

DESAFIOS NA PREVENÇÃO E REPRESSÃO DOS CRIMES DIGITAIS: UMA ANÁLISE JURÍDICO-NORMATIVA DA LEGISLAÇÃO BRASILEIRA

CHALLENGES IN THE PREVENTION AND REPRESSION OF CYBERCRIMES:
A LEGAL-NORMATIVE ANALYSIS OF BRAZILIAN LEGISLATION

Ciências Sociais Aplicadas • 23/10/2026

REGISTRO DOI: [10.70773/revistatopicos/792643030](https://doi.org/10.70773/revistatopicos/792643030)

Jhefeson Silva Rocha¹

Andressa Costenaro de Alencar²

RESUMO

Este estudo analisa os alcances e as limitações jurídicas dos instrumentos normativos brasileiros de prevenção e repressão aos crimes digitais, fenômeno que cresce na mesma proporção em que a sociedade se torna dependente das tecnologias da informação. Por meio de pesquisa bibliográfica e documental, examinam-se os principais diplomas normativos que tratam da matéria, como a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, 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, que tornou mais graves os crimes de invasão de dispositivo informático, furto e estelionato praticados por meio eletrônico. Conclui-se que, apesar dos avanços normativos, a literatura especializada aponta obstáculos relevantes à repressão desses delitos. Entre eles estão o anonimato proporcionado pelo ambiente virtual, que dificulta a identificação da autoria, e a volatilidade da prova digital, que pode ser alterada ou apagada com facilidade. Somam-se a isso a carência de peritos e de estrutura técnica especializada nos órgãos de investigação e a cooperação internacional ainda limitada, apesar da recente adesão do Brasil à Convenção de Budapeste. Diante desse cenário, sustenta-se a necessidade de aprimoramentos legislativos e institucionais, com investimento na capacitação dos agentes públicos, na modernização dos meios de investigação e no fortalecimento dos mecanismos de cooperação entre países, a fim de garantir uma resposta estatal mais eficaz aos crimes cometidos no meio digital.

Palavras-chave: Crimes digitais; Legislação brasileira; Prevenção; Repressão penal.

ABSTRACT

This study analyzes the scope and legal limitations of Brazilian regulatory instruments for the prevention and prosecution of

cybercrime, a phenomenon that grows in step with society's increasing dependence on information technology. Through bibliographic and documentary research, it examines the main legal instruments governing the subject, such as Law No. 12,737/2012, known as the Carolina Dieckmann Law, the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014), the General Data Protection Law (Law No. 13,709/2018), and Law No. 14,155/2021, which made the crimes of unauthorized access to computer devices, theft and fraud committed by electronic means more serious. The study concludes that, despite these legislative advances, the specialized literature points to significant obstacles to the prosecution of such offenses. These include the anonymity afforded by the virtual environment, which makes it difficult to identify perpetrators, and the volatility of digital evidence, which can be easily altered or deleted. In addition, there is a shortage of forensic experts and specialized technical infrastructure within investigative bodies, as well as limited international cooperation, despite Brazil's recent accession to the Budapest Convention. In light of this scenario, the study argues for legislative and institutional improvements, including investment in training public officials, modernization of investigative tools, and stronger cooperation mechanisms between countries, in order to ensure a more effective state response to crimes committed in the digital environment.

Keywords: Digital crimes; Brazilian legislation; Prevention; Criminal repression.

1. INTRODUÇÃO

A evolução da tecnologia e a expansão do acesso à internet transformaram significativamente a forma como as pessoas se comunicam, trabalham e realizam diversas atividades do cotidiano.

O ambiente digital passou a integrar a rotina da sociedade, possibilitando avanços importantes na circulação de informações e na interação social por meio de plataformas como redes sociais e aplicativos de mensagens. Entretanto, ao lado desses benefícios, surgiram novas formas de práticas ilícitas realizadas no meio virtual, conhecidas como crimes digitais, que envolvem fraudes, invasão de dispositivos informáticos, disseminação de conteúdos ilícitos e outras condutas que desafiam a atuação do Direito.

Diante desse cenário, questiona-se: quais são os alcances e as limitações jurídicas dos instrumentos normativos brasileiros de prevenção e repressão aos crimes digitais e quais obstáculos institucionais e probatórios, segundo a literatura especializada, dificultam sua aplicação diante do avanço das tecnologias? A relevância do tema decorre da crescente inserção da sociedade no ambiente virtual e da necessidade de compreender como o Direito brasileiro tem buscado acompanhar essa transformação, identificando eventuais lacunas normativas e institucionais. O objetivo geral deste artigo é analisar os instrumentos normativos brasileiros de prevenção e repressão aos crimes digitais, identificando seus alcances e limitações jurídicas e examinando os obstáculos institucionais e probatórios apontados pela literatura especializada. Como objetivos específicos, busca-se conceituar essas infrações, identificar suas principais modalidades praticadas no Brasil, examinar a legislação aplicável e analisar os desafios enfrentados pelas autoridades na investigação e responsabilização dos autores, conforme descritos nas fontes consultadas.

