



FRANCISCA LAVYNNIA SOBREIRA BISPO

MATEUS BRITO DE ARÊA LEÃO

MATHEUS LOPES CAVALCANTE NOGUEIRA

**CRIMES CIBERNÉTICOS NO BRASIL: DESAFIOS PARA O DIREITO PENAL NA
ERA DIGITAL**

TERESINA-PI

2025

FRANCISCA LAVYNNIA SOBREIRA BISPO

MATEUS BRITO DE ARÊA LEÃO

MATHEUS LOPES CAVALCANTE NOGUEIRA

**CRIMES CIBERNÉTICOS NO BRASIL: DESAFIOS PARA O DIREITO PENAL NA
ERA DIGITAL**

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Direito em Uninovafapi.

Orientador(a): Viviane Maria de Pádua
Rios Magalhães

TERESINA – PI

2025

FICHA CATALOGRÁFICA

3622c Bispo, Francisca Lavynnia Sobreira

Crimes Cibernéticos no Brasil: Desafios para o direito penal na era digital. / Francisca Lavynnia Sobreira Bispo; Mateus Brito de Arêa Leão; Matheus Lopes Cavalcante Nogueira: UNINOVAFAPI, 2025.

Orientador (a): Prof^o. Viviane Maria de Pádua Rios Magalhães – UNINOVAFAPI, 2025.

48.p.; 23cm.

Trabalho de conclusão (Graduação em Direito) – UNINOVAFAPI, Teresina, 2025.

1. Crimes cibernéticos. 2. Direito penal brasileiro. 3. Jurisdição. Título. II. Bispo, Francisca Lavynnia Sobreira. III. Leão, Mateus Brito de Arêa. IV. Nogueira, Matheus Lopes Cavalcante.

CDD 341.5

FRANCISCA LAVYNNIA SOBREIRA BISPO
MATEUS BRITO DE ARÊA LEÃO
MATHEUS LOPES CAVALCANTE NOGUEIRA

**CRIMES CIBERNÉTICOS NO BRASIL: desafios para o direito penal na
era digital**

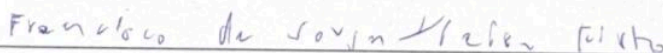
Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 13 / 11 / 2025

BANCA EXAMINADORA



Professora Mestra Viviane Maria de Padua Rios Magalhães
Afya Centro Universitário Uninovafapi
(Orientadora)



Professor Mestre Francisco de Sousa Vieira Filho
Afya Centro Universitário Uninovafapi
(1º Examinador)



Professor Mestre José Augusto de Carvalho Mendes Filho
Afya Centro Universitário Uninovafapi
(2º Examinador)

RESUMO

A crescente digitalização das relações pessoais, comerciais e institucionais no Brasil tem intensificado a ocorrência de crimes cibernéticos, caracterizados por infrações praticadas por meio de sistemas informáticos e redes digitais, que afetam direitos fundamentais, segurança, privacidade e integridade de dados. Apesar de avanços legislativos, como a Lei nº 12.737/2012 e o Marco Civil da Internet (Lei nº 12.965/2014), o direito penal brasileiro ainda enfrenta limitações na repressão dessas infrações. Este trabalho tem como objetivo geral analisar os desafios do direito penal brasileiro no enfrentamento dos crimes cibernéticos, com enfoque nos objetivos específicos de identificar dificuldades na coleta, preservação e valoração de provas digitais, examinar limitações da jurisdição e da competência penal, e analisar lacunas legislativas que dificultam a repressão penal de delitos digitais. Adotou-se abordagem qualitativa, baseada em pesquisa bibliográfica e documental, com análise de legislação, doutrina e jurisprudência. Os resultados indicam que lacunas legais, insuficiência de recursos técnicos, ausência de padronização de procedimentos e falta de capacitação especializada comprometem a efetividade do sistema penal. Conclui-se que a modernização legislativa, a capacitação institucional e a criação de protocolos específicos são essenciais para fortalecer a atuação do direito penal frente aos crimes digitais no Brasil.

Palavras-chave: Crimes cibernéticos; Direito penal brasileiro; Jurisdição.

ABSTRACT

The increasing digitalization of personal, commercial, and institutional relations in Brazil has intensified the occurrence of cybercrimes, defined as offenses committed through computer systems and digital networks, which affect fundamental rights, security, privacy, and data integrity. Despite legislative advances, such as Law No. 12.737/2012 and the Brazilian Internet Civil Framework (Law No. 12.965/2014), Brazilian criminal law still faces limitations in suppressing these offenses. This study aims to analyze the challenges faced by Brazilian criminal law in addressing cybercrimes, focusing on identifying difficulties in the collection, preservation, and evaluation of digital evidence, examining limitations of jurisdiction and criminal competence, and analyzing legislative gaps that hinder the penal repression of digital crimes. A qualitative approach was adopted, based on bibliographic and documentary research, including the analysis of legislation, doctrine, and jurisprudence. The results indicate that legal gaps, insufficient technical resources, lack of standardized procedures, and inadequate specialized training compromise the effectiveness of the criminal justice system. It is concluded that legislative modernization, institutional capacity building, and the creation of specific protocols are essential to strengthen criminal law performance against digital crimes in Brazil.

Keywords: Cybercrime; Brazilian criminal law; Jurisdiction.

SUMÁRIO

1 INTRODUÇÃO 8

2 ARTIGO 8

3 CONSIDERAÇÕES FINAIS 28

REFERÊNCIAS 29

ANEXO A - COMPROVANTE DE SUBMISSÃO..... 30

1 INTRODUÇÃO

A criminalidade digital impõe um desafio de adaptação imediata ao sistema de justiça criminal brasileiro. O crescimento exponencial dos crimes cibernéticos, evidenciado pelo aumento de 56,4% nos incidentes graves em 2023 no Brasil (Palo Alto Networks, 2024), torna urgente a análise da eficácia da resposta penal. Embora o ordenamento jurídico tenha avançado com marcos como a LGPD e o Marco Civil da Internet, a repressão ainda é comprometida por obstáculos técnicos, probatórios e de competência. Neste contexto, o problema de pesquisa central deste trabalho é: Quais são as limitações e possibilidades do direito penal brasileiro no enfrentamento dos crimes cibernéticos, diante dos desafios normativos, técnicos e institucionais que comprometem a eficácia da repressão penal?

O estudo se justifica pela necessidade de fortalecer a segurança digital e otimizar a atuação institucional. O objetivo geral é analisar a eficácia do sistema penal, identificando suas limitações e propondo melhorias. Para tal, os objetivos específicos abrangem: (a) identificar desafios na coleta, preservação e valoração das provas eletrônicas; (b) demonstrar a aplicação da jurisdição e competência penal; e (c) elencar as lacunas legislativas que dificultam a repressão. A metodologia é de natureza qualitativa, pautada em pesquisa bibliográfica e documental (legislação, doutrina e jurisprudência do STJ). O trabalho está estruturado em três seções que abordarão, respectivamente, os desafios técnicos da prova digital, a questão da jurisdição e competência penal e as lacunas normativas.

2 ARTIGO

CRIMES CIBERNÉTICOS NO BRASIL: desafios para o direito penal na era digital

CYBERCRIMES IN BRAZIL: challenges for criminal law in the digital era

RESUMO

A crescente digitalização das relações pessoais, comerciais e institucionais no Brasil tem intensificado a ocorrência de crimes cibernéticos, caracterizados por infrações praticadas por meio de sistemas informáticos e redes digitais, que afetam direitos fundamentais, segurança, privacidade e integridade de dados. Apesar de avanços

legislativos, como a Lei nº 12.737/2012 e o Marco Civil da Internet (Lei nº 12.965/2014), o direito penal brasileiro ainda enfrenta limitações na repressão dessas infrações. Este trabalho tem como objetivo geral analisar os desafios do direito penal brasileiro no enfrentamento dos crimes cibernéticos, com enfoque nos objetivos específicos de identificar dificuldades na coleta, preservação e valoração de provas digitais, examinar limitações da jurisdição e da competência penal, e analisar lacunas legislativas que dificultam a repressão penal de delitos digitais. Adotou-se abordagem qualitativa, baseada em pesquisa bibliográfica e documental, com análise de legislação, doutrina e jurisprudência. Os resultados indicam que lacunas legais, insuficiência de recursos técnicos, ausência de padronização de procedimentos e falta de capacitação especializada comprometem a efetividade do sistema penal. Conclui-se que a modernização legislativa, a capacitação institucional e a criação de protocolos específicos são essenciais para fortalecer a atuação do direito penal frente aos crimes digitais no Brasil.

Palavras-chave: Crimes cibernéticos; Direito penal brasileiro; Jurisdição.

ABSTRACT

The increasing digitalization of personal, commercial, and institutional relations in Brazil has intensified the occurrence of cybercrimes, defined as offenses committed through computer systems and digital networks, which affect fundamental rights, security, privacy, and data integrity. Despite legislative advances, such as Law No. 12.737/2012 and the Brazilian Internet Civil Framework (Law No. 12.965/2014), Brazilian criminal law still faces limitations in suppressing these offenses. This study aims to analyze the challenges faced by Brazilian criminal law in addressing cybercrimes, focusing on identifying difficulties in the collection, preservation, and evaluation of digital evidence, examining limitations of jurisdiction and criminal competence, and analyzing legislative gaps that hinder the penal repression of digital crimes. A qualitative approach was adopted, based on bibliographic and documentary research, including the analysis of legislation, doctrine, and jurisprudence. The results indicate that legal gaps, insufficient technical resources, lack of standardized procedures, and inadequate specialized training compromise the effectiveness of the criminal justice system. It is concluded that legislative modernization, institutional capacity building, and the creation of specific protocols are essential to strengthen criminal law performance against digital crimes in Brazil.

Keywords: Cybercrime; Brazilian criminal law; Jurisdiction.

INTRODUÇÃO

Um relatório divulgado pela Palo Alto Networks apontou que, em 2023, o Brasil enfrentou 61 incidentes distintos de crimes digitais graves, marcando um aumento de 56,4% em relação a 2021, evidenciando a urgência de respostas jurídicas mais eficazes (Palo Alto Networks, 2024). Hoje, praticamente tudo passa pelo meio digital, desde transações financeiras até simples conversas em redes sociais, e isso acaba abrindo espaço para novas formas de crime. Diante desse

cenário, o direito penal brasileiro vem sendo desafiado a se adaptar a uma realidade que muda o tempo todo, exigindo respostas rápidas, seguras e eficazes.

O ordenamento jurídico brasileiro avançou na regulamentação dos crimes cibernéticos, destacando-se a Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, que tipifica a invasão de dispositivos informáticos, e a Lei nº 12.965, de 23 de abril de 2014, denominada Marco Civil da Internet, que estabelece princípios, garantias e direitos relacionados ao uso da internet. Mais recentemente, a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), complementada pelo Decreto nº 12.573, de 15 de janeiro de 2025, que regulamenta dispositivos da LGPD e institui a Política Nacional de Cibersegurança (PNCiber), consolidou diretrizes para a proteção de dados e cibersegurança, reforçando a necessidade de integração entre políticas públicas, ética e legislação na tutela dos direitos digitais.

Nesse sentido, o problema de pesquisa deste trabalho consiste em compreender quais são as limitações e possibilidades do direito penal brasileiro no enfrentamento dos crimes cibernéticos, diante dos desafios normativos, técnicos e institucionais que comprometem a eficácia da repressão penal nesse campo, considerando tanto a legislação vigente quanto os obstáculos práticos enfrentados pelas autoridades?

Este estudo é relevante frente ao cenário de expansão da criminalidade digital no país e aos graves reflexos sociais, econômicos e jurídicos que ele impõe, pois proteger dados pessoais, garantir a segurança da informação e zelar pelos direitos fundamentais exige que as normas e instituições estejam em constante aprimoramento. Por isso, o trabalho que se propõe a compreender os limites do direito penal e apontar caminhos para sua melhora é essencial para o fortalecimento da segurança digital e para otimizar a resposta das instituições responsáveis pela repressão.

O objetivo geral deste trabalho é analisar a eficácia do sistema penal brasileiro no enfrentamento dos crimes cibernéticos, identificando suas limitações e propondo caminhos para a melhoria da legislação e da atuação institucional. Busca-se compreender de que forma o ordenamento jurídico, aliado às políticas públicas e à cooperação entre órgãos de investigação e instituições judiciais, consegue lidar com as novas modalidades de delitos digitais que surgem com o avanço da tecnologia.

Os objetivos específicos são identificar os desafios enfrentados pelo direito penal com foco na coleta, preservação e valoração das provas eletrônicas, demonstrar segundo a jurisdição e a competência penal que são aplicáveis aos delitos cibernéticos no Brasil e, por fim, demonstrar as lacunas legislativas que dificultam a repressão penal de delitos digitais.

A metodologia é qualitativa, foi estruturada a partir de uma extensa pesquisa bibliográfica e documental. Já a análise concentrou-se em textos legais, doutrinas e artigos científicos, destacando-se a legislação nacional atinente aos crimes cibernéticos e à proteção de dados. Assim, esse trabalho incorpora, ainda, a revisão de decisões judiciais e estudos que debruçam-se sobre a eficácia das políticas públicas e a articulação entre os órgãos investigativos e o sistema de justiça.

O trabalho se divide em três seções, na primeira seção, são discutidos os principais desafios à eficácia do direito penal digital, abordando aspectos como coleta, preservação e valoração de provas digitais, bem como as dificuldades decorrentes da jurisdição, na segunda seção trata da jurisdição e competência penal no Brasil, evidenciando como o ordenamento jurídico atua frente à criminalidade digital, e na última seção identifica lacunas legislativas que dificultam a repressão penal de delitos digitais, sugerindo caminhos para o aprimoramento normativo e institucional.

DESAFIOS ENFRENTADOS PELO DIREITO PENAL COM FOCO NA COLETA, PRESERVAÇÃO E VALORAÇÃO DAS PROVAS ELETRÔNICAS

A investigação de crimes cibernéticos impõe desafios singulares em relação aos delitos tradicionais, principalmente devido à natureza altamente volátil das provas digitais. Essas evidências podem ser alteradas, apagadas ou corrompidas em questão de segundos, ao contrário das provas físicas, elas demandam cautela extrema e procedimentos técnicos especializados para que sua validade seja assegurada no âmbito judicial.

Coleta de provas digitais

A coleta de provas digitais envolve dispositivos físicos, como computadores e smartphones, mas também dados armazenados em nuvem, redes sociais e servidores de empresas de tecnologia. É fundamental que essa coleta siga protocolos padronizados, como os estabelecidos pela ABNT NBR ISO/IEC

27037:2013, garantindo a integridade dos dados e evitando nulidades processuais. Além disso, deve respeitar direitos fundamentais do investigado, como a privacidade e o sigilo das comunicações (Castro, 2020; Silva; Oliveira, 2021; Zanoni, 2022).

A coleta de dados envolve não apenas dispositivos físicos, como computadores e smartphones, mas também registros armazenados em servidores na nuvem e redes sociais, que muitas vezes contêm elementos essenciais à investigação. Segundo Zanoni (2022), a análise deve ser abrangente, considerando todos os meios digitais utilizados pelo suspeito, e realizada com ferramentas técnicas capazes de capturar a totalidade das informações sem comprometer a integridade dos dados originais.

É muito importante que a coleta de provas digitais respeite os direitos fundamentais do investigado, como a intimidade, a vida privada e o sigilo das comunicações, previstos no art. 5º da Constituição Federal de 1988. Como destaca Castro (2020), a atuação pericial precisa equilibrar a necessidade de obter provas com a preservação dessas garantias, evitando qualquer abuso que possa comprometer a legitimidade do processo penal. Essa complexidade aumenta ainda mais quando os dados estão espalhados por diferentes países, já que provedores estrangeiros podem estar sujeitos a legislações próprias, tornando o acesso às informações mais difícil. Nesse sentido, Carvalho e Branco (2021) ressaltam que a cooperação internacional é essencial, garantindo que seja possível obter legalmente evidências armazenadas fora do território nacional.

Ferramentas de anonimização e criptografia, como VPNs, Tor e softwares de proteção de dados, representam obstáculos adicionais à coleta de provas. Tais recursos podem ocultar a identidade do autor e dificultar o rastreamento de condutas ilícitas, exigindo técnicas avançadas de perícia e investigação digital (Silva; Oliveira, 2021).

A documentação detalhada de todo o processo de coleta é crítica para assegurar a cadeia de custódia das provas digitais, conforme estabelece o Art. 158-A do Código de Processo Penal, introduzido pela Lei do Pacote Anticrime (Brasil, 2019).

O artigo 158-A do Código de Processo Penal, introduzido pela Lei nº 13.964, de 24 de dezembro de 2019, conhecida como “Pacote Anticrime”, dispõe sobre procedimentos específicos relacionados à coleta de provas digitais, buscando conciliar a efetividade da investigação com a proteção dos direitos fundamentais do investigado (Brasil, 2019).

O STJ tem enfatizado, em decisões sobre crimes cibernéticos, que a validade

das provas digitais depende não apenas de sua existência, mas também do rigor técnico e documental empregado durante a coleta e preservação. Em julgados relacionados à invasão de dispositivos e fraudes eletrônicas, o STJ ressaltou que a ausência de registro preciso de quem realizou a coleta, quando e como ocorreu, pode levar à nulidade da prova, comprometendo a instrução processual. Esse entendimento foi reafirmado no julgamento do Recurso Especial nº 1.977.658/SP, em que a Corte destacou que a integridade das evidências digitais deve ser comprovada mediante documentação adequada de toda a cadeia de custódia, sob pena de violação do devido processo legal (Brasil, 2022).

O STJ é categórico ao descrever a importância de procedimentos periciais padronizados na coleta de provas digitais, e isso evidencia que a aceitação dessas evidências em juízo está condicionada tanto à sua materialidade quanto ao rigor técnico e documental aplicado durante o processo de coleta (Brasil, 2022).

O Tribunal, em julgados envolvendo invasão de dispositivos eletrônicos e fraudes informáticas, alertou que a omissão de um registro exato (detalhando o responsável, o momento e o método da coleta) é capaz de prejudicar a instrução processual, podendo invalidar a prova.

Nesses julgados, o tribunal reforça que a coleta deve seguir normas técnicas, como a ABNT NBR ISO/IEC 27037:2013, que orientam justamente sobre a identificação, a coleta, a aquisição e sobre a preservação de evidências digitais, garantindo que sejam reconhecidas como válidas em juízo. Dessa maneira, o STJ enfatiza que é necessário equilibrar a urgência investigativa com a preservação dos direitos constitucionais, estabelecendo parâmetros práticos para a condução de investigações de delitos cibernéticos no Brasil.

A legislação brasileira, apesar de prever a guarda de registros por provedores de internet, apresenta limitações quanto à abrangência e à temporalidade desses dados. O Marco Civil da Internet estabelece a retenção mínima de seis meses, o que frequentemente é insuficiente para investigações complexas que demandam maior tempo para análise e requisição judicial (Brasil, 2014).

Por isso, a capacitação de profissionais envolvidos na coleta de provas digitais é determinante para a eficácia das investigações, já que muitos erros operacionais e técnicos decorrem da falta de treinamento adequado, o que compromete a qualidade das evidências. Conforme Castro (2020) reforça, que a formação contínua de peritos e agentes públicos deve acompanhar o ritmo das

transformações tecnológicas para garantir a eficiência da coleta. Essa cooperação entre órgãos públicos e plataformas privadas também é essencial, pois as empresas de tecnologia detêm informações cruciais para a investigação, e a ausência de protocolos claros de comunicação pode atrasar a obtenção de dados ou até inviabilizá-la.

Segundo Carvalho e Branco (2021), os mecanismos de cooperação público-privada são estratégicos para ampliar o alcance das investigações e agilizar o acesso às provas. Então, por fim, a coleta de provas digitais exige equilíbrio entre celeridade e legalidade. Enquanto a urgência investigativa demanda rapidez na obtenção de dados, é imprescindível que todos os procedimentos respeitem a legislação e os direitos constitucionais, a prática adequada da coleta digital fortalece a confiabilidade do processo penal e contribui para a efetiva responsabilização dos autores de delitos cibernéticos (Silva; Oliveira, 2021; Zanoni, 2022).

Preservação de provas digitais

Segundo Zanoni (2022), a preservação envolve medidas técnicas que assegurem a imutabilidade do conteúdo, incluindo o armazenamento seguro, a criação de cópias forenses e o registro detalhado de todos os procedimentos realizados durante a investigação. A preservação das provas digitais é uma etapa muito essencial para que garanta que as informações coletadas permanecerão íntegras até o momento da análise e apresentação em juízo, já que essa natureza volátil dos dados eletrônicos, que podem ser apagados ou modificados de forma involuntária ou intencional, o que torna essa etapa particularmente crítica.

O Marco Civil da Internet estabelece diretrizes para a guarda de registros de conexão e de acesso a aplicações, obrigando os provedores a manterem essas informações por um período mínimo de seis meses. Contudo, estudiosos alertam que esse prazo revela-se insuficiente para a complexidade e a duração das investigações de crimes cibernéticos. Assim, a lacuna é ainda mais evidente em casos que envolvem cooperação internacional ou a análise de um grande volume de dados (Mello, 2019).

A preservação dessas provas digitais no Brasil deve observar não apenas os dispositivos do Marco Civil, mas também legislações mais recentes que complementam a regulamentação sobre crimes cibernéticos e proteção de dados. Além disso, a Lei nº 14.811, de 11 de setembro de 2024, que dispõe sobre a

tipificação do bullying e do cyberbullying, estabelece responsabilidades penais específicas para atos cometidos por meio digital, reforçando a necessidade de alinhamento entre a coleta de dados, a legislação e a proteção dos direitos dos indivíduos (Brasil, 2024).

O Decreto nº 11.491, de 24 de agosto de 2023, que promulgou a Convenção sobre Cibercrime de Budapeste, institui normas de cooperação internacional para a investigação de delitos cibernéticos, incluindo acesso ilegal a sistemas e fraude informática, reforçando a importância de alinhamento entre procedimentos investigativos e regulamentação internacional (Brasil, 2023). Essas normas reforçam a importância da preservação adequada de dados digitais, garantindo que as evidências possam ser utilizadas de forma legítima e segura em processos judiciais, respeitando princípios como a legalidade, a integridade da prova e a proteção dos direitos fundamentais (Carvalho; Branco, 2021; Zanoni, 2022).

A utilização de cópias forenses, aliada à geração de códigos hash, permite comprovar que os arquivos originais não foram alterados desde a coleta. Zanoni (2022) enfatiza que tais procedimentos são fundamentais não apenas para garantir a autenticidade, mas também para permitir que múltiplos peritos possam analisar os dados de forma independente, sem comprometer a integridade da prova original.

Além disso, a preservação dos dados exige cuidados rigorosos tanto no seu aspecto físico quanto lógico, pois os dispositivos eletrônicos, por exemplo, devem ser acondicionados de modo a evitar danos causados por fatores externos, como variações de temperatura, umidade ou interferência magnética, que podem corromper as evidências. Igualmente essencial é a manutenção de backups redundantes em sistemas seguros, garantindo que falhas em um local não comprometam a investigação (Castro, 2020).

Existe ainda mais um obstáculo, que reside na cooperação entre autoridades e provedores de serviços, especialmente quando os dados cruciais para a investigação estão armazenados fora do território nacional. Segundo destacam Carvalho e Branco (2021), a preservação ultrapassa os procedimentos técnicos internos; ela depende da capacidade de solicitar e obter informações de empresas estrangeiras de forma legal e tempestiva, respeitando os acordos internacionais e legislações específicas. Por essa razão, a cadeia de custódia assume um papel central na preservação das provas: cada movimentação, análise ou cópia do dado deve ser minuciosamente registrada, identificando o responsável e a data da

operação.

De acordo com Silva e Oliveira (2021), essas falhas na documentação da cadeia de custódia podem levar à contestação da prova e, em casos extremos, à sua exclusão do processo, prejudicando a persecução penal.

A rapidez na preservação das provas é outro ponto crucial. Dados digitais podem ser alterados ou apagados automaticamente por sistemas operacionais, aplicativos ou pelo próprio usuário, o que exige que as equipes periciais adotem procedimentos céleres desde o momento da apreensão até a análise. Nesse sentido, Castro (2020) reforça que a demora nesse processo compromete não apenas a validade da prova, mas também a eficácia da investigação como um todo.

Pois a complexidade aumenta quando se trata de evidências armazenadas em ambientes de nuvem, serviços de armazenamento distribuído ou aplicativos móveis. A obtenção desses dados depende do acesso autorizado por provedores e da compatibilidade entre sistemas, que exige planejamento e conhecimento técnico aprofundado. Por isso Zanoni (2022) argumenta que a preservação em ambientes digitais complexos requer protocolos adaptativos que contemplem diferentes cenários tecnológicos.

A legislação brasileira ainda apresenta lacunas quanto à regulamentação detalhada da preservação de dados digitais. A Lei do Pacote Anticrime reforça a importância da cadeia de custódia, mas não detalha procedimentos técnicos específicos, deixando a cargo das normas técnicas e da jurisprudência a definição de boas práticas (Brasil, 2019).

A capacitação contínua de peritos e profissionais do sistema de justiça é determinante para a preservação adequada das provas digitais. Nesse sentido, Castro (2020) destaca que erros operacionais, como a abertura de arquivos sem registro ou a manipulação inadequada de dispositivos, podem comprometer a integridade das evidências, tornando a formação técnica e a atualização constante requisitos essenciais.

Além disso, a preservação deve considerar aspectos éticos e legais relacionados à privacidade e proteção de dados pessoais. A LGPD estabelece limites sobre o tratamento de informações pessoais, exigindo que a preservação seja realizada de forma proporcional, necessária e adequada, garantindo que a investigação não viole direitos fundamentais (Brasil, 2018; Carvalho; Branco, 2021).

Por fim, a preservação de provas digitais não é um fim isolado, mas parte de

um ciclo investigativo que inclui coleta, análise e valoração. Sua eficácia depende da integração entre procedimentos técnicos, normas legais e protocolos de documentação, garantindo que os dados possam ser utilizados de forma confiável em processos judiciais e contribuindo para a efetiva responsabilização dos autores de crimes cibernéticos (Silva; Oliveira, 2021; Zanoni, 2022).

Valoração de provas digitais

A valoração das provas digitais é um grande desafio para o direito penal atual, pois envolve não apenas a análise de sua autenticidade, envolve também a sua relevância e a sua suficiência para a formação da convicção do magistrado. Totalmente diferente das provas físicas, os vestígios digitais demandam interpretação técnica e jurídica, considerando que o contexto, a integridade e a origem dos dados podem influenciar muito sua credibilidade (Galdino, 2021).

O princípio da proporcionalidade é fundamental na valoração das provas digitais, já que a investigação pode implicar na análise de informações sensíveis, incluindo dados pessoais e comunicações privadas. Nesse sentido, os juízes precisam equilibrar o interesse público na persecução penal com a proteção de direitos fundamentais, garantindo que a obtenção e a utilização das provas digitais não ultrapassem limites legais estabelecidos pela Constituição e pela LGPD (Brasil, 2018; Carvalho; Branco, 2021).

A interpretação da prova digital requer conhecimentos técnicos especializados, magistrados e operadores do direito frequentemente dependem do parecer de peritos para compreender a complexidade de arquivos, logs, metadados e registros de sistemas. Galdino (2021) enfatiza que, sem a participação de profissionais capacitados, há risco de erro na valoração, que pode resultar em decisões judiciais equivocadas ou injustas.

A autenticidade da prova é elemento central na sua valoração. Para que um dado eletrônico seja considerado confiável, é necessário comprovar que ele não foi alterado desde sua coleta. Técnicas como a utilização de cópias forenses, geração de hashes e documentação da cadeia de custódia contribuem para fortalecer a credibilidade da prova digital em juízo (Zanoni, 2022).

A jurisprudência brasileira tem reconhecido a importância da valoração adequada das provas digitais, destacando que falhas na cadeia de custódia ou na documentação do processo de coleta podem comprometer a admissibilidade do

material. O STJ tem reiterado que a demonstração clara de como a prova foi obtida e preservada é indispensável para garantir sua aceitação nos processos penais, a exemplo do Recurso Especial nº 1.977.658/SP, em que a Corte reafirmou que a integridade das evidências digitais deve ser comprovada mediante documentação completa da cadeia de custódia, sob pena de nulidade da prova (Brasil, 2022).

Outro desafio consiste na verificação da relevância e suficiência da prova digital, nem todo dado coletado possui valor probatório significativo. Pois cabe ao perito e ao juiz avaliar se os elementos apresentados contribuem efetivamente para esclarecer os fatos e comprovar a autoria do delito, evitando decisões baseadas em informações irrelevantes ou fragmentadas (Castro, 2020).

A valoração também envolve a análise do contexto tecnológico em que a prova foi produzida. Por exemplo, logs de sistemas ou registros de rede podem indicar uma ação suspeita, mas é necessário interpretar esses dados considerando o funcionamento dos sistemas, padrões de operação e possibilidade de falhas técnicas. Segundo Silva e Oliveira (2021), a compreensão adequada do contexto evita equívocos e fortalece a confiabilidade do juízo sobre a prova digital.

A transparência e a documentação detalhada de todas as etapas do processo de coleta e preservação são indispensáveis para a valoração da prova. Cada ação tomada durante a investigação deve ser registrada, permitindo que advogados, magistrados e peritos possam verificar a integridade do material e a legalidade dos procedimentos adotados (Zanoni, 2022).

Em casos complexos de crimes cibernéticos envolvendo múltiplas jurisdições, a valoração das provas digitais exige ainda cooperação internacional. A obtenção de dados armazenados em servidores estrangeiros deve seguir protocolos legais específicos, garantindo que a prova seja aceita tanto no país de origem quanto no Brasil, sem comprometer direitos fundamentais ou normas de proteção de dados (Carvalho; Branco, 2021).

A valoração da prova digital deve sempre considerar o risco de manipulação ou adulteração por terceiros, como crimes cibernéticos frequentemente envolvem ataques a sistemas, o uso de *malwares* ou a alteração de registros, é imprescindível uma análise técnica detalhada para validar a autenticidade dos elementos apresentados.

Galdino (2021) frisa que a perícia tem o papel de identificar indícios de adulteração, impedindo que informações falsas influenciem decisões judiciais. Além

dessa verificação técnica, o aspecto legal da valoração exige que os magistrados considerem precedentes e as normas aplicáveis, como o Código de Processo Penal, o Marco Civil e a LGPD. Essa aplicação consistente desses dispositivos garante uniformidade na análise da prova digital e fortalece a segurança jurídica, evitando interpretações divergentes (Brasil, 2018; Silva; Oliveira, 2021).

Portanto, essa valoração das provas digitais representa, também, a etapa de um ciclo que envolve tanto a coleta, quanto a preservação e a análise, portanto, sua eficácia depende da integração entre procedimentos técnicos, normas legais e princípios da constituição, que asseguram que os dados sejam utilizados de forma confiável em processos judiciais. Já que essa correta valoração fortalece a persecução penal, protege direitos fundamentais e contribui para a responsabilização adequada dos autores de delitos cibernéticos (Zanoni, 2022; Castro, 2020).

JURISDIÇÃO, COMPETÊNCIA PENAL NO ENFRENTAMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL

A jurisdição representa o poder-dever do Estado de aplicar o direito no âmbito de seu território e em relação às pessoas nele situadas. No contexto dos crimes cibernéticos, esse conceito encontra desafios significativos, pois as condutas ilícitas podem ser praticadas em um país e gerar efeitos em outro.

Jurisdição

Como observa Greco (2020), a transnacionalidade dos delitos digitais dificulta a aplicação do princípio clássico da territorialidade previsto no art. 5º do Código Penal brasileiro, exigindo soluções jurídicas mais flexíveis. A internet, por sua própria estrutura descentralizada, rompe com a lógica tradicional da jurisdição vinculada ao espaço físico. Assim, um crime pode ser cometido em múltiplos lugares ao mesmo tempo, gerando dúvidas quanto ao foro competente. Segundo Bitencourt (2021), a ubiquidade dos atos digitais torna insuficiente a aplicação isolada do critério territorial, sendo necessária a adoção de princípios complementares, como o da defesa e o da nacionalidade.

A jurisprudência brasileira tem enfrentado situações em que a definição da jurisdição se mostra controversa. O STJ já reconheceu que crimes cometidos pela internet podem ser julgados tanto no local da conduta quanto no local do resultado,

adotando uma interpretação ampliada do art. 70 do Código de Processo Penal (Brasil, 2020). Essa postura busca compatibilizar o direito processual penal com as peculiaridades da criminalidade virtual.

O princípio da ubiquidade, que é previsto no art. 6º do Código Penal, é um dos mais aplicados para dirimir conflitos de jurisdição em crimes cibernéticos, pois esse princípio considera que o crime se consuma tanto no lugar da ação quanto no lugar do resultado, permitindo que o Estado brasileiro exerça sua jurisdição em casos em que o delito tenha efeitos no território nacional, ainda que praticado a distância. Portanto, a aplicação desse princípio encontra respaldo em casos práticos, como por exemplo, os de fraudes eletrônicas em que a vítima está no Brasil, mas o autor opera em outro país. Por isso, a jurisdição nacional se estabelece pelo local onde ocorreu o resultado, ou seja, o prejuízo patrimonial da vítima (Brasil, 1940).

Greco (2020) destaca que tal interpretação é essencial para garantir a efetividade da tutela penal no ciberespaço. Contudo, a jurisdição nacional enfrenta limitações quando não existe a cooperação internacional, pois em situações em que o autor reside em país estrangeiro e não há tratado de extradição ou acordo de auxílio jurídico mútuo, o exercício da jurisdição brasileira pode se tornar ineficaz, mesmo quando o resultado do crime ocorre em território nacional (Mello, 2019).

Outro aspecto relevante é a jurisdição em relação a crimes cibernéticos que afetam bens jurídicos difusos, como ataques a infraestruturas críticas e sistemas de interesse coletivo. Nessas hipóteses, há uma sobreposição de interesses estatais que exige interpretação ampliada das regras de jurisdição, especialmente diante da interconexão global dos sistemas de informação (Carvalho; Branco, 2021).

Conforme Bitencourt (2021), diz que, sem essa adaptação, a jurisdição se torna meramente formal, incapaz de dar respostas adequadas às demandas da sociedade digital. Além disso, essa aplicação da jurisdição em crimes digitais deve respeitar princípios constitucionais, como o devido processo legal e o juiz natural. Nesse sentido, a expansão da jurisdição não pode ocorrer de forma arbitrária, devendo estar fundamentada em regras legais e em garantias processuais que assegurem a legitimidade da atuação estatal (Greco, 2020).

Ou seja, a jurisdição em crimes cibernéticos exige uma releitura dos princípios tradicionais do Direito Penal e Processual Penal, visando compatibilizá-los com as particularidades inerentes à internet. Desse modo, a conjugação do princípio da

ubiquidade com a cooperação internacional e com mecanismos jurídicos inovadores configura-se como caminho indispensável. Tal estratégia permite ao Estado exercer, de forma eficaz, seu poder jurisdicional sobre delitos perpetrados no ambiente digital (Bitencourt, 2021; Brasil, 2022).

Competência Penal no enfrentamento de crimes cibernéticos

O enfrentamento dos crimes cibernéticos no Brasil apresenta desafios significativos no que tange à jurisdição e à competência penal, sobretudo devido à natureza dinâmica e difusa desses delitos. A jurisdição penal brasileira precisa, assim, lidar com a complexidade de determinar o órgão competente para investigar, processar e julgar ilícitos digitais. Tal dificuldade se intensifica ao considerar que esses crimes podem envolver múltiplos estados da Federação ou agentes localizados em regiões distintas do território nacional.

Segundo Bitencourt (2023), essa transnacionalidade virtual que ocorre dentro do espaço nacional exige uma interpretação mais flexível dos critérios de territorialidade previstos no Código Penal brasileiro, o que nem sempre se mostra suficiente para garantir uma resposta eficaz. Além disso, essa definição de competência penal enfrenta obstáculos práticos e legais pois a Lei Carolina Dieckmann, tipifica a invasão de dispositivos informáticos, mas não detalha expressamente os critérios de competência entre varas criminais estaduais e federais.

Segundo Greco (2023), essa lacuna provoca insegurança jurídica e atrasos processuais, já que autoridades investigativas podem divergir sobre qual instância deve conduzir o processo, prejudicando a eficiência da persecução penal. Além disso, a identificação do agente criminoso, visto que, muitas vezes, a autoria de delitos digitais é ocultada ou mascarada. Tal fato dificulta a delimitação territorial do crime e, por conseguinte, a definição da jurisdição competente. Pinheiro (2022) alerta que, sem o apoio de ferramentas técnicas avançadas e de perícia digital especializada, o processo penal brasileiro enfrenta limitações significativas na instrução probatória. Isso compromete a responsabilização dos agentes e, consequentemente, a aplicação efetiva da lei.

A competência penal em casos de crimes cibernéticos no Brasil também se encontra afetada pela diversidade normativa entre os estados e pela centralização limitada de recursos especializados. Souza (2021) aponta que grande parte das

unidades policiais e do Ministério Público carece de infraestrutura tecnológica adequada, o que impede a realização de investigações rápidas e eficazes, especialmente quando o delito envolve sistemas complexos ou múltiplas vítimas.

Além disso, a multiplicidade de tipos penais aplicáveis a crimes digitais, desde fraudes eletrônicas, crimes contra a honra, invasão de dispositivos e estelionato digital, exige uma articulação clara entre instâncias estaduais e federais. Bitencourt (2023) destaca que, sem regulamentação mais específica sobre a distribuição de competência, ocorre uma fragmentação na investigação e no julgamento, resultando em morosidade processual e insegurança jurídica para vítimas e operadores do direito.

A coordenação entre órgãos é outro ponto crucial. A Polícia Federal, responsável por investigar crimes que envolvem sistemas críticos ou prejuízos de relevância nacional, muitas vezes atua em conjunto com polícias civis estaduais, porém a ausência de protocolos padronizados para encaminhamento de casos dificulta a definição da competência inicial. Greco (2023) enfatiza que a falta de uniformidade nos procedimentos compromete a eficácia penal e favorece a impunidade.

Outro aspecto relevante é a adequação do Código de Processo Penal frente à prova digital, uma vez que a competência para análise de dados armazenados em nuvem, dispositivos eletrônicos ou servidores de terceiros ainda carece de regulamentação detalhada, sendo necessária a atuação coordenada de juízes, promotores e peritos digitais para garantir a validade jurídica das provas. Pinheiro (2022) reforça que a ausência de padronização aumenta o risco de nulidades processuais, comprometendo a responsabilização do agente.

O avanço da criminalidade digital exige também maior capacitação dos magistrados e promotores, pois essa interpretação da legislação penal brasileira em face de novas condutas exige conhecimento técnico específico, não contemplado suficientemente na formação tradicional. Por isso, Souza (2021) diz que cursos de atualização e especialização em direito digital são imprescindíveis para assegurar decisões coerentes e alinhadas à realidade tecnológica.

A aplicação de princípios como o da territorialidade e o da especialidade, previstos no Código Penal, precisa ser reinterpretada à luz do ambiente virtual, considerando que o local do crime nem sempre coincide com o local do agente ou da vítima. Bitencourt (2023) ressalta que essa adaptação é fundamental para

garantir segurança jurídica e efetividade na persecução penal de crimes cibernéticos no Brasil.

Por fim, a jurisprudência brasileira tem buscado preencher lacunas, definindo critérios para a competência e jurisdição em casos específicos de delitos digitais. Assim, Greco (2023) enfatiza que decisões recentes reforçam a necessidade de centralização de procedimentos complexos em varas especializadas ou fóruns com capacidade técnica, garantindo celeridade e qualidade na instrução processual. Contudo, ainda há muito espaço para regulamentação complementar e aprimoramento institucional, a fim de tornar o enfrentamento dos crimes cibernéticos mais eficiente e seguro para todos os envolvidos.

LACUNAS LEGISLATIVAS QUE DIFICULTAM A REPRESSÃO PENAL DE DELITOS DIGITAIS

O enfrentamento dos crimes cibernéticos no Brasil é prejudicado por lacunas legislativas, que geram incerteza jurídica e dificultam a atuação eficiente das autoridades competentes, entre essas lacunas mais relevantes está a insuficiência de normativas para crimes relacionados a ataques cibernéticos complexos, a invasão de sistemas críticos, a fraude digital e, também, a violação de dados pessoais.

Lacunas legislativas

Embora existam dispositivos legais específicos, como a Lei Carolina Dieckmann e o Marco Civil da Internet, muitas modalidades de delitos digitais não encontram tipificação clara no Código Penal, o que limita a repressão penal e favorece a impunidade (Bitencourt, 2023).

Segundo Greco (2023), a legislação atual ainda não contempla adequadamente a sofisticação tecnológica dos crimes digitais, tornando difícil a aplicação do princípio da legalidade penal, que exige tipificação prévia e precisa da conduta criminosa

Além disso, a ausência de regras detalhadas sobre a competência e a jurisdição para casos que envolvem múltiplos estados brasileiros cria incertezas processuais. Pinheiro (2022) destaca que, sem critérios claros de territorialidade, autoridades podem divergir quanto à instância competente, gerando atrasos na investigação e no julgamento. Essa indefinição compromete a eficácia do sistema

penal e afeta diretamente a proteção das vítimas.

Mais um ponto crítico é a regulamentação insuficiente sobre provas digitais, já que o Código de Processo Penal e a legislação vigente não detalham procedimentos específicos para coleta, preservação e valoração de evidências digitais, o que pode acarretar nulidades processuais. Nesse sentido, Souza (2021) afirma que a falta de normatização uniforme e de protocolos claros para perícia digital aumenta a insegurança jurídica e dificulta a responsabilização de criminosos digitais.

A legislação brasileira também não prevê expressamente condutas como o uso de *malware*, *ransomwares*, *deepfakes* ou crimes cometidos via inteligência artificial, que têm se tornado cada vez mais comuns. De acordo com Peck (2022), essa lacuna legislativa impede que o direito penal acompanhe a velocidade das inovações tecnológicas, criando um descompasso entre a criminalidade e os instrumentos jurídicos disponíveis.

Além das lacunas na tipificação, há fragilidades em relação à proteção de dados e privacidade. Apesar da LGPD, que trouxe avanços significativos, ainda existem desafios na integração dessa norma com o direito penal, especialmente quanto à responsabilização de agentes e empresas por incidentes digitais. Greco (2023) ressalta que a ausência de regulamentação complementar dificulta a aplicação prática das normas e a proteção efetiva dos direitos dos cidadãos, pois a falta de uniformidade legislativa entre normas estaduais e federais também contribui para a complexidade do enfrentamento penal de delitos digitais.

Bitencourt (2023) observa que, enquanto alguns estados têm regulamentações específicas sobre crimes digitais, a coexistência de normas fragmentadas cria dificuldades interpretativas e divergências processuais, prejudicando a coerência da atuação penal no território nacional. Além disso, a legislação penal brasileira ainda carece de incentivos à capacitação de profissionais e à criação de estruturas especializadas.

Já Souza (2021) enfatiza que, sem regulamentação que preveja investimentos em tecnologia, treinamento e unidades especializadas, mesmo crimes tipificados podem não ser investigados de forma eficiente, reforçando a sensação de impunidade.

Outro problema relevante é a ausência de mecanismos claros para cooperação entre órgãos públicos e setor privado, especialmente em casos que envolvem empresas de tecnologia, provedores de internet e plataformas digitais.

Pinheiro (2022) aponta que a inexistência de diretrizes legislativas prejudica o acesso rápido a informações essenciais para a investigação e a repressão de delitos cibernéticos.

Portanto, é evidente que a modernização legislativa é urgente, visto que, a atualização constante das normas, a criação de tipificações específicas para novas modalidades de crimes digitais e a regulamentação detalhada de procedimentos probatórios são medidas essenciais para tornar o direito penal brasileiro mais eficaz e alinhado à realidade tecnológica atual. Pois a superação dessas lacunas permitirá não apenas maior proteção às vítimas, mas também maior segurança jurídica para operadores do direito e mais eficiência na persecução penal (Peck, 2022; Greco, 2023; Bittencourt, 2023).

CONSIDERAÇÕES FINAIS

Diante da análise desenvolvida ao longo do trabalho, foi constatado que o avanço tecnológico e a expansão do ambiente digital impõem ao Direito Penal brasileiro desafios inéditos e complexos. Uma vez que a criminalidade cibernética, marcada por sua transnacionalidade, pelo anonimato e pela sofisticação técnica. O que evidencia as limitações estruturais, normativas e operacionais do sistema penal, especialmente no que se refere à tipificação adequada das condutas, à coleta e preservação das provas digitais e à efetiva cooperação entre instituições e países.

A partir da discussão dos temas abordados como jurisdição, competência penal, cooperação internacional e valoração das provas digitais, verificou-se que, embora o ordenamento jurídico brasileiro possua marcos legais importantes, como o Marco Civil da Internet e a lei Carolina Dieckmann, ainda persiste uma defasagem significativa entre a evolução tecnológica e a capacidade de resposta jurídica. A ausência de instrumentos técnicos uniformizados e a carência de capacitação de profissionais do direito e da segurança pública contribuem para a morosidade e ineficiência na persecução penal desses delitos.

Sob uma perspectiva mais otimista, observam-se importantes melhorias: a adesão à Convenção de Budapeste sobre o Cibercrime, as discussões legislativas em curso e o fortalecimento da cooperação internacional representam avanços cruciais para alinhar o Brasil às melhores práticas globais. Soma-se a isso a integração entre órgãos investigativos, o investimento em tecnologia forense e a criação de políticas públicas focadas em educação digital, medidas essenciais para

reduzir a vulnerabilidade cibernética e ampliar a eficácia penal.

A valoração da prova digital exige critérios técnicos rigorosos e observância estrita às normas jurídicas, considerando a complexidade e a volatilidade dos dados eletrônicos. Para que esses elementos sejam reconhecidos como meios probatórios legítimos, é indispensável que a cadeia de custódia seja preservada, que os métodos de coleta sejam transparentes e reprodutíveis, e que as análises periciais sigam padrões consolidados. Além disso, a natureza transnacional dos delitos cibernéticos demanda uma jurisdição capaz de dialogar com diferentes sistemas legais, garantindo cooperação internacional eficaz. Nesse contexto, o fortalecimento da legislação específica e a uniformização de protocolos periciais tornam-se essenciais para assegurar a confiabilidade, a eficácia e a segurança jurídica no tratamento das provas digitais.

Em conclusão, o enfrentamento dos crimes cibernéticos exige não apenas aperfeiçoamento normativo, mas também uma mudança estrutural e cultural no sistema de justiça criminal. Pois a consolidação de um ambiente jurídico mais adaptável, dinâmico e interdisciplinar é indispensável para garantir a tutela efetiva dos direitos fundamentais e da segurança digital dos cidadãos. Desse modo, o Direito Penal deve evoluir em harmonia com a inovação tecnológica, preservando seus princípios, mas assumindo uma postura mais proativa e cooperativa diante das novas realidades do ciberespaço.

REFERÊNCIAS

BITENCOURT, Cezar. **Direito penal e crimes cibernéticos: desafios contemporâneos**. 3. ed. São Paulo: Saraiva, 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 out. 2025.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 1 out. 2025.

BRASIL. **Decreto nº 11.491, de 9 de maio de 2023**. Promulga a Convenção sobre o Crime Cibernético, conhecida como Convenção de Budapeste, firmada em 23 de novembro de 2001. Diário Oficial da União, Brasília, DF, 10 maio 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm.

Acesso em: 6 out. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 6 out. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 out. 2025.

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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 6 out. 2025.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019.** Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime). Diário Oficial da União, Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 6 out. 2025.

BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, e a Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para tipificar os crimes de bullying e cyberbullying, e dá outras providências. Diário Oficial da União, Brasília, DF, 15 jan. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2024/Lei/L14811.htm. Acesso em: 6 out. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.977.658/SP. Relator: Ministro Ribeiro Dantas.** Brasília, DF, julgado em 10 maio 2022. Diário da Justiça Eletrônico, Brasília, DF, 16 maio 2022. Disponível em: <https://www.stj.jus.br>. Acesso em: 29 out. 2025.

CARVALHO, Ana Paula; BRANCO, Ricardo. Proteção de dados e privacidade: desafios na investigação criminal digital. **Revista de Direito Digital**, São Paulo, v. 7, n. 2, p. 45-62, 2021.

CASTRO, Lucas. **Perícias digitais e criminalidade cibernética: desafios na coleta, preservação e valoração das provas.** Rio de Janeiro: Forense, 2020.

GALDINO, Mariana. Valoração de provas digitais no direito penal brasileiro. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 9, n. 3, p. 112-130, 2021.

GRECO, Rogério. **Direito penal contemporâneo e crimes cibernéticos: análise da jurisdição e competência.** 2. ed. São Paulo: Método, 2023.

MELLO, Fernanda. Investigação digital e cooperação internacional: desafios da criminalidade cibernética. **Revista de Direito Penal e Processual Penal**, Curitiba, v. 15, n. 1, p. 55-74, 2019.

PALO ALTO NETWORKS. **Brazil is the most vulnerable country to hacker attacks in Latin America for the 3rd consecutive year, according to research**. TI Inside Online, 12 mar. 2024. Disponível em: <https://tiinside.com.br/en/12/03/2024/brasil-e-o-pais-mais-vulneravel-a-ataques-hackers-na-al-pelo-3o-ano-consecutivo-segundo-pesquisa/>. Acesso em: 20 out. 2025.

PECK, Jonathan. Lacunas legislativas e criminalidade digital: uma análise comparativa. **Revista de Direito e Tecnologia**, Rio de Janeiro, v. 4, n. 2, p. 78-95, 2022.

PINHEIRO, Ricardo. **Competência penal em delitos cibernéticos: estudo sobre jurisdição e provas digitais**. São Paulo: RT, 2022.

SILVA, Mariana; OLIVEIRA, Tiago. **Coleta, preservação e valoração de provas digitais: fundamentos e desafios**. Belo Horizonte: Del Rey, 2021.

STJ – SUPERIOR TRIBUNAL DE JUSTIÇA. **Jurisprudência sobre crimes cibernéticos e provas digitais**. Brasília, DF: STJ, 2020-2022. Disponível em: <https://www.stj.jus.br>. Acesso em: 6 out. 2025.

ZANONI, Felipe. **Evidências digitais e processo penal: técnicas e protocolos de perícia**. Curitiba: Juruá, 2022.

3 CONSIDERAÇÕES FINAIS

O presente estudo analisou a eficácia do sistema penal brasileiro no combate aos crimes cibernéticos, concluindo que o sistema se encontra em evolução forçada, mas ainda carente de sincronia com a realidade tecnológica. As principais descobertas apontam que a vulnerabilidade da cadeia de custódia da prova digital, a indefinição nos critérios de competência penal e as persistentes lacunas legislativas representam as maiores barreiras para a repressão penal. Em síntese, o enfrentamento eficaz da criminalidade cibernética exige mais do que aperfeiçoamento normativo; demanda uma transformação estrutural e cultural no sistema de justiça. A consolidação de um ambiente jurídico mais adaptável, dinâmico e interdisciplinar é fundamental para garantir a tutela dos direitos e da segurança digital. Portanto, o Direito Penal deve urgentemente investir em capacitação, cooperação e modernização normativa, assumindo uma postura proativa frente ao ciberespaço.

REFERÊNCIAS

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal.** Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 6 out. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 out. 2025.

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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 6 out. 2025.

PALO ALTO NETWORKS. **Brazil is the most vulnerable country to hacker attacks in Latin America for the 3rd consecutive year, according to research.** TI Inside Online, 12 mar. 2024. Disponível em: <https://tiinside.com.br/en/12/03/2024/brasil-e-o-pais-mais-vulneravel-a-ataques-hackers-na-al-pelo-3o-ano-consecutivo-segundo-pesquisa/>. Acesso em: 20 out. 2025.

ANEXO A - COMPROVANTE DE SUBMISSÃO

20:31




Revista de Direito UNINOVAF...



← Back to Submissões

Me. Viviane Maria de Pádua Rios Magalhães

Contato principal para correspondência editorial.

Sem ORCID informado

E-mail: viviane.rios@afya.com.br

220	CRIMES CIBERNÉTICOS NO BRASIL: Desafios para o direito penal na era digital	Em fila
223	ANÁLISE DA (IN) EFICIÊNCIA DO MÉTODO APAC (ASSOCIAÇÃO DE PROTEÇÃO E ASSISTÊNCIA AOS CONDENADOS) EM FACE À RESSOCIALIZAÇÃO DOS CONDENADOS	Em fila
228 ¹	A REVITIMIZAÇÃO DE MULHERES EM CONTEXTO DE VIOLÊNCIA SEXUAL NO SISTEMA DE JUSTIÇA DO PIAUÍ	Em fila

Página(s) >> 1

uninovafapi.emnuvens.com.br

