital, mas a legislação vigente ainda é insuficiente para enfrentar a velocidade e a sofisticação com que os crimes cibernéticos evoluem.

No que se refere aos principais marcos legais, observou-se que a proteção penal do ambiente digital foi construída de maneira reativa e progressiva. A Lei n.º 12.737/2012 inaugurou a tipificação específica das invasões informáticas; o Marco Civil da Internet estabeleceu os princípios fundamentais da governança digital e as obrigações dos provedores; a LGPD regulamentou o tratamento de dados pessoais; a Lei n.º 14.155/2021 agravou as penas para delitos patrimoniais eletrônicos; e o Decreto n.º 11.419/2023 inseriu o Brasil no sistema global de cooperação em matéria de cibercrime por meio da Convenção de Budapeste.

No entanto, a pesquisa identificou lacunas normativas relevantes que comprometem a eficácia da tutela penal. A defasagem conceitual do Código Penal de 1940, estruturado em torno de conceitos de materialidade física incompatíveis com a desmaterialização dos ativos digitais, resulta em zonas de atipicidade para condutas praticadas com tecnologias emergentes, como a inteligência artificial e os *deepfakes*. A ausência de tipos penais autônomos para determinadas modalidades delitivas e a oscilação jurisprudencial sobre o enquadramento correto das condutas geram insegurança jurídica e favorecem a impunidade.

A análise dos desafios processuais revelou que a ineficácia não é exclusivamente normativa: a volatilidade das provas digitais, as dificuldades de manutenção de cadeia de custódia adequada e a insuficiência técnica das instituições de persecução penal constituem obstáculos igualmente relevantes. O precedente do STJ no HC 828.054 (2024) ilustra com clareza que a ausência de metodologia técnica adequada na coleta de provas eletrônicas pode inviabilizar condenações, independentemente da suficiência normativa.

Diante do exposto, conclui-se que o enfrentamento eficaz dos crimes cibernéticos no Brasil demanda uma abordagem multidimensional, que integre a atualização e o aperfeiçoamento normativo, o investimento em capacitação técnica e infraestrutura de persecução penal, o fortalecimento da cooperação internacional e a adoção de políticas preventivas de educação digital. Mais do que legislar sobre ferramentas tecnológicas específicas estratégia fadada à obsolescência, o Estado deve desenvolver normas perenes que protejam os bens jurídicos essenciais ameaçados no ciberespaço a privacidade, o patrimônio, a honra e a dignidade humana independentemente da forma tecnológica que a conduta criminosa venha a assumir.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves; SILVA, Marllon. Crimes cibernéticos: investigação, persecução e prova. 3. ed. Rio de Janeiro: Brasport, 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 10 mar. 2025.

BRASIL. Decreto-lei n.º 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 — Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 14.155, de 27 de maio de 2021. Torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 14.811, de 12 de janeiro de 2024. Institui medidas de proteção à convivência nas comunidades escolares. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/L14811.htm>. Acesso em: 10 mar. 2025.

BRASIL. Decreto n.º 11.419, de 17 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético (Convenção de Budapeste). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11419.htm>. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus n.º 828.054. Rel. Min. Joel Ilan Paciornik. Quinta Turma. Julgado em 2024.

CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

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, Porto Alegre, v. 1, n. 16, p. 32-60, maio/ago. 2023. DOI: 10.63451/ti.v1i16.155. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/view/155>. Acesso em: 10 mar. 2025.

DAOUN, Alexandre Jean. Cybercrimes. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Coord.). Manual de Direito Eletrônico e Internet. São Paulo: Lex, 2001.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). Direito & Internet: aspectos jurídicos relevantes. Bauru: EDIPRO, 2010.

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008.

JESUS, Damásio de; MILAGRES, José Antônio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

JUVÊNCIO, Tiago. Crimes cibernéticos em 2026: o novo campo de batalha do Direito Penal. [S.l.]: [s.n.], 2023.

KUNRATH, Schirley. Crimes virtuais: aspectos legais e lacunas normativas. Revista Direito e Liberdade, Natal, v. 19, n. 2, 2017.

ROCHA, Veronica Alkmim et al. As (in)eficiências comprobatórias da legislação brasileira e os desafios da persecução penal nos crimes de invasão de dispositivos informáticos. New Science, São Paulo, 2025.

RODRIGUES, Vanessa Costa; FERREIRA, Rafaela Oliveira da Costa. A eficácia da legislação brasileira no combate aos crimes cibernéticos. Revista FT, ed. 151, 2025.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP, 2007.

SILVA, Gabriellen Oliveira da. A fragilidade da legislação penal frente aos crimes de furto em bancos digitais: uma análise das lacunas normativas e da ausência de regulamentação específica para crimes digitais no sistema penal brasileiro. 2025. 35 f. Monografia (Graduação em Direito) — Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás, Goiânia, 2025.

SOUZA, Renata; LIMA, Fábio. Cibersegurança e Direito Penal: desafios da capacitação institucional no Brasil. Revista Brasileira de Direito Digital, v. 4, n. 2, 2022.