Para tanto, adotou-se abordagem qualitativa e exploratória, com aplicação do método dedutivo e utilização de técnicas de pesquisa bibliográfica e documental, cujos procedimentos são detalhados em

seção própria. O artigo está estruturado, além desta introdução, em uma seção de desenvolvimento, na qual são discutidos o panorama da criminalidade informática, os desafios da prevenção e da repressão, as modalidades específicas de infrações praticadas no ambiente virtual, a disciplina da prova digital e da cadeia de custódia, o regramento do Marco Civil da Internet e da cooperação jurídica internacional e as alterações promovidas pela Lei nº 14.155/2021, seguida da seção de metodologia, dos resultados e análises, das considerações finais e das referências utilizadas.

2. O CENÁRIO DA CRIMINALIDADE INFORMÁTICA E A EVOLUÇÃO DOUTRINÁRIA

O avanço das tecnologias digitais transformou significativamente a forma como a sociedade se organiza, trazendo benefícios, mas também novos desafios, sobretudo quanto à prática de infrações no ambiente virtual. A transição da sociedade para o meio digital acarretou a migração de condutas ilícitas para o ciberespaço. Segundo Rossini (2021), a criminalidade informática não se resume à criação de novos tipos penais, mas à utilização de novos meios para atingir bens jurídicos já tutelados, o que exige do Direito uma adaptação constante, sendo a natureza transfronteiriça da rede um dos principais obstáculos à repressão.

Nessa direção, Crespo (2022) destaca que o ambiente virtual proporciona anonimato e volatilidade das provas, fatores que dificultam a atuação das autoridades policiais.

Verifica-se, nesse contexto, uma evolução legislativa gradual e reativa por parte do legislador brasileiro. A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, inaugurou a tipificação da

invasão de dispositivo informático, ao inserir o artigo 154-A no Código Penal. Poucos anos depois, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu o regramento principiológico do uso da rede no país, seguido pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que disciplinou o tratamento de dados pessoais tanto pelo poder público quanto pela iniciativa privada. Essa sucessão de diplomas legais evidencia que o ordenamento jurídico brasileiro tem respondido às demandas da criminalidade digital de maneira fragmentada e posterior ao surgimento das próprias condutas lesivas, circunstância que corrobora a hipótese de pesquisa segundo a qual a legislação, embora existente e relevante, ainda carece de instrumentos de antecipação normativa capazes de acompanhar a velocidade da inovação tecnológica.

2.1. Desafios na Prevenção: Educação Digital e Compliance

A prevenção constitui o primeiro pilar no combate às infrações virtuais e concentra-se na redução da vulnerabilidade dos sistemas e dos usuários. Para Pinheiro (2020), a LGPD não representa apenas uma obrigação legal, mas uma ferramenta preventiva essencial, pois a conscientização do usuário é a barreira mais eficaz contra crimes de engenharia social, como o phishing. Vendramini (2023) acrescenta que os protocolos de segurança cibernética devem alcançar também a esfera comportamental, de modo que a prevenção se mostra, com frequência, o caminho menos oneroso para o Estado e para o particular.

Nessa perspectiva, o artigo 6º da LGPD consagra princípios como a finalidade, a necessidade, a transparência, a segurança, a prevenção e a responsabilização e prestação de contas, que servem de parâmetro para aferir a diligência exigida dos agentes de

tratamento, públicos ou privados. Sua inobservância sujeita o agente às sanções administrativas da ANPD (art. 52) e à responsabilidade civil pelos danos causados aos titulares (arts. 42 a 45). A LGPD, contudo, não tipifica crimes: a responsabilidade penal depende da prática de conduta prevista na legislação penal, como a invasão de dispositivo informático (art. 154-A do CP) ou a fraude eletrônica (art. 171, § 2º-A, do CP), e recai sobre quem a praticou. Assim, quando terceiros usam dados vazados para cometer crimes, a falha de segurança da instituição repercute nas esferas administrativa e civil, sem torná-la automaticamente responsável pelo delito. Ainda assim, a prevenção deixa de ser mera diretriz ética e passa a integrar verdadeiro dever jurídico, cujo descumprimento gera consequências concretas para o agente de tratamento.

2.2. A Repressão Penal e os Obstáculos Investigativos

A coleta de provas deve observar procedimentos rigorosos de preservação da integridade dos vestígios digitais. Nesse contexto, a cadeia de custódia constitui aspecto relevante da investigação criminal, pois falhas na coleta, no armazenamento e na documentação dos dados podem comprometer sua confiabilidade. Essas dificuldades podem ser agravadas pela insuficiência de capacitação técnica e de recursos especializados nos órgãos responsáveis pela investigação.

No que tange à repressão, o ordenamento jurídico brasileiro avançou com diplomas como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), voltada à tipificação da invasão de dispositivos informáticos, mas a aplicação prática ainda enfrenta gargalos técnicos. Segundo Rossini (2021), a cooperação internacional constitui um dos principais

entraves, visto que muitos dados necessários à investigação estão hospedados em servidores localizados fora da jurisdição nacional.

A facilidade de disseminação de informações em redes sociais também potencializou a ocorrência de crimes contra a honra, como calúnia, difamação e injúria. Segundo Pinheiro (2020), o ambiente digital atua como catalisador de danos, pois a rapidez do compartilhamento torna a reparação quase impossível, sendo tênue a linha entre a liberdade de expressão e a violação da honra.

No que se refere aos crimes contra a honra, destaca-se o julgamento do Recurso Extraordinário nº 1.010.606/RJ (Tema 786 da repercussão geral), concluído pelo Supremo Tribunal Federal em 11 de fevereiro de 2021. Nele, fixou-se a tese de que é incompatível com a Constituição Federal a ideia de um direito ao esquecimento, ressaltando-se que eventuais excessos ou abusos no exercício da liberdade de expressão devem ser analisados caso a caso, à luz da proteção à honra, à imagem e à privacidade. Embora não trate especificamente de crimes digitais, a decisão orienta a responsabilização por conteúdos publicados na internet e exige análise casuística. Para Rossini (2021), essa orientação impõe ao operador do Direito constante ponderação, pois a mesma conduta pode configurar exercício legítimo da liberdade de expressão ou crime contra a honra, a depender das circunstâncias do caso concreto.

Outro desafio relevante é o estelionato digital, praticado por meio de engenharia social, como o phishing, em que a ausência de contato físico reduz a percepção de risco do infrator (Crespo, 2022). Vendramini (2023) defende que instituições financeiras e empresas de comércio eletrônico invistam em sistemas capazes de identificar

comportamentos atípicos antes da consumação do dano. No plano civil, a responsabilidade dessas empresas perante o consumidor é, em regra, objetiva (art. 14 do CDC). A Súmula 479 do STJ dispõe que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias” (BRASIL, 2012). Essa responsabilidade, porém, pode ser afastada diante de culpa exclusiva do consumidor ou de terceiro (art. 14, § 3º, II, do CDC) e não se confunde com a responsabilidade penal do autor da fraude. Quanto ao vazamento de dados, Pinheiro (2020) destaca que o dado pessoal é ativo estratégico cuja proteção constitui direito fundamental, ao passo que Crespo (2022) ressalta a complexidade da perícia necessária para comprovar a invasão de dispositivo informático (art. 154-A do Código Penal), sobretudo quando os servidores estão em diferentes jurisdições.

2.3. Os Limites do Aparato Estatal e a Necessidade de Aprimoramento

A eficácia do Direito Penal depende não apenas da criação de normas incriminadoras, mas da capacidade real do Estado de processar e julgar os infratores. Rossini (2021) aponta uma lacuna entre a sofisticação dos criminosos e a capacidade das instituições de repressão. Nesse contexto, a estrutura das delegacias especializadas pode não acompanhar o crescimento da demanda, cenário que favorece o que se denomina, neste trabalho, impunidade tecnológica. A expressão não é empregada como conceito doutrinário consolidado, e sim em sentido descritivo, para designar a infração digital que deixa de ser apurada ou punida por limitações técnicas, estruturais ou jurisdicionais, como a dificuldade

de identificar a autoria, de preservar a prova ou de obter dados armazenados no exterior.

Segundo Crespo (2022), a insuficiência de peritos oficiais capacitados pode comprometer a cadeia de custódia e expor a prova digital a questionamentos quanto à sua validade. Por isso, o aprimoramento do aparato estatal deve ser também estrutural, com aquisição de ferramentas de perícia computacional e formação contínua dos agentes. Vendramini (2023) acrescenta que a repressão isolada não soluciona o problema e defende a integração de sistemas de inteligência entre as esferas federal e estadual, bem como parcerias com provedores de conexão e de aplicação. Pinheiro (2020), por sua vez, sustenta que magistrados e promotores precisam de letramento digital suficiente para compreender as nuances das infrações virtuais.

