Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i11.22598

CIBERCRIMES E FRAUDES EM REDES SOCIAIS: O DESAFIO DO DIREITO PENAL E A IMPORTÂNCIA DA PERÍCIA DIGITAL FORENSE[1]

CYBERCRIMES AND FRAUD ON SOCIAL NETWORKS: THE CHALLENGE OF CRIMINAL LAW AND THE IMPORTANCE OF DIGITAL FORENSIC EXPERTISE

Franceilton Silva Nacimento[2]
Josué Barbosa Andrade[3]
Juliano de Oliveira Leonel[4]

RESUMO: A crescente digitalização das relações sociais e o uso intensivo das redes sociais têm impulsionado o aumento dos cibercrimes e das fraudes digitais, desafiando a atuação do Direito Penal brasileiro. Este artigo tem como objetivo geral analisar a atuação da perícia digital forense como instrumento de efetivação da justiça penal frente aos crimes cibernéticos cometidos em redes sociais. A pesquisa justifica-se pela relevância social e jurídica do tema, diante da necessidade de fortalecer os mecanismos de investigação e responsabilização penal no ambiente virtual. Metodologicamente, trata-se de uma pesquisa qualitativa, com abordagem bibliográfica e documental, fundamentada em autores como Peck (2021), Teixeira (2022), Cunha (2009), entre outros, além da análise de jurisprudência do Superior Tribunal de Justiça. Os resultados apontam que a perícia digital é essencial para a coleta, preservação e análise de provas técnicas, contribuindo significativamente para a responsabilização dos infratores e para a construção de um ambiente digital mais seguro. Conclui-se que a efetividade da justiça penal na era digital depende da valorização da prova técnica, da capacitação dos operadores do Direito e da integração entre os órgãos de segurança pública, o Poder Judiciário e as plataformas digitais. A atuação da perícia digital forense, portanto, representa um avanço necessário para enfrentar os desafios impostos pela criminalidade informacional, promovendo a proteção dos direitos fundamentais e a credibilidade do sistema penal.

Palavras- Chave: Cibercrimes. Redes sociais. Perícia digital forense. Direito Penal.Segurança digital.

ABSTRACT: The increasing digitalization of social relations and the intensive use of social networks have driven the rise of cybercrimes and digital fraud, challenging the effectiveness of Brazilian Criminal Law. This article aims to analyze the role of digital forensic expertise as an instrument for ensuring criminal justice in cases of cybercrimes committed on social networks. The research is justified by its social and legal relevance, given the need to strengthen mechanisms for investigation and criminal accountability in the virtual environment. Methodologically, this is a qualitative study based on bibliographic and documentary research, supported by authors such as Peck (2021), Teixeira (2022), and Cunha (2009), as well as case law from the Superior Court of Justice. The findings indicate that digital forensics is essential for collecting, preserving, and analyzing technical evidence, significantly contributing to the accountability of offenders and the construction of a safer digital environment. It is concluded that the effectiveness of criminal justice in the digital era depends on valuing technical evidence, training legal professionals, and promoting integration among law enforcement agencies, the judiciary, and digital platforms. Therefore, digital forensic expertise represents a necessary advancement to address the challenges posed by informational crime, ensuring the protection of fundamental rights and the credibility of the criminal justice system.

Keywords: Cybercrimes. sScial networks; Digital forensics Criminal law. Digital security.

[1]Trabalho de Conclusão de Curso apresentado no Centro Universitário Santo Agostinho (UNIFSA), no Curso de Direito, Teresina-PI, 04 de setembro de 2025.
[2]Bacharelando do Curso de Direito do Centro Universitário Santo Agostinho (UNIFSA).
[3]Bacharelando do Curso de Direito do Centro Universitário Santo Agostinho (UNIFSA).
[4]Doutorado em Ciências Criminais (PUC/RS). Mestre em Direito (UCB/DF). Especialista penal e processo penal (UFPI).

1 INTRODUÇÃO

A crescente digitalização das relações sociais e o uso intensivo das redes sociais têm transformado profundamente a forma como os indivíduos se comunicam, interagem e consomem informação. No entanto, esse avanço tecnológico também tem proporcionado o surgimento de práticas delituosas no ambiente virtual, como os cibercrimes e as fraudes digitais, que desafiam a atuação do Direito Penal e exigem respostas jurídicas eficazes.

O problema de pesquisa deste estudo surge da dificuldade enfrentada pelo sistema jurídico brasileiro em responsabilizar penalmente os autores de crimes cibernéticos, especialmente aqueles praticados em redes sociais, diante da complexidade técnica e do anonimato que caracterizam essas infrações. Para tanto, o objetivo geral da pesquisa é analisar a atuação da perícia digital forense como instrumento de efetivação da justiça penal frente aos crimes cibernéticos cometidos em redes sociais.

A relevância da pesquisa se justifica pela necessidade de fortalecer os mecanismos de investigação e responsabilização penal no ambiente digital, contribuindo para a proteção dos direitos fundamentais, como a honra, a imagem e a privacidade dos usuários. Do ponto de vista social, científico e jurídico, o estudo busca fomentar o debate sobre a importância da perícia digital como ferramenta técnica essencial para a coleta e preservação de provas digitais.

Além disso, a crescente utilização de redes sociais tem facilitado a disseminação de discursos de ódio, fraudes, golpes e outras formas de violência virtual, levantando questões sobre os limites da liberdade de expressão e a proteção dos direitos individuais. A Constituição Federal de 1988 assegura a inviolabilidade da vida privada e da honra das pessoas, mas a aplicação desses direitos no contexto digital é um desafio constante.

Nesse cenário, a perícia digital forense surge como ferramenta indispensável para a investigação de crimes cibernéticos. Por meio de técnicas especializadas, é possível rastrear atividades suspeitas, recuperar dados apagados, identificar autores e preservar provas digitais com validade jurídica. A atuação dos peritos contribui diretamente para a efetividade da persecução penal, especialmente em casos em que não há contato físico entre autor e vítima.

A jurisprudência do Superior Tribunal de Justiça tem reconhecido a relevância da perícia digital como instrumento essencial para a responsabilização penal em crimes cibernéticos. No julgamento do AgRg no RHC 192461/RJ, o STJ manteve a prisão preventiva de um acusado por integrar organização criminosa especializada em fraudes digitais, destacando que a medida era necessária para acautelar a ordem pública e interromper as atividades do grupo criminoso.

Diante disso, este artigo tem como objetivo geral analisar a atuação da perícia digital forense como instrumento de efetivação da justiça penal frente aos crimes cibernéticos cometidos em redes sociais.

Metodologicamente, trata-se de uma pesquisa qualitativa, com abordagem bibliográfica e documental, fundamentada em autores como Peck (2021), Teixeira (2022), Cunha (2009), entre outros, além da análise de jurisprudência do Superior Tribunal de Justiça. A investigação se apoia em fontes legislativas, doutrinárias e jurisprudenciais para compreender os limites e possibilidades do Direito Penal frente à criminalidade digital.

Este estudo está dividido em quatro seções. A primeira seção, intitulada "Cibercrimes e Fraudes em Redes Sociais", tem como objetivo contextualizar o fenômeno da criminalidade digital e os principais tipos de infrações praticadas nesse ambiente. A segunda seção, "A Evolução dos Crimes Cibernéticos e o Papel das Redes Sociais", analisa a transformação dos delitos digitais ao longo do tempo e o impacto das redes sociais na sua disseminação. A terceira seção, "Legislação Brasileira sobre Crimes Cibernéticos", apresenta os principais diplomas legais aplicáveis à temática. Por fim, a quarta seção, "A Importância da Perícia Digital Forense", discute o papel da perícia na investigação e responsabilização penal dos infratores.

2 CRIMES DIGITAIS E REDES SOCIAIS

A crescente digitalização das relações sociais e a popularização das redes sociais como espaços de convivência, expressão e consumo de informação têm gerado profundas transformações no campo jurídico, especialmente no âmbito penal. A internet, ao mesmo tempo em que democratiza o acesso à comunicação, também se tornou palco para a prática de condutas ilícitas que desafiam os limites tradicionais da legislação penal. Nesse cenário, os chamados cibercrimes "especialmente aqueles cometidos por meio de redes sociais" passaram a demandar respostas mais eficazes do sistema de justiça, tanto no plano normativo quanto investigativo.

Entre os crimes mais recorrentes nesse ambiente estão a difamação, a injúria, a calúnia, o estelionato digital, a falsidade ideológica, o compartilhamento não autorizado de imagens íntimas, o discurso de ódio e a criação de perfis falsos com o intuito de prejudicar terceiros. A facilidade de acesso às plataformas, o anonimato proporcionado por ferramentas tecnológicas e a velocidade de disseminação de conteúdos tornam esses delitos especialmente danosos e de difícil repressão.

A legislação brasileira tem buscado acompanhar essa evolução, ainda que de forma reativa e fragmentada. A promulgação da Lei nº 12.737/2012 (Lei Carolina Dieckmann), que tipificou crimes informáticos como a invasão de dispositivos eletrônicos, representou um marco inicial. Posteriormente, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios e garantias para o uso da rede, incluindo a proteção da privacidade e a responsabilização dos provedores. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), por sua vez, trouxe avanços significativos no tratamento de dados pessoais, mas ainda carece de integração plena com o sistema penal, especialmente no que tange à responsabilização criminal por vazamentos e uso indevido de informações.

Apesar desses avanços, o ordenamento jurídico brasileiro ainda enfrenta dificuldades para lidar com a complexidade dos crimes digitais. A tipificação penal nem sempre é clara ou suficiente para abranger as novas formas de conduta ilícita surgidas no ambiente virtual. Além disso, a investigação desses crimes exige conhecimentos técnicos específicos, acesso rápido a registros digitais e cooperação entre instituições públicas e privadas, o que nem sempre ocorre de forma eficiente. A morosidade processual, aliada à escassez de recursos humanos e tecnológicos, contribui para a perpetuação da impunidade e para o descrédito da população em relação à efetividade da justiça penal.

A atuação da perícia digital forense tem se mostrado indispensável para a superação dos obstáculos técnicos que envolvem a investigação de crimes cometidos em redes sociais. Por meio de técnicas especializadas, os peritos conseguem identificar rastros digitais, recuperar dados apagados, verificar a autenticidade de conteúdos e estabelecer vínculos entre os autores e os atos ilícitos. A confiabilidade da prova técnica é essencial para a responsabilização penal, especialmente em casos em que a autoria é contestada ou os dados foram manipulados. A perícia, portanto, não apenas contribui para a elucidação dos fatos, mas também fortalece a segurança jurídica e a credibilidade do processo penal.

Contudo, a efetividade da perícia digital depende de uma estrutura institucional adequada, que inclua laboratórios equipados, profissionais capacitados e protocolos de atuação bem definidos. A escassez de recursos e a falta de padronização entre os órgãos de segurança pública dificultam a atuação pericial, comprometendo a celeridade e a qualidade das investigações. Além disso, a cooperação entre autoridades nacionais e internacionais é fundamental, uma vez que muitos crimes digitais envolvem servidores localizados fora do

território brasileiro, exigindo medidas de cooperação jurídica internacional e acesso a dados transfronteiriços.

A evolução da justiça penal frente aos crimes digitais requer, portanto, uma abordagem multidisciplinar, que una o conhecimento jurídico ao domínio técnico e à atuação integrada entre instituições. A formação dos operadores do Direito deve incluir noções de tecnologia da informação, segurança cibernética e análise de provas digitais, de modo a permitir uma atuação mais eficaz e consciente diante dos desafios impostos pela era digital. A atualização legislativa, por sua vez, deve ser contínua e orientada por princípios de proteção aos direitos fundamentais, como a privacidade, a liberdade de expressão e a dignidade da pessoa humana.

Em síntese, os crimes digitais praticados em redes sociais representam um dos maiores desafios contemporâneos para o Direito Penal. A sensação de impunidade, alimentada pela complexidade técnica e pela lentidão investigativa, só poderá ser superada com o fortalecimento da perícia digital forense, a modernização legislativa e a capacitação dos profissionais envolvidos na persecução penal. A justiça penal, para ser efetiva na era digital, precisa evoluir em sintonia com a tecnologia, sem perder de vista os valores que sustentam o Estado Democrático de Direito.

2.1 O cenário dos crimes digitais nas redes sociais

A ascensão das redes sociais como principal meio de comunicação interpessoal e disseminação de informações transformou significativamente a forma como os indivíduos interagem, compartilham conteúdos e constroem suas identidades digitais. Plataformas como *Facebook*, *Instagram*, *TikTok*, *WhatsApp* e *X* (antigo *Twitter*) passaram a ocupar um papel central na vida cotidiana, sendo utilizadas não apenas para fins recreativos, mas também como ferramentas de trabalho, mobilização política e expressão pessoal. No entanto, essa popularização também abriu espaço para a prática de condutas ilícitas que desafiam os limites tradicionais do Direito Penal (PECK, 2021).

Os crimes digitais praticados em redes sociais apresentam características peculiares, como o anonimato, a velocidade de propagação de conteúdos e a dificuldade de delimitação territorial. Tais elementos tornam a repressão penal mais complexa, especialmente em casos de difamação, injúria, calúnia, estelionato digital, perseguição virtual (*cyberstalking*), divulgação não autorizada de imagens íntimas e criação de perfis falsos com fins fraudulentos. A viralização de conteúdos ofensivos ou fraudulentos pode causar danos irreparáveis à honra, à

imagem e à privacidade das vítimas, muitas vezes em questão de minutos (BISPO; BINTO, 2023).

A ausência de fronteiras físicas no ambiente digital impõe desafios adicionais à atuação dos órgãos de persecução penal. Crimes cometidos por meio de redes sociais frequentemente envolvem servidores localizados em outros países, o que exige mecanismos de cooperação jurídica internacional para a obtenção de provas e identificação dos autores. Além disso, a volatilidade das evidências digitais, que podem ser facilmente apagadas, alteradas ou ocultadas, dificulta a preservação da materialidade delitiva, exigindo atuação técnica especializada desde os primeiros momentos da investigação (OLIVEIRA; SANTIAGO; COSTA, 2023).

A atuação integrada entre instituições públicas e privadas é essencial para o enfrentamento eficaz dos crimes digitais. Sem cooperação, os esforços investigativos tornam-se fragmentados e ineficazes, comprometendo a responsabilização penal e a proteção dos direitos fundamentais.

Outro fator relevante é a crescente sofisticação das fraudes digitais, que envolvem técnicas como a engenharia social (*social engineering*), o uso de inteligência artificial para a criação de *deepfakes*, a clonagem de contas e a manipulação de algoritmos para direcionamento de conteúdos. Essas práticas, além de violarem direitos individuais, colocam em risco a segurança coletiva, sobretudo quando utilizadas para fins de desinformação, manipulação política ou extorsão (PECK, 2021; WENDT; NOGUEIRA, 2021). A atuação criminosa em redes sociais, portanto, não se limita a ações isoladas, mas pode integrar esquemas organizados e transnacionais, exigindo respostas jurídicas e investigativas mais complexas.

A vulnerabilidade das vítimas também merece atenção. Crianças, adolescentes, idosos e pessoas com baixa familiaridade com o ambiente digital figuram entre os principais alvos de crimes em redes sociais (BRASIL, 2025). A ausência de mecanismos eficazes de prevenção, educação digital e proteção institucional contribui para a perpetuação dessas práticas, tornando urgente a implementação de políticas públicas voltadas à conscientização da população e ao fortalecimento da segurança digital (CASSANTI, 2014). O enfrentamento dessa realidade exige uma resposta penal articulada, que una tecnologia, investigação e proteção dos direitos fundamentais — uma diretriz que deve orientar a atuação do Estado e das instituições de justiça.

A atuação criminosa em redes sociais também se vale de estratégias sofisticadas de manipulação psicológica, como a *social engineering*, que consiste na exploração de vulnerabilidades humanas para obtenção de informações confidenciais ou indução a

comportamentos prejudiciais (DAMÁSIO DE JESUS; MILAGRE, 2016). Essa técnica é amplamente utilizada em golpes que envolvem falsas promoções, links maliciosos e perfis falsos que simulam autoridades ou empresas conhecidas. A capacidade de enganar usuários por meio de interações aparentemente legítimas torna esse tipo de crime especialmente eficaz e difícil de detectar, exigindo atenção redobrada por parte dos órgãos de investigação e da própria sociedade.

Outro fenômeno preocupante é o uso de *bots* e *fake accounts* para a disseminação de conteúdos fraudulentos, discursos de ódio e campanhas de desinformação. Essas ferramentas automatizadas permitem a criação de redes artificiais de perfis que interagem entre si para conferir aparência de legitimidade a determinadas narrativas, influenciando a opinião pública e, em alguns casos, interferindo em processos democráticos. A identificação e neutralização dessas estruturas exigem conhecimento técnico avançado e cooperação entre plataformas digitais e autoridades investigativas (WENDT; NOGUEIRA, 2021; PECK, 2021).

A disseminação de *deepfakes* — vídeos ou áudios manipulados com o uso de inteligência artificial para simular falas ou ações de pessoas reais — representa uma ameaça crescente à integridade da informação e à reputação das vítimas. Esses conteúdos podem ser utilizados para fins de extorsão, vingança, difamação ou manipulação política, e sua detecção requer ferramentas especializadas de análise forense digital. A ausência de regulamentação específica sobre o uso e a responsabilização por *deepfakes* ainda constitui um ponto crítico na legislação brasileira (DAMÁSIO DE JESUS; MILAGRE, 2016; TEIXEIRA, 2022).

Além dos aspectos técnicos, é necessário considerar o impacto psicológico e social dos crimes digitais praticados em redes sociais. As vítimas frequentemente enfrentam sentimentos de vergonha, medo e impotência, o que pode dificultar a denúncia e a busca por justiça. Em muitos casos, o dano causado pela exposição pública ou pela violação da intimidade é irreversível, afetando não apenas a vida pessoal, mas também a profissional e a saúde mental dos envolvidos. A atuação do sistema penal, portanto, deve ser sensível a essas dimensões, oferecendo mecanismos de proteção e acolhimento às vítimas (CASSANTI, 2014).

Nesse contexto, é imprescindível que o sistema jurídico brasileiro avance na construção de uma política penal voltada para o enfrentamento dos crimes digitais, especialmente aqueles praticados em redes sociais. Isso inclui não apenas a atualização legislativa, mas também o fortalecimento das instituições responsáveis pela investigação e persecução penal, com investimentos em tecnologia, capacitação de profissionais e integração entre os diversos atores

envolvidos. A atuação preventiva, por meio da educação digital e da conscientização da sociedade, também deve ser considerada como estratégia fundamental para a redução da incidência desses delitos (PECK, 2021; BRASIL, 2025).

Em síntese, o cenário dos crimes digitais nas redes sociais revela uma realidade complexa e multifacetada, que exige do Direito Penal uma postura proativa, técnica e humanizada. A impunidade decorrente da fragilidade investigativa e da lentidão normativa só poderá ser superada com a valorização da prova digital, a atuação especializada da perícia forense e a construção de um sistema de justiça capaz de dialogar com os desafios da era da informação. O enfrentamento eficaz dessa nova criminalidade depende, sobretudo, da capacidade das instituições jurídicas de se reinventarem diante da velocidade das transformações tecnológicas.

2.2 Tipificação penal e lacunas legislativas

A evolução tecnológica e o surgimento de novas formas de interação social por meio das redes digitais têm desafiado o Direito Penal a acompanhar, com precisão e eficácia, as condutas ilícitas que emergem nesse ambiente. A tipificação penal dos crimes digitais, especialmente aqueles praticados em redes sociais, ainda se mostra insuficiente diante da complexidade e da velocidade com que essas infrações se transformam. Embora o ordenamento jurídico brasileiro tenha avançado em alguns pontos, ainda apresenta lacunas significativas que dificultam a repressão efetiva desses delitos (BISPO; BINTO, 2023; DAMÁSIO DE JESUS; MILAGRE, 2016).

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi um marco inicial ao criminalizar a invasão de dispositivos informáticos, introduzindo os artigos 154-A e 154-B no Código Penal. No entanto, sua abrangência é limitada, não contemplando diversas condutas que ocorrem em redes sociais, como a criação de *fake profiles* para fins fraudulentos, o uso de *deepfakes* para difamação ou extorsão, e o *cyberbullying*. O Marco Civil da Internet (Lei nº 12.965/2014), por sua vez, trouxe importantes princípios sobre privacidade, responsabilidade dos provedores e preservação de registros, mas não possui natureza penal, o que limita sua aplicação repressiva (PECK, 2021; BRASIL, 2014).

A ausência de tipos penais específicos para condutas digitais complexas obriga os operadores do Direito a recorrerem a enquadramentos genéricos, como os crimes contra a honra (arts. 138 a 140 do Código Penal), o estelionato (art. 171), a falsidade ideológica (art. 299) e a ameaça (art. 147). Embora esses dispositivos possam ser utilizados em alguns casos, eles não

foram concebidos para o ambiente digital, o que gera insegurança jurídica, interpretações divergentes e, muitas vezes, a impunidade dos infratores. A jurisprudência ainda caminha de forma tímida na consolidação de entendimentos sobre essas práticas (CUNHA, 2009; TEIXEIRA, 2022).

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) trouxe avanços significativos no tratamento de dados pessoais, estabelecendo regras claras sobre coleta, armazenamento e compartilhamento de informações. Contudo, sua aplicação no campo penal é indireta, voltada principalmente à responsabilização administrativa e civil. A ausência de previsão expressa de sanções penais para o uso indevido de dados em redes sociais, como em casos de *data leaks* ou comercialização de informações pessoais, evidencia a necessidade de integração normativa entre a LGPD e o Código Penal.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) trouxe avanços significativos no tratamento de dados pessoais, estabelecendo regras claras sobre coleta, armazenamento e compartilhamento de informações. Contudo, sua aplicação no campo penal é indireta, voltada principalmente à responsabilização administrativa e civil. A ausência de previsão expressa de sanções penais para o uso indevido de dados em redes sociais, como em casos de *data leaks* ou comercialização de informações pessoais, evidencia a necessidade de integração normativa entre a LGPD e o Código Penal (PECK, 2021; BRASIL, 2018).

A jurisprudência brasileira tem buscado suprir algumas dessas lacunas por meio da interpretação extensiva de tipos penais já existentes, especialmente nos casos de crimes contra a honra e estelionato praticados em redes sociais. Embora essa prática seja necessária diante da omissão legislativa, ela pode comprometer o princípio da legalidade penal, que exige a tipificação clara e prévia da conduta criminosa. A ausência de normas específicas para o ambiente digital dificulta a uniformização das decisões judiciais e a previsibilidade das consequências jurídicas para os infratores, gerando insegurança jurídica e favorecendo interpretações divergentes entre os tribunais (CUNHA, 2009; TEIXEIRA, 2022).

A atuação dos provedores de aplicação e conexão também representa um ponto sensível na discussão sobre a tipificação penal dos crimes digitais. O *Marco Civil da Internet* (Lei nº 12.965/2014) estabelece diretrizes sobre a guarda de registros e o fornecimento de dados mediante ordem judicial, mas não impõe obrigações de monitoramento ou filtragem de conteúdo. Essa limitação, embora proteja a liberdade de expressão e a neutralidade da rede, pode dificultar a responsabilização de plataformas que se omitem diante de práticas criminosas recorrentes. A

responsabilização penal de intermediários digitais ainda é tema controverso, exigindo um equilíbrio entre a proteção de direitos fundamentais e a repressão eficaz das condutas ilícitas (PECK, 2021; BRASIL, 2014).

A ausência de uma legislação penal unificada e atualizada sobre crimes digitais impacta diretamente a atuação da perícia forense. Sem tipos penais claros e específicos, a coleta e análise de provas digitais podem ser questionadas quanto à sua pertinência e legalidade, especialmente em processos que envolvem dados sensíveis ou comunicações privadas. A falta de diretrizes técnicas e jurídicas para a produção de provas digitais no processo penal brasileiro reforça a necessidade de regulamentação que contemple os aspectos próprios da investigação cibernética (PIERITZ NETTO; PIERITZ, 2023).

Nesse contexto, torna-se imprescindível que o legislador brasileiro avance na construção de um marco penal digital capaz de abranger as novas formas de criminalidade sem comprometer os direitos fundamentais assegurados pela Constituição Federal. A experiência internacional, como a *Budapest Convention on Cybercrime*, pode servir de referência para a elaboração de normas que conciliem repressão eficaz com garantias processuais adequadas. A adesão do Brasil a tratados internacionais sobre crimes cibernéticos também pode fortalecer a cooperação jurídica internacional e facilitar a obtenção de provas em casos transnacionais (NUCCI, 2023; LOPES JR., 2021).

A construção de um sistema penal eficaz para o enfrentamento dos crimes digitais exige, portanto, uma abordagem legislativa dinâmica, técnica e sensível às transformações sociais e tecnológicas. A criminalidade digital não pode ser enfrentada com os mesmos instrumentos utilizados para os delitos convencionais, pois envolve novas formas de execução, novas vítimas e novos meios de prova. A legislação deve ser capaz de acompanhar essas mudanças, sem abrir mão dos princípios constitucionais que regem o Direito Penal, como a legalidade, a proporcionalidade e a dignidade da pessoa humana.

Em conclusão, as lacunas legislativas que ainda permeiam a tipificação dos crimes digitais praticados em redes sociais representam um obstáculo significativo à efetividade da justiça penal. A ausência de normas específicas, a dificuldade de enquadramento jurídico e a insuficiência de mecanismos de cooperação internacional comprometem a responsabilização dos infratores e a proteção das vítimas. A superação desses desafios passa pela atualização normativa, pela valorização da prova digital e pela construção de um marco penal que dialogue com os avanços tecnológicos e com os direitos fundamentais da era digital.

2.3 A impunidade como reflexo da fragilidade investigativa

A sensação de impunidade que permeia os crimes digitais praticados em redes sociais está diretamente relacionada à fragilidade dos mecanismos investigativos disponíveis no sistema de justiça penal brasileiro. A complexidade técnica envolvida na coleta, preservação e análise de provas digitais exige uma estrutura institucional que ainda não está plenamente consolidada, o que compromete a efetividade da persecução penal e favorece a reincidência de condutas ilícitas nesse ambiente (PIERITZ NETTO; PIERITZ, 2023).

Um dos principais desafios enfrentados pelas autoridades é a volatilidade das evidências digitais. Diferentemente das provas físicas, os dados eletrônicos podem ser facilmente apagados, modificados ou ocultados, especialmente quando armazenados em servidores estrangeiros ou protegidos por sistemas de *criptografia*. A ausência de protocolos padronizados para a preservação imediata de registros em redes sociais dificulta a atuação da polícia judiciária e do Ministério Público, que muitas vezes dependem da colaboração voluntária das plataformas para obter informações essenciais à investigação (NUCCI, 2023; LOPES JR., 2021).

Outro fator que contribui para a impunidade é a escassez de profissionais capacitados para lidar com crimes cibernéticos. A investigação digital demanda conhecimentos específicos em tecnologia da informação, segurança de redes, análise forense e legislação especializada, áreas que ainda não são plenamente dominadas por grande parte dos operadores do Direito. A falta de formação técnica adequada compromete a qualidade das investigações e pode levar à invalidação de provas por vícios processuais ou ausência de cadeia de custódia (DAMÁSIO DE JESUS; MILAGRE, 2016).

Outro fator que agrava esse cenário é a morosidade na tramitação dos processos. A lentidão na obtenção de ordens judiciais para quebra de sigilo, a demora na resposta das plataformas digitais e a sobrecarga dos órgãos periciais contribuem para o enfraquecimento da resposta penal. Em muitos casos, quando as provas finalmente são obtidas, já não possuem valor probatório relevante ou foram comprometidas pela passagem do tempo. Essa realidade reforça a necessidade de medidas urgentes para agilizar os procedimentos investigativos e garantir a efetividade da justiça (BISPO; BINTO, 2023).

A crescente sensação de impunidade nos crimes digitais, especialmente aqueles praticados em redes sociais, está diretamente ligada à fragilidade dos mecanismos investigativos disponíveis no sistema de justiça penal brasileiro. A complexidade técnica envolvida na coleta, preservação e análise de provas digitais exige uma estrutura institucional especializada, que

ainda se encontra em processo de consolidação. Essa deficiência compromete a efetividade da persecução penal e favorece a reincidência de condutas ilícitas nesse ambiente (PIERITZ NETTO; PIERITZ, 2023).

Um dos principais desafios enfrentados pelas autoridades é a volatilidade das evidências digitais. Diferentemente das provas físicas, os dados eletrônicos podem ser facilmente apagados, modificados ou ocultados, sobretudo quando armazenados em servidores estrangeiros ou protegidos por sistemas de *criptografia*. A ausência de protocolos padronizados para a preservação imediata de registros em redes sociais dificulta a atuação da polícia judiciária e do Ministério Público, que muitas vezes dependem da colaboração voluntária das plataformas para obter informações essenciais à investigação (NUCCI, 2023; LOPES JR., 2021).

A escassez de profissionais capacitados para lidar com crimes cibernéticos também contribui significativamente para a impunidade. A investigação digital demanda conhecimentos específicos em tecnologia da informação, segurança de redes, análise forense e legislação especializada — áreas que ainda não são plenamente dominadas por grande parte dos operadores do Direito. A ausência de formação técnica adequada compromete a qualidade das investigações e pode levar à invalidação de provas por vícios processuais ou quebra da cadeia de custódia (DAMÁSIO DE JESUS; MILAGRE, 2016).

Outro fator que agrava esse cenário é a morosidade na tramitação dos processos. A lentidão na obtenção de ordens judiciais para quebra de sigilo, a demora na resposta das plataformas digitais e a sobrecarga dos órgãos periciais contribuem para o enfraquecimento da resposta penal. Em muitos casos, quando as provas finalmente são obtidas, já não possuem valor probatório relevante ou foram comprometidas pela passagem do tempo. Essa realidade reforça a necessidade de medidas urgentes para agilizar os procedimentos investigativos e garantir a efetividade da justiça (BISPO; BINTO, 2023).

Além disso, a ausência de cooperação internacional estruturada dificulta a responsabilização de infratores que atuam a partir de outros países. A natureza transnacional dos crimes digitais exige acordos bilaterais e multilaterais que permitam o acesso rápido a dados armazenados fora do território nacional. A não adesão do Brasil à *Budapest Convention on Cybercrime*, por exemplo, limita a capacidade de resposta do Estado diante de infrações que envolvem jurisdições estrangeiras, comprometendo a eficácia da investigação e a aplicação da lei penal (LOPES JR., 2021).

A ausência de integração entre os sistemas de segurança pública e os provedores de redes sociais também contribui para a fragilidade investigativa. Muitas plataformas internacionais, como *Facebook*, *Instagram*, *TikTok* e *X*, possuem políticas próprias de privacidade e armazenamento de dados, que nem sempre estão alinhadas com as exigências legais brasileiras. A obtenção de informações técnicas, como IPs, registros de acesso e conteúdