v.6, n.4, 2026



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

RESPONSABILIZAÇÃO PENAL NOS CRIMES CIBERNÉTICOS NO BRASIL: DESAFIOS JURÍDICOS E INVESTIGATIVOS

CRIMINAL LIABILITY FOR CYBERCRIMES IN BRAZIL: LEGAL AND INVESTIGATIVE CHALLENGES

RESPONSABILIDAD PENAL POR LOS DELITOS CIBERNÉTICOS EN BRASIL: DESAFÍOS JURÍDICOS Y DE INVESTIGACIÓN

Júlia Reis Almeida[1], Mariah Oliveira Drummond[2], Erika Loureiro Borba[3]

e64357
https://doi.org/10.63026/acertte.v6i4.357

PUBLICADO: 11/2026

RESUMO

A expansão das tecnologias da informação e da comunicação ampliou as possibilidades de interação social, mas também favoreceu a ocorrência de crimes cibernéticos, impondo novos desafios à investigação e à responsabilização penal. Nesse contexto, este artigo tem como objetivo analisar os principais desafios jurídicos e investigativos relacionados à identificação e à responsabilização penal dos autores de crimes cibernéticos no Brasil, considerando a legislação aplicável e os mecanismos disponíveis para o enfrentamento dessas condutas. Metodologicamente, trata-se de pesquisa qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de revisão bibliográfica e análise documental, com exame da legislação brasileira e de publicações científicas sobre o tema. A discussão aborda a conceituação e a classificação dos crimes cibernéticos, os instrumentos normativos de responsabilização penal e os obstáculos relacionados à identificação dos infratores, à obtenção e à preservação das provas digitais, à cadeia de custódia e à cooperação institucional. A análise evidencia que, embora o ordenamento jurídico brasileiro tenha avançado na regulamentação dessas condutas, a efetividade da responsabilização penal ainda depende do aprimoramento da capacidade técnica e operacional dos órgãos de investigação, da qualificação dos profissionais envolvidos e da adequada preservação dos elementos probatórios. Conclui-se que o enfrentamento da criminalidade cibernética exige não apenas instrumentos legais, mas também condições institucionais e tecnológicas que possibilitem sua aplicação efetiva.

Palavras-chave: Crimes cibernéticos. Responsabilização penal. Provas digitais. Investigação criminal. Direito digital.

ABSTRACT

The expansion of information and communication technologies has broadened opportunities for social interaction, but it has also contributed to the occurrence of cybercrimes, creating new challenges for criminal investigation and criminal liability. In this context, this article aims to analyze the main legal and investigative challenges related to identifying and establishing the criminal liability of cybercrime perpetrators in Brazil, considering the applicable legislation and the mechanisms available to address such offenses. Methodologically, this is a qualitative, exploratory, and descriptive study conducted through a bibliographic review and documentary analysis, including an examination of Brazilian legislation and scientific publications on the subject. The discussion addresses the conceptualization and classification of cybercrimes, the legal instruments governing criminal liability, and the obstacles related to identifying offenders, obtaining and preserving digital evidence, maintaining the chain of custody, and promoting institutional cooperation. The analysis shows that, although the Brazilian legal system has made progress in regulating such conduct, the effectiveness of criminal liability still depends on improving the technical and operational capacity of investigative agencies, enhancing the

[1] Graduanda em Direito pelo Afya Centro Universitário de São João del-Rei (Afya SJ del-Rei), Minas Gerais, Brasil.

[2] Graduanda em Direito pelo Afya Centro Universitário de São João del-Rei (Afya SJ del-Rei), Minas Gerais, Brasil.

[3] Doutora em Ciências da Linguagem pela Universidade do Vale do Sapucaí (UNIVÁS) e mestre em Administração Pública pela Universidade Federal de Lavras (UFLA). Especialista em Direito Processual Civil e Gestão Pública Municipal. Graduada em Direito e Administração Pública. Orientadora voluntária da pesquisa.



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

qualifications of the professionals involved, and ensuring the proper preservation of evidentiary material. It is concluded that addressing cybercrime requires not only legal instruments but also institutional and technological conditions that enable their effective application.

***Keywords**: Cybercrimes. Criminal liability. Digital evidence. Criminal investigation. Digital law.*

RESUMEN
La expansión de las tecnologías de la información y la comunicación ha ampliado las posibilidades de interacción social, pero también ha favorecido la comisión de delitos cibernéticos, lo que plantea nuevos desafíos para la investigación y la responsabilidad penal. En este contexto, este artículo tiene como objetivo analizar los principales desafíos jurídicos y de investigación relacionados con la identificación y la responsabilidad penal de los autores de delitos cibernéticos en Brasil, considerando la legislación aplicable y los mecanismos disponibles para hacer frente a estas conductas. Metodológicamente, se trata de una investigación cualitativa, de carácter exploratorio y descriptivo, desarrollada mediante una revisión bibliográfica y un análisis documental, que comprende el examen de la legislación brasileña y de publicaciones científicas sobre el tema. La discusión aborda la conceptualización y clasificación de los delitos cibernéticos, los instrumentos normativos de responsabilidad penal y los obstáculos relacionados con la identificación de los infractores, la obtención y preservación de las pruebas digitales, la cadena de custodia y la cooperación institucional. El análisis demuestra que, aunque el ordenamiento jurídico brasileño ha avanzado en la regulación de estas conductas, la efectividad de la responsabilidad penal todavía depende del fortalecimiento de la capacidad técnica y operativa de los organismos de investigación, de la cualificación de los profesionales involucrados y de la adecuada preservación de los elementos probatorios. Se concluye que el enfrentamiento de la ciberdelincuencia exige no solo instrumentos legales, sino también condiciones institucionales y tecnológicas que permitan su aplicación efectiva.

***Palabras clave**: Delitos cibernéticos. Responsabilidad penal. Pruebas digitales. Investigación criminal. Derecho digital.*

1 INTRODUÇÃO

O avanço das tecnologias da informação e da comunicação transformou profundamente as relações sociais, econômicas e institucionais, modificando a maneira como as pessoas se comunicam, trabalham, realizam transações financeiras e compartilham informações. Embora a expansão do ambiente digital tenha proporcionado inúmeros benefícios, também ampliou as possibilidades de práticas ilícitas, contribuindo para o crescimento dos crimes cibernéticos. Essas condutas abrangem desde fraudes eletrônicas e estelionato digital até invasões de dispositivos, apropriação indevida de dados e outras práticas que comprometem o patrimônio, a privacidade e a segurança das vítimas.

A complexidade dessa modalidade de criminalidade decorre, entre outros fatores, da velocidade de circulação das informações, da possibilidade de ocultação da identidade dos responsáveis, da volatilidade das evidências digitais e da utilização de plataformas e serviços tecnológicos sediados em diferentes países. No Brasil, foram estabelecidos importantes instrumentos jurídicos para enfrentar essas práticas, destacando-se a Lei nº 12.737/2012, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e a Lei nº 14.155/2021, que promoveu alterações na legislação penal relacionadas às fraudes eletrônicas. Entretanto, a existência de normas específicas não assegura, por si só, a efetividade da responsabilização penal, que também depende de recursos tecnológicos, profissionais capacitados e procedimentos adequados de investigação e preservação das provas.



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

Nesse contexto, o presente artigo tem como objeto a análise da responsabilização penal dos autores de crimes cibernéticos à luz do ordenamento jurídico brasileiro, com ênfase nas dificuldades de identificação dos infratores, obtenção e preservação das provas digitais e limitações estruturais e operacionais dos órgãos responsáveis pela investigação e persecução penal, especialmente no âmbito dos municípios. A partir dessa delimitação, estabelece-se o seguinte problema de pesquisa: os mecanismos jurídicos e investigativos atualmente disponíveis no ordenamento jurídico brasileiro são suficientes para garantir a identificação dos autores e a adequada responsabilização penal pelos crimes cibernéticos?

O objetivo do artigo consiste em analisar a responsabilização penal nos crimes cibernéticos no Brasil, considerando os instrumentos jurídicos existentes e os obstáculos à sua aplicação. Especificamente, busca-se examinar a legislação brasileira pertinente, identificar as dificuldades relacionadas à identificação dos responsáveis e à preservação das evidências digitais e discutir os desafios institucionais enfrentados pelos órgãos encarregados da investigação desses delitos.

A relevância do estudo justifica-se pelos impactos sociais e patrimoniais da criminalidade digital e pela necessidade de compreender a distância entre a previsão normativa e as condições concretas de sua aplicação. Sob essa perspectiva, a pesquisa contribui para a discussão sobre a efetividade da legislação penal, a capacidade investigativa das instituições e a necessidade de aprimoramento dos recursos tecnológicos e humanos destinados ao enfrentamento dos crimes cibernéticos.

Quanto à metodologia, trata-se de pesquisa de abordagem qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de revisão bibliográfica e análise documental. A pesquisa bibliográfica fundamenta-se em livros e artigos científicos relacionados aos crimes cibernéticos, à responsabilização penal e ao Direito Digital, enquanto a pesquisa documental compreende o exame da legislação brasileira aplicável ao tema. Conforme Gil (2022), as pesquisas exploratórias contribuem para ampliar a compreensão do problema investigado, enquanto a dimensão descritiva permite caracterizar os aspectos relevantes do fenômeno estudado. Os procedimentos adotados seguem as orientações de Prodanov e Freitas (2013) quanto à organização e ao desenvolvimento da pesquisa científica.

2 CONCEITO E CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

A expressão “crime cibernético” não corresponde a um tipo penal único, mas designa um conjunto de condutas ilícitas praticadas com o emprego de tecnologias da informação ou direcionadas contra dispositivos, sistemas, redes e dados informáticos. Trata-se, portanto, de uma categoria ampla, que abrange diferentes modalidades de infrações cuja execução ou cujos efeitos estão relacionados ao ambiente digital.

Segundo Rossini (2018), os crimes cibernéticos são aqueles praticados mediante a utilização de dispositivos informáticos ou que têm tais dispositivos como objeto ou alvo da conduta criminosa. Essa definição permite compreender que a tecnologia pode assumir diferentes funções na prática

delitiva: servir como instrumento para a execução do crime, constituir o próprio objeto da ação criminosa ou representar o ambiente em que a conduta se desenvolve.

Na mesma perspectiva, Pinheiro (2021) observa que a expansão das tecnologias digitais modificou as formas de interação social e ampliou as possibilidades de realização de condutas ilícitas. O desenvolvimento tecnológico, portanto, não apenas introduziu novos meios de comunicação e armazenamento de informações, mas também modificou a dinâmica de delitos já conhecidos pelo Direito Penal.

Uma classificação recorrente na literatura jurídica distingue os crimes cibernéticos em próprios e impróprios. Os crimes cibernéticos próprios são aqueles cuja configuração está diretamente relacionada à utilização de sistemas ou dispositivos informáticos, tendo como alvo os próprios dispositivos, redes ou dados digitais. É o caso da invasão de dispositivo informático, prevista no art. 154-A do Código Penal, introduzido pela Lei nº 12.737/2012 (BRASIL, 1940; BRASIL, 2012).

Nessa modalidade, a tecnologia constitui elemento essencial da conduta criminosa, uma vez que o sistema informático ou os dados digitais podem representar o próprio objeto material da ação. Rossini (2018) destaca, nesse sentido, a particularidade dos delitos em que os recursos computacionais são diretamente atingidos pela prática criminosa.

Por sua vez, os crimes cibernéticos impróprios correspondem a infrações penais tradicionais praticadas com o auxílio de recursos tecnológicos. Enquadram-se nessa categoria, por exemplo, o estelionato cometido por meio eletrônico, as ameaças realizadas por aplicativos de mensagens e os crimes contra a honra praticados em redes sociais. Nessas situações, a tecnologia modifica o modo de execução da conduta, embora o bem jurídico protegido pela norma penal não seja necessariamente novo.

Pinheiro (2021) observa que a utilização de ferramentas tecnológicas pode alterar significativamente a dinâmica de delitos já conhecidos, especialmente em razão da velocidade de circulação das informações e da multiplicidade de meios utilizados para sua execução. Assim, a distinção entre crimes próprios e impróprios contribui para compreender tanto a natureza da infração quanto as particularidades envolvidas em sua apuração.

Essa classificação também apresenta relevância para a investigação criminal. Nos crimes próprios, a análise pode envolver o dispositivo atingido, os registros de acesso, os arquivos modificados e os mecanismos de segurança eventualmente violados. Nos crimes impróprios, além da identificação do autor e da comprovação da materialidade, podem ser necessários o exame de comunicações, transações financeiras, dados cadastrais e registros mantidos por provedores de conexão e de aplicações.

Para Queiroz (2025), a investigação dessas infrações exige atenção às informações armazenadas em ambientes digitais e à necessidade de preservação dos dados para sua utilização no processo penal. A qualificação técnica dos agentes responsáveis pela apuração também constitui aspecto relevante para a adequada condução dos procedimentos investigativos.



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

É importante destacar, contudo, que a distinção entre crimes próprios e impróprios não deve ser compreendida de maneira rígida. Um mesmo episódio pode envolver diferentes condutas e, eventualmente, mais de uma infração penal. Uma fraude eletrônica, por exemplo, pode ser precedida pela invasão de uma conta e pelo uso indevido de dados pessoais, seguida de transferências de valores para contas de terceiros. Por essa razão, a análise jurídica deve considerar o conjunto das condutas praticadas, e não apenas o recurso tecnológico utilizado.

Desse modo, a compreensão dos crimes cibernéticos exige a análise conjunta da conduta, do tipo penal aplicável, dos recursos tecnológicos empregados e dos elementos digitais que podem contribuir para a identificação dos responsáveis. Essa delimitação conceitual constitui ponto de partida para o exame da legislação brasileira e dos mecanismos de responsabilização penal, abordados na seção seguinte.

3 RESPONSABILIZAÇÃO PENAL E LEGISLAÇÃO BRASILEIRA APLICÁVEL AOS CRIMES CIBERNÉTICOS

A evolução legislativa brasileira relacionada aos crimes cibernéticos ocorreu de forma gradual, acompanhando a expansão do uso da internet, dos dispositivos móveis, das redes sociais e dos serviços digitais. Esse processo exigiu adaptações no ordenamento jurídico para contemplar condutas praticadas por meio de recursos tecnológicos e estabelecer parâmetros para a proteção de direitos no ambiente virtual. Segundo Pinheiro (2021), o desenvolvimento das tecnologias digitais modificou as relações sociais e ampliou a necessidade de regulamentação jurídica dessas novas formas de interação.

Um dos primeiros marcos específicos foi a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que introduziu no Código Penal o art. 154-A, tipificando a invasão de dispositivo informático (BRASIL, 2012). O dispositivo prevê a responsabilização penal pela invasão de dispositivo informático de uso alheio, conectado ou não à rede de computadores, quando presentes as circunstâncias e finalidades previstas na legislação. A norma representou um avanço ao estabelecer resposta penal específica para determinadas condutas dirigidas contra dispositivos e sistemas informáticos.

A importância dessa alteração está relacionada ao reconhecimento de que os recursos tecnológicos podem constituir não apenas instrumentos para a prática de delitos tradicionais, mas também objetos diretamente atingidos pela ação criminosa. Conforme Rossini (2018), a criminalidade informática exige que o Direito Penal considere as particularidades dos sistemas e dispositivos utilizados ou atingidos pela conduta. Entretanto, a criação de tipos penais específicos não elimina os desafios decorrentes da constante transformação tecnológica, da multiplicidade de plataformas e da utilização de serviços digitais sediados em outros países.

Em 2014, foi promulgada a Lei nº 12.965/2014, denominada Marco Civil da Internet, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil (BRASIL, 2014). Entre seus fundamentos estão a proteção dos direitos humanos, a liberdade de expressão e a

preservação da privacidade. O art. 8º, por sua vez, estabelece a proteção da privacidade e da liberdade de expressão nas comunicações como condição para o pleno exercício do direito de acesso à internet.

Segundo Souza et al. (2018), o Marco Civil da Internet estabeleceu parâmetros jurídicos para o funcionamento da rede no país, disciplinando questões relacionadas à privacidade, aos registros digitais e à responsabilidade dos provedores. Essa regulamentação possui relevância para as investigações criminais que dependem da obtenção de informações armazenadas por empresas responsáveis por serviços digitais.

Nesse contexto, os arts. 10 a 15 do Marco Civil apresentam disposições importantes para a preservação e a obtenção de informações digitais. O art. 10 determina que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações, bem como de dados pessoais e do conteúdo de comunicações privadas, devem respeitar a intimidade, a vida privada, a honra e a imagem das partes envolvidas (BRASIL, 2014). O acesso ao conteúdo de comunicações privadas armazenadas depende de ordem judicial, observadas as condições legais.

Os arts. 13 e 15 estabelecem obrigações específicas de guarda de registros. O primeiro prevê, como regra, a conservação dos registros de conexão pelo prazo de um ano pelos provedores de conexão; o segundo estabelece o prazo de seis meses para a guarda dos registros de acesso a aplicações de internet pelos provedores abrangidos pela disposição legal (BRASIL, 2014). Esses registros podem contribuir para a reconstrução de fatos e a identificação de possíveis responsáveis, desde que sua obtenção observe os requisitos legais e as garantias fundamentais.

A relevância desses ambientes digitais também pode ser compreendida a partir da expansão da Internet das Coisas, que amplia a conexão entre dispositivos e serviços. De Liberal (2025), ao discutir os desafios da criação de produtos e serviços com essa tecnologia, chama atenção para questões relacionadas ao monitoramento permanente e aos possíveis impactos sobre a privacidade dos indivíduos. Embora o estudo não tenha como objeto específico a investigação criminal, sua abordagem contribui para compreender a ampliação dos ambientes tecnológicos nos quais informações podem ser produzidas, armazenadas e utilizadas, aspecto que reforça a importância da proteção de dados e da segurança digital.

Em 2018, foi publicada a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que regulamenta o tratamento de dados pessoais e estabelece princípios como finalidade, adequação, necessidade, segurança, prevenção e responsabilização (BRASIL, 2018). Boff, Fortes e Freitas (2018) destacam a crescente relevância da proteção de dados diante da expansão das tecnologias da informação e da utilização de informações pessoais em ambientes digitais.

A relação entre a LGPD e o enfrentamento dos crimes cibernéticos, contudo, exige uma distinção jurídica. Embora a proteção de dados pessoais seja relevante para a segurança e a privacidade dos indivíduos, a própria LGPD estabelece, em seu art. 4º, inciso III, alínea “d”, que suas disposições não se aplicam ao tratamento de dados realizado para fins exclusivos de investigação e repressão de infrações penais. Isso não significa ausência de limites jurídicos para o tratamento dessas informações, que deve observar as garantias constitucionais e a legislação pertinente. Assim, a

proteção de dados e a investigação criminal devem ser compreendidas em suas respectivas esferas normativas.

Outro marco relevante foi a Lei nº 13.964/2019, conhecida como Pacote Anticrime, que introduziu no Código de Processo Penal os arts. 158-A a 158-F, responsáveis por disciplinar a cadeia de custódia dos vestígios (BRASIL, 2019). Esse conjunto de procedimentos busca documentar a trajetória do vestígio desde seu reconhecimento até sua destinação final, permitindo acompanhar as etapas de coleta, armazenamento, manuseio, transferência e análise.

A cadeia de custódia assume especial importância nas investigações de crimes cibernéticos, uma vez que as evidências podem estar armazenadas em computadores, celulares, servidores, aplicativos e outros sistemas digitais. Badaró (2024) destaca que a prova digital apresenta características próprias, exigindo procedimentos técnicos adequados para sua obtenção, conservação, análise e apresentação judicial. Dessa forma, a confiabilidade da evidência depende não apenas de seu conteúdo, mas também da possibilidade de demonstrar como foi obtida e preservada.

Em 2021, a Lei nº 14.155 promoveu alterações no Código Penal e no Código de Processo Penal, tornando mais graves determinadas condutas relacionadas à violação de dispositivos informáticos, ao furto e ao estelionato praticados por meios eletrônicos ou pela internet (BRASIL, 2021). Entre as alterações, destaca-se a inclusão do § 2º-A no art. 171 do Código Penal, que prevê a fraude eletrônica como modalidade de estelionato praticada mediante utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos, correio eletrônico fraudulento ou outros meios semelhantes.

A mesma lei também acrescentou o § 4º ao art. 70 do Código de Processo Penal, estabelecendo regra específica de competência territorial para determinadas modalidades de estelionato, com referência ao domicílio da vítima. Nos casos de pluralidade de vítimas, a competência é definida pela prevenção, conforme previsto no dispositivo legal (BRASIL, 1941; BRASIL, 2021).

A evolução normativa demonstra que o ordenamento jurídico brasileiro passou a dispor de instrumentos penais e processuais relevantes para o enfrentamento dos crimes praticados com a utilização de tecnologias digitais. Entretanto, a existência de normas específicas não assegura, isoladamente, a efetividade da responsabilização penal. Sua aplicação depende também da capacidade de identificar os envolvidos, obter informações por meios juridicamente adequados, preservar as evidências e garantir a confiabilidade da prova produzida. Esses aspectos conduzem à análise dos desafios investigativos e institucionais abordados na seção seguinte.

4 DESAFIOS DA INVESTIGAÇÃO E EFETIVIDADE DA RESPONSABILIZAÇÃO PENAL

A prova digital constitui elemento central na investigação dos crimes cibernéticos, podendo estar presente em computadores, celulares, servidores, aplicativos, redes sociais, sistemas bancários, serviços de armazenamento em nuvem e outros dispositivos conectados à internet. Diferentemente de vestígios físicos tradicionais, os dados digitais apresentam características específicas, como

volatilidade, facilidade de reprodução e possibilidade de alteração, o que exige procedimentos técnicos adequados para sua obtenção, conservação e análise.

Segundo Badaró (2024), a prova digital possui particularidades que exigem atenção metodológica durante todas as etapas de sua produção. Nesse sentido, sua confiabilidade não depende apenas do conteúdo apresentado, mas também da demonstração de como a informação foi obtida, armazenada, examinada e preservada. Massena (2023) também destaca a importância da cadeia de custódia para assegurar a rastreabilidade dos vestígios e possibilitar o exercício do contraditório e da ampla defesa.

No ordenamento jurídico brasileiro, os arts. 158-A a 158-F do Código de Processo Penal estabelecem procedimentos destinados a documentar a trajetória do vestígio, desde seu reconhecimento até sua destinação final (BRASIL, 1941). Nas investigações que envolvem evidências digitais, essa documentação deve permitir a identificação dos responsáveis pela coleta e pelo manuseio, dos equipamentos e ferramentas utilizados, das condições de armazenamento e das transferências realizadas. Tais cuidados contribuem para preservar a integridade do material e permitir seu posterior controle pelas partes.

Entre os recursos técnicos utilizados para verificar a integridade de arquivos digitais estão os códigos hash, que geram identificadores matemáticos a partir do conteúdo de determinado arquivo. A comparação desses identificadores pode indicar se houve alteração no material entre diferentes etapas do procedimento. Entretanto, esse recurso não deve ser considerado isoladamente: a confiabilidade da evidência também depende da documentação dos procedimentos, da preservação dos dados originais e da possibilidade de avaliação técnica dos métodos empregados (BADARÓ, 2024).

Outro desafio relevante consiste na identificação dos responsáveis pelas condutas criminosas. O endereço IP pode contribuir para localizar uma conexão à internet, mas não permite, isoladamente, determinar quem praticou o delito. O Marco Civil da Internet define o endereço IP como código atribuído a um terminal de uma rede para permitir sua identificação (BRASIL, 2014). Isso não significa, contudo, que o titular da conexão seja necessariamente o autor da infração, uma vez que diferentes pessoas podem utilizar o mesmo equipamento ou acesso à internet.

Queiroz (2025) ressalta que a investigação de crimes cibernéticos pode depender da análise conjunta de diferentes informações, especialmente diante da utilização de múltiplas plataformas e serviços digitais. Além disso, mecanismos de anonimização, contas falsas, linhas telefônicas cadastradas em nome de terceiros, computadores públicos e serviços estrangeiros podem dificultar a identificação dos envolvidos. Esses recursos não tornam necessariamente impossível a apuração dos fatos, mas podem ampliar o tempo e a complexidade das investigações.

A evolução tecnológica também acrescenta novos desafios à segurança cibernética. A inteligência artificial, por exemplo, pode ser utilizada tanto no desenvolvimento de mecanismos de proteção quanto no aperfeiçoamento de ameaças digitais. Laroche Borba e Araujo Mota (2024), ao analisarem os riscos da inteligência artificial nos ciberataques, discutem as ameaças potenciais, as táticas utilizadas por agentes maliciosos e as estratégias de defesa. Essa discussão evidencia que a



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

sofisticação dos recursos tecnológicos exige atualização constante dos conhecimentos e instrumentos empregados na prevenção e na investigação dos delitos digitais.

Correa Junior (2024) aponta que a apuração dessas infrações também enfrenta obstáculos relacionados à utilização de mecanismos de criptografia, à necessidade de decisões judiciais para determinados acessos e à dificuldade de obtenção de informações junto aos responsáveis por sua guarda. Por esse motivo, a identificação dos autores não deve se fundamentar exclusivamente em um único elemento, como o endereço IP, mas na análise integrada de registros de conexão, dados de acesso a aplicações, informações cadastrais, registros financeiros, mensagens e outros elementos pertinentes à reconstrução dos fatos.

A obtenção dessas informações, entretanto, deve respeitar os limites constitucionais e legais. O acesso ao conteúdo de comunicações privadas está sujeito às garantias estabelecidas pelo ordenamento jurídico e, nas hipóteses legalmente previstas, depende de autorização judicial (BRASIL, 1988; BRASIL, 2014). Da mesma forma, os pedidos de fornecimento de dados devem apresentar elementos que permitam delimitar as informações pretendidas, observando os critérios de necessidade e adequação e evitando medidas genéricas que possam comprometer direitos fundamentais.

A localização de dados em servidores estrangeiros constitui outra dificuldade. Empresas responsáveis por plataformas digitais podem manter estruturas empresariais e servidores em diferentes países, o que pode exigir mecanismos de cooperação jurídica internacional para a obtenção das informações necessárias. Nesse contexto, a diferença entre a rapidez com que os crimes podem ser praticados e o tempo necessário para formalizar pedidos, obter decisões judiciais e receber respostas dos provedores representa um obstáculo à efetividade da investigação.

Para Queiroz (2025), a preservação tempestiva dos dados é relevante para evitar que informações importantes deixem de estar disponíveis durante a apuração. Assim, a atuação dos órgãos responsáveis deve conciliar a rapidez necessária à preservação dos vestígios com o respeito às garantias fundamentais, especialmente à privacidade, ao sigilo das comunicações, ao contraditório e à ampla defesa.

Além das dificuldades técnicas e jurídicas, a estrutura institucional disponível também influencia os resultados das investigações. Em diferentes localidades, especialmente nos municípios do interior, os casos podem ser conduzidos por unidades policiais com atribuições gerais, sem especialização exclusiva em crimes digitais. A inexistência de uma delegacia especializada não significa, necessariamente, ausência de investigação, mas pode ampliar a demanda sobre equipes que também atuam em outras modalidades criminosas.

Esse cenário pode dificultar a formação e a manutenção de equipes com conhecimentos específicos em informática forense, análise de dispositivos móveis, rastreamento de transações, preservação de metadados, interpretação de registros de acesso e elaboração de solicitações direcionadas aos provedores. Conforme destaca Queiroz (2025), a qualificação dos agentes responsáveis constitui aspecto relevante, considerando que mesmo delitos tradicionalmente conhecidos podem apresentar evidências armazenadas em ambientes virtuais.



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

A disponibilidade de equipamentos e ferramentas adequados também interfere na qualidade da investigação. A aquisição e a análise forense de dispositivos exigem procedimentos técnicos documentados e profissionais capacitados para interpretar os resultados. Não basta, portanto, que os órgãos responsáveis disponham de recursos tecnológicos: é necessário assegurar treinamento, padronização metodológica e condições para que os procedimentos realizados possam ser posteriormente examinados e questionados pelas partes.

Outro aspecto diz respeito à disponibilidade de profissionais especializados em perícia digital. Quando determinada localidade não dispõe de estrutura pericial própria, pode depender do deslocamento de profissionais, do encaminhamento dos equipamentos para outras cidades ou da atuação de unidades regionais. Essa dependência pode aumentar o tempo necessário para a análise dos vestígios e comprometer a agilidade da investigação, especialmente quando há dados sujeitos à alteração ou perda.

A efetividade da responsabilização penal também depende da comunicação e da cooperação entre os diferentes órgãos e instituições envolvidos. A investigação pode exigir atuação articulada entre polícia judiciária, perícia oficial, Ministério Público, Poder Judiciário, instituições financeiras e provedores de aplicação. Correa Junior (2024) destaca a importância da cooperação e do acesso às informações diante da complexidade das investigações digitais, indicando que a atuação isolada dos órgãos pode dificultar a obtenção de elementos necessários à elucidação dos fatos.

Dessa forma, os desafios da responsabilização penal nos crimes cibernéticos não decorrem exclusivamente da existência ou da ausência de normas específicas. Embora o ordenamento jurídico brasileiro disponha de instrumentos para tipificação de condutas, preservação de registros e produção da prova, sua efetividade depende da capacidade concreta de investigação, da qualificação dos profissionais, da disponibilidade de recursos técnicos e da cooperação institucional. A distância entre a previsão normativa e as condições reais de aplicação representa, portanto, um dos principais obstáculos à apuração desses delitos e à responsabilização de seus autores.

5 CONSIDERAÇÕES

A análise realizada permite concluir que a responsabilização penal nos crimes cibernéticos ainda enfrenta obstáculos que ultrapassam a existência de normas jurídicas específicas. Embora o ordenamento jurídico brasileiro tenha avançado na regulamentação das condutas praticadas no ambiente digital, especialmente por meio da Lei nº 12.737/2012, do Marco Civil da Internet, da Lei Geral de Proteção de Dados e da Lei nº 14.155/2021, a aplicação efetiva desses instrumentos depende de condições técnicas, institucionais e operacionais adequadas.

O estudo demonstrou que os crimes cibernéticos apresentam características próprias, podendo ser classificados em próprios e impróprios, conforme a relação entre a tecnologia e a conduta criminosa. Essa distinção contribui para compreender as diferentes formas de execução dos delitos e as particularidades envolvidas em sua investigação. Verificou-se, ainda, que a identificação dos responsáveis constitui um dos principais desafios da persecução penal, sobretudo diante da utilização

de mecanismos de anonimização, da multiplicidade de plataformas digitais e da insuficiência de elementos isolados, como o endereço IP, para determinar a autoria.

Em relação à produção probatória, constatou-se que a volatilidade e a possibilidade de alteração dos dados digitais exigem procedimentos específicos de coleta, preservação e análise. Nesse contexto, a observância da cadeia de custódia, prevista no Código de Processo Penal, é fundamental para assegurar a integridade e a confiabilidade dos vestígios, bem como possibilitar o contraditório e a ampla defesa. A obtenção das informações também deve respeitar as garantias constitucionais e os limites legais, conciliando as necessidades da investigação com a proteção dos direitos fundamentais.

Quanto aos desafios institucionais, a análise evidenciou que a insuficiência de profissionais especializados, a limitação de equipamentos e estruturas periciais e as dificuldades de cooperação entre os órgãos envolvidos podem comprometer a agilidade e a qualidade das investigações. A atuação integrada entre polícia judiciária, perícia oficial, Ministério Público, Poder Judiciário, instituições financeiras e provedores de aplicação mostra-se relevante para a obtenção de informações e a adequada apuração dos fatos.

Diante dessas constatações, o problema de pesquisa pode ser respondido no sentido de que o Brasil dispõe de instrumentos jurídicos relevantes para a responsabilização penal dos autores de crimes cibernéticos, mas sua suficiência normativa não assegura, por si só, a efetividade da investigação e da aplicação da lei. A concretização dessa responsabilização depende da articulação entre legislação, capacidade técnica, recursos institucionais, preservação adequada das provas e cooperação entre os diferentes atores envolvidos.

Conclui-se, portanto, que o enfrentamento da criminalidade cibernética exige aperfeiçoamento contínuo das estruturas de investigação, investimento em capacitação profissional e atualização dos recursos tecnológicos, sem afastar as garantias fundamentais que orientam o processo penal. Como contribuição, o estudo reforça que a efetividade da responsabilização penal não depende apenas da criação de novos tipos penais, mas também das condições concretas para identificar os responsáveis, produzir provas confiáveis e assegurar a aplicação adequada do ordenamento jurídico brasileiro.

REFERÊNCIAS

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, p. 7–9, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 12 nov. 2026.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 nov. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Institui o Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 nov. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Institui o Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 12 nov. 2026.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 nov. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 nov. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2026.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 12 nov. 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 – 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. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 12 nov. 2026.

CORREA JUNIOR, Edilson Carlos Lima. Os obstáculos da investigação dos crimes digitais. **Avante: Revista Acadêmica da Polícia de Minas Gerais**, [S. l.], v. 1, n. 4, 2024. DOI: https://doi.org/10.70365/2764-0779.2023.84. Disponível em: https://revistaavante.policiacivil.mg.gov.br/index.php/avante/article/view/84. Acesso em: 12 nov. 2026.

DE LIBERAL, Renan Costa. Desafios na criação de produtos e serviços com a Internet das Coisas. **Revista Científica ACERTTE**, v. 5, n. 3, e53227, 2025. DOI: https://doi.org/10.63026/acertte.v5i3.227.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2022.

LAROCHE BORBA, Gabriel; ARAUJO MOTA, Luis Felipe. Análise dos riscos da inteligência artificial nos ciberataques. **Revista Científica ACERTTE**, v. 4, n. 4, e44182, 2024. DOI: https://doi.org/10.63026/acertte.v4i4.182.

MASSENA, Caio Badaró. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. **Boletim IBCCRIM**, São Paulo, v. 31, n. 368, p. 19–21, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506. Acesso em: 12 nov. 2026.

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

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. **Revista do CNMP**, [S. l.], n. 12, p. 417–448, 2025. DOI:



REVISTA CIENTÍFICA ACERTTE
ISSN 2763-8928

https://doi.org/10.36662/revistadocnmp.i12.707. Disponível em: https://ojs.cnmp.mp.br/index.php/revistacnmp/article/view/707. Acesso em: 12 nov. 2026.

ROSSINI, Augusto Eduardo de Souza. **Crimes eletrônicos e provas digitais**. São Paulo: Saraiva, 2018.

SOUZA, Carlos Affonso Pereira de et al. **Marco Civil da Internet: jurisprudência comentada**. São Paulo: Revista dos Tribunais, 2018.