No plano institucional, as Delegacias Especializadas em Crimes Cibernéticos, presentes em parte dos estados, e a atuação da Polícia Federal em investigações interestaduais e internacionais revelam esforços concretos de estruturação, cuja suficiência ainda carece de avaliação sistemática. A sociedade civil também contribui: segundo a SaferNet Brasil, a Central Nacional de Denúncias de Crimes Cibernéticos recebeu 87.689 novas denúncias únicas em 2025, crescimento de 28,4% em relação ao ano anterior, das quais 63.214 relacionadas a imagens de abuso e exploração sexual infantil (Cruz, 2026). Esses números revelam o aumento das denúncias, o que não equivale necessariamente a um crescimento proporcional dos crimes praticados, pois podem refletir também maior conscientização dos usuários e maior acesso aos canais de denúncia. Ainda assim, evidenciam a relevância do fenômeno e reforçam que o enfrentamento da criminalidade digital depende da articulação

entre Estado, iniciativa privada e sociedade civil, e não apenas da criação de novos tipos penais.

2.4. Outras Modalidades Emergentes: Crimes Contra a Dignidade Sexual e a Perseguição no Ambiente Digital

A expansão das redes sociais e dos aplicativos de mensagens também deu origem a modalidades específicas de violência praticada contra a dignidade sexual das vítimas. A Lei nº 13.718/2018 inseriu no Código Penal o artigo 218-C, que criminaliza as condutas de oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio, inclusive por meio de comunicação de massa ou sistema de informática ou telemática, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia, com pena de reclusão de um a cinco anos, se o fato não constitui crime mais grave. O § 1º do mesmo artigo prevê aumento de pena de um terço a dois terços quando o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação, hipótese que corresponde à prática popularmente conhecida como “pornografia de vingança”. Na mesma linha, a Lei nº 13.772/2018 alterou o artigo 7º, inciso II, da Lei Maria da Penha (Lei nº 11.340/2006), para incluir a violação da intimidade da mulher entre as formas de violência psicológica, e inseriu no Código Penal o artigo 216-B, que tipifica o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado.

Já a Lei nº 14.132/2021 introduziu no Código Penal o crime de perseguição, previsto no artigo 147-A, que tipifica a conduta de perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade, com pena de reclusão de seis meses a dois anos e multa. Embora o dispositivo não mencione expressamente os meios eletrônicos, a expressão “por qualquer meio” permite alcançar condutas praticadas no ambiente digital, como o monitoramento indevido de redes sociais e o envio reiterado de mensagens indesejadas. A mesma lei revogou o artigo 65 da Lei das Contravenções Penais (Decreto-Lei nº 3.688/1941), que previa a contravenção de perturbação da tranquilidade. Tais alterações demonstram a preocupação do legislador em tutelar a integridade psicológica e a liberdade das vítimas também no ambiente digital, ampliando os instrumentos de proteção penal aplicáveis a comportamentos que podem ser enquadrados nos tipos penais pertinentes, conforme as circunstâncias do caso concreto.

2.5. A Cadeia de Custódia da Prova Digital e o Pacote Anticrime

A confiabilidade da prova constitui pressuposto indispensável à persecução penal, exigência que se revela ainda mais sensível no âmbito dos crimes digitais, nos quais a evidência é volátil e facilmente sujeita a alterações, cópias ou destruição. Nesse contexto, a Lei nº 13.964/2019, conhecida como Pacote Anticrime, positivou expressamente o instituto da cadeia de custódia no Código de Processo Penal, mediante a inclusão dos artigos 158-A a 158-F, os quais disciplinam o conjunto de procedimentos destinados a documentar a história cronológica do vestígio, desde o seu reconhecimento até o eventual descarte, assegurando sua

rastreabilidade, autenticidade e idoneidade probatória. No campo da prova digital, tais dispositivos assumem relevância acentuada, pois a manipulação inadequada de equipamentos eletrônicos apreendidos, a ausência de espelhamento forense (imagem pericial) do dispositivo ou a demora na formalização da apreensão podem comprometer a integridade dos dados e ensejar questionamentos judiciais quanto à validade ou ao valor probatório da prova.

Nessa linha, Crespo (2022) ressalta a importância da preservação da cadeia de custódia nos processos que envolvem crimes cibernéticos, uma vez que sua inobservância pode comprometer a confiabilidade da prova e, conforme as circunstâncias do caso, enfraquecer a sustentação da acusação, o que reforça a necessidade de capacitação técnica contínua dos peritos oficiais e de investimento permanente em ferramentas de forense computacional capazes de assegurar a autenticidade da prova desde a fase investigativa até o julgamento definitivo da causa. A inobservância dos procedimentos de cadeia de custódia deve ser examinada à luz das circunstâncias concretas da coleta e da preservação do vestígio, especialmente quanto à possibilidade de verificar sua autenticidade e integridade. Por isso, a existência de irregularidade não deve ser equiparada, de forma automática, à inadmissibilidade da prova, sendo necessário avaliar suas consequências processuais conforme o caso concreto.

Esse entendimento foi adotado pela Sexta Turma do Superior Tribunal de Justiça no julgamento do Habeas Corpus nº 653.515/RJ, em 23 de novembro de 2021, ocasião em que se firmou a orientação de que a quebra da cadeia de custódia não acarreta, de maneira obrigatória, a inadmissibilidade ou a nulidade da prova colhida. Segundo o precedente, as irregularidades constatadas devem ser sopesadas pelo juiz com os demais elementos produzidos na

instrução, a fim de aferir se a prova é confiável; não havendo outros elementos capazes de sustentar a acusação, a consequência é o reconhecimento da insuficiência probatória (BRASIL, 2022). No âmbito dos crimes digitais, essa orientação reforça a importância de que os órgãos de investigação documentem cada etapa da coleta e da preservação dos vestígios eletrônicos, inclusive por meio de técnicas que permitam verificar sua integridade, como o cálculo do código hash e a extração de imagem forense dos dispositivos, de modo a reduzir o risco de que a prova digital tenha sua confiabilidade questionada em juízo.

2.6. O Marco Civil da Internet e o Regime Jurídico da Prova Digital

O Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e disciplina aspectos essenciais da produção da prova digital. A lei obriga os provedores de conexão a guardar os registros de conexão por um ano (art. 13) e os provedores de aplicações a guardar os registros de acesso a aplicações por seis meses (art. 15). Esses prazos são determinantes para as investigações, pois a falta de requisição tempestiva pode levar à perda definitiva da prova. Por isso, a autoridade policial ou administrativa e o Ministério Público podem requerer cautelarmente a guarda por prazo superior (arts. 13, § 2º, e 15, § 2º). Nesse caso, devem ingressar em sessenta dias com o pedido de autorização judicial de acesso, sob pena de o requerimento perder a eficácia (art. 13, §§ 3º e 4º).

Preservar os registros, porém, não é o mesmo que fornecê-los às autoridades. A preservação apenas evita a eliminação dos dados, ao passo que o fornecimento depende de ordem judicial (art. 10, § 1º). O respectivo requerimento deve indicar, sob pena de

inadmissibilidade, fundados indícios do ilícito, a justificativa da utilidade dos registros e o período a que se referem (art. 22). Essa distinção compatibiliza a obtenção tempestiva da prova com a proteção da privacidade dos usuários, mas exige das autoridades atuação célere e tecnicamente qualificada. Segundo Rossini (2021), a disciplina da guarda de registros representa avanço relevante para a persecução penal, mas sua efetividade depende da capacidade dos órgãos de investigação de requisitar e processar os dados antes do descarte pelos provedores. Essa dificuldade é maior em localidades sem estrutura pericial especializada.

É importante distinguir a preservação cautelar dos registros de seu efetivo fornecimento às autoridades. A preservação busca evitar a eliminação dos dados enquanto são adotadas as providências legais cabíveis, ao passo que o acesso aos registros está sujeito aos requisitos previstos na legislação, inclusive à ordem judicial quando exigida. Essa distinção permite compatibilizar a necessidade de obtenção tempestiva da prova com a proteção da privacidade dos usuários.

2.7. A Cooperação Jurídica Internacional e a Convenção de Budapeste

Como já destacado, a natureza transnacional da internet impõe desafios acentuados à persecução penal, uma vez que servidores, provedores de aplicação e usuários frequentemente estão submetidos a jurisdições distintas, o que dificulta sobremaneira a obtenção de provas hospedadas no exterior. Nesse cenário, a Convenção sobre o Cibercrime, firmada em Budapeste no ano de 2001 no âmbito do Conselho da Europa, constitui o principal tratado internacional voltado à harmonização de tipos penais informáticos e

à facilitação da cooperação entre Estados, prevendo a tipificação de condutas como o acesso ilícito a sistemas informáticos, a interferência em sistemas e dados, a fraude informática e a pornografia infantil, além de instituir uma rede de pontos de contato disponível 24 horas por dia, sete dias por semana, entre os países signatários para o atendimento urgente de pedidos de preservação de prova digital.

O Brasil foi convidado pelo Conselho da Europa a aderir à Convenção em 2019. O texto foi aprovado pelo Congresso Nacional por meio do Decreto Legislativo nº 37, de 16 de dezembro de 2021, e o instrumento de adesão foi depositado junto ao Secretário-Geral do Conselho da Europa em 30 de novembro de 2022, tendo a Convenção entrado em vigor para o Brasil, no plano jurídico externo, em 1º de março de 2023, e sido promulgada internamente pelo Decreto nº 11.491, de 12 de abril de 2023 (BRASIL, 2023). A adesão representa avanço relevante na integração do país aos padrões internacionais de enfrentamento à criminalidade cibernética e amplia as possibilidades de obtenção célere de dados armazenados em servidores estrangeiros. Não obstante, Crespo (2022) pondera que a adesão formal a tratados internacionais não é suficiente por si só, sendo indispensável a internalização de procedimentos ágeis de cooperação e o investimento em canais diretos de comunicação com provedores estrangeiros, sob pena de a cooperação internacional permanecer mais formal do que efetivamente célere para os fins da persecução penal.

2.8. Evolução Legislativa Recente: A Lei Nº 14.155/2021 e a Tipificação da Fraude Eletrônica

A Lei nº 14.155/2021 representa um dos mais recentes esforços do legislador brasileiro para adequar o Código Penal à realidade da criminalidade patrimonial praticada por meios eletrônicos. A norma alterou o artigo 154-A, elevando a pena da invasão de dispositivo informático para reclusão de um a quatro anos e multa e ampliando para um terço a dois terços o aumento de pena aplicável quando da invasão resulta prejuízo econômico, e inseriu o § 4º-B no artigo 155, que prevê pena de reclusão de quatro a oito anos e multa para o furto mediante fraude cometido por meio de dispositivo eletrônico ou informático. Além disso, incluiu o § 2º-A no artigo 171, que prevê a fraude eletrônica, punida com reclusão de quatro a oito anos e multa quando a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. A lei previu, ainda, causas de aumento de pena para essas modalidades, aplicáveis quando o crime é praticado mediante a utilização de servidor mantido fora do território nacional (art. 155, § 4º-C, I, e art. 171, § 2º-B) ou contra idoso ou vulnerável (art. 155, § 4º-C, II, e art. 171, § 4º). Trata-se de sanção significativamente superior à cominada ao estelionato simples (reclusão de um a cinco anos e multa), o que evidencia a intenção do legislador de conferir tratamento penal mais rigoroso às fraudes praticadas com uso de meios informáticos, tais como golpes envolvendo aplicativos de mensagens, clonagem de cartões e páginas falsas de instituições financeiras.

A lei também acrescentou o § 4º ao artigo 70 do Código de Processo Penal, segundo o qual, nos crimes previstos no artigo 171 do Código Penal, quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a

competência será definida pelo local do domicílio da vítima e, em caso de pluralidade de vítimas, firmar-se-á pela prevenção. Trata-se, portanto, de regra restrita ao estelionato praticado nessas modalidades, que não se estende automaticamente a outros crimes digitais, como o furto mediante fraude eletrônica. A medida busca facilitar o acesso à justiça e reduzir a impunidade decorrente da dispersão geográfica entre vítimas e agentes fraudadores. Para Vendramini (2023), essa alteração de competência é especialmente relevante nos crimes cibernéticos patrimoniais, nos quais o infrator frequentemente atua a partir de localidade distinta da vítima, o que dificultava, sob a regra geral de competência do local da consumação do delito, a efetiva responsabilização penal e o ressarcimento do prejuízo sofrido.

3. METODOLOGIA

A pesquisa caracteriza-se como qualitativa e exploratória, com aplicação do método dedutivo, partindo de princípios gerais do Direito, como as normas jurídicas, a segurança da informação e a responsabilidade penal, para a compreensão das situações específicas relacionadas aos crimes cibernéticos (Marconi; Lakatos, 2021). O caráter exploratório mostrou-se adequado por se tratar de campo em constante transformação, possibilitando maior aproximação com o tema e a identificação das principais características dos crimes digitais e dos fatores que contribuem para sua ocorrência (Gil, 2022).

Quanto às técnicas, utilizaram-se a pesquisa bibliográfica, realizada em livros, artigos científicos e demais materiais acadêmicos sobre o tema, e a pesquisa documental, que abrangeu a legislação pertinente, notadamente o Código Penal, o Código de Processo

Penal, o Código de Defesa do Consumidor, a Lei nº 12.737/2012, o Marco Civil da Internet, a Lei Geral de Proteção de Dados, as Leis nº 13.718/2018, nº 13.772/2018, nº 13.964/2019 (Pacote Anticrime), nº 14.132/2021 e nº 14.155/2021 e o Decreto nº 11.491/2023, que promulgou a Convenção de Budapeste, além de precedentes do Supremo Tribunal Federal e do Superior Tribunal de Justiça e de dados estatísticos divulgados pela SaferNet Brasil. Os dispositivos legais foram examinados em sua redação vigente e interpretados à luz da doutrina especializada em Direito Digital e Direito Processual Penal.

Registre-se, como limitação, que a pesquisa não envolveu a análise sistemática de processos judiciais nem a coleta de dados junto a usuários da internet. Por essa razão, suas conclusões decorrem da revisão bibliográfica e documental realizada e não se destinam a mensurar empiricamente a efetividade das normas examinadas.

4. RESULTADOS E ANÁLISES

A partir da revisão teórica realizada, verifica-se que a legislação brasileira, a exemplo da Lei nº 12.737/2012 e da Lei Geral de Proteção de Dados, representa avanços relevantes no enfrentamento dos crimes digitais, mas, segundo as fontes examinadas, enfrenta limitações em sua aplicação diante da velocidade das transformações tecnológicas. Os principais obstáculos apontados pela literatura consultada dizem respeito ao anonimato proporcionado pelo ambiente virtual, à volatilidade da prova digital, à insuficiência de peritos especializados, às limitações estruturais dos órgãos de investigação e às dificuldades de cooperação internacional para obtenção de dados hospedados em servidores estrangeiros, elementos que, em conjunto, contribuem para o cenário aqui denominado impunidade tecnológica.

Verificou-se, ademais, que a positivação da cadeia de custódia pela Lei nº 13.964/2019 e a disciplina da guarda de registros estabelecida pelo Marco Civil da Internet representam avanços relevantes para a confiabilidade da prova digital, mas sua efetividade permanece condicionada à capacidade operacional dos órgãos de investigação em requisitar tempestivamente os dados eletrônicos antes de seu descarte pelos provedores e em preservar corretamente os vestígios coletados. De igual modo, constatou-se que a adesão brasileira à Convenção de Budapeste e as alterações promovidas pela Lei nº 14.155/2021, ao prever formas mais graves de furto e de estelionato praticados mediante fraude eletrônica e ao fixar, para o estelionato praticado mediante depósito, cheque ou transferência de valores, a competência do domicílio da vítima, bem como pelas Leis nº 13.718/2018, nº 13.772/2018 e nº 14.132/2021, ao tipificarem, respectivamente, a divulgação de cena de sexo, nudez ou pornografia sem o consentimento da vítima, o registro não autorizado da intimidade sexual e a perseguição praticada por qualquer meio, inclusive o eletrônico, ampliam o instrumental penal disponível ao Estado. Quanto ao crescimento de 28,4% nas denúncias de crimes cibernéticos recebidas pela SaferNet Brasil em 2025 (Cruz, 2026), esse dado demonstra o volume de denúncias recebidas pelo canal, mas não comprova, por si só, aumento proporcional da criminalidade nem ineficácia da legislação, pois pode refletir também maior conscientização dos usuários e maior acesso aos canais de denúncia. A avaliação da eficácia prática das normas exigiria outros indicadores, como o número de inquéritos instaurados, os índices de identificação da autoria, as denúncias oferecidas pelo Ministério Público e as condenações obtidas, os quais não foram objeto desta pesquisa.

Ainda assim, o volume de denúncias evidencia a relevância do fenômeno e reforça, à luz das fontes examinadas, a necessidade de que a aplicação da lei seja acompanhada de investimento estrutural e de capacitação técnica permanente dos órgãos de investigação.

A bibliografia consultada indica, ainda, que fatores subjetivos, como a sensação de anonimato e a baixa percepção de risco decorrente da ausência de contato físico com a vítima (Crespo, 2022), podem contribuir para a prática de condutas ilícitas no ambiente digital, o que reforça a importância de estratégias de prevenção pautadas na educação e no letramento digital, associadas ao aprimoramento normativo e estrutural do aparato estatal.

5. CONSIDERAÇÕES FINAIS

Com base na pesquisa bibliográfica e documental realizada, conclui-se que o ordenamento jurídico brasileiro dispõe de instrumentos relevantes para a prevenção e a repressão dos crimes digitais, mas sua aplicação enfrenta desafios relacionados à identificação da autoria, à preservação da prova digital, à capacidade técnica dos órgãos de investigação e à cooperação internacional. A pesquisa permite identificar limitações normativas e operacionais discutidas nas fontes examinadas, mas não mensurar diretamente a eficácia prática da legislação ou os índices de responsabilização penal.

Nesse sentido a aplicação das regras de cadeia de custódia da prova digital e dos dispositivos introduzidos ou alterados pela Lei nº 14.155/2021, especialmente aqueles relativos à invasão de dispositivo informático, ao furto mediante fraude eletrônica, ao estelionato eletrônico e à competência territorial em determinadas modalidades de estelionato.

Por fim, entende-se que a educação digital, iniciada ainda na formação básica, pode constituir instrumento preventivo de longo prazo, complementar à repressão penal, na medida em que busca atuar sobre fatores que favorecem o comportamento ilícito, e não apenas sobre suas consequências. Assim, políticas públicas de letramento digital, voltadas tanto a crianças e adolescentes quanto a adultos usuários frequentes da internet, deveriam integrar, de forma permanente e não meramente pontual, a agenda legislativa e educacional brasileira, em articulação com as demais medidas normativas, periciais e institucionais discutidas ao longo deste artigo, de modo que prevenção e repressão deixem de operar de forma isolada e passem a compor um sistema integrado e coerente de enfrentamento à criminalidade praticada no ambiente virtual.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

Diário Oficial da União, Brasília, DF, 13 abr. 2023.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940.

BRASIL. Decreto-Lei nº 3.688, de 3 de outubro de 1941. Lei das Contravenções Penais. **Diário Oficial da União**, Rio de Janeiro, 13 out. 1941.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**, Rio de Janeiro, 13 out. 1941.

BRASIL. Lei nº 11.340, de 7 de agosto de 2006. Lei Maria da Penha. **Diário Oficial da União**, Brasília, DF, 8 ago. 2006.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. **Diário Oficial da União**, Brasília, DF, 3 dez. 2012.

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.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.718, de 24 de setembro de 2018. Tipifica os crimes de importunação sexual e de divulgação de cena de estupro. **Diário Oficial da União**, Brasília, DF, 25 set. 2018.

BRASIL. Lei nº 13.772, de 19 de dezembro de 2018. Altera a Lei Maria da Penha e o Código Penal para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. **Diário Oficial da União**, Brasília, DF, 20 dez. 2018.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. **Diário Oficial da União**, Brasília, DF, 24 dez. 2019.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Acrescenta o art. 147-A ao Código Penal, para prever o crime de perseguição. **Diário Oficial**

da União, Brasília, DF, 1 abr. 2021.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal e o Código de Processo Penal 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.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 12 set. 1990.

BRASIL. Superior Tribunal de Justiça (Segunda Seção). **Súmula nº 479**. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Julgada em 27 jun. 2012. Diário da Justiça Eletrônico, Brasília, DF, 1 ago. 2012.

BRASIL. Supremo Tribunal Federal (Plenário). **Recurso Extraordinário nº 1.010.606/RJ**. Tema 786 da repercussão geral. Relator: Min. Dias Toffoli. Julgado em 11 fev. 2021. Diário da Justiça Eletrônico, Brasília, DF, 20 maio 2021.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. 3. ed. São Paulo: Saraiva, 2022.

CRUZ, Elaine Patrícia. Denúncias de crimes cibernéticos crescem 28% em 2025, mostra Safernet. **Agência Brasil**, Brasília, DF, 10 fev. 2026.

Disponível

em:

<https://agenciabrasil.ebc.com.br/geral/noticia/2026-02/denuncias-de-crimes-ciberneticos-crescem-28-em-2025-mostra-safernet>. Acesso em: 17 set. 2026.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 7. ed. São Paulo: Atlas, 2022.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 9. ed. São Paulo: Atlas, 2021.

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva, 2020.

ROSSINI, Augusto Eduardo de Souza. **Informática, direito e criminalidade**. 2. ed. São Paulo: Almedina, 2021.

VENDRAMINI, João Paulo. **Cybersecurity e os desafios do direito moderno**. Rio de Janeiro: Lumen Juris, 2023.

¹ Acadêmico do 10º período do Curso de Direito da Faculdade de Educação Santa Terezinha – FEST, Imperatriz-MA. E-mail: [acesse o artigo original para visualizar o e-mail](#).

² Professora orientadora do Curso de Direito da Faculdade de Educação Santa Terezinha – FEST, Imperatriz-MA. E-mail: [acesse o artigo original para visualizar o e-mail](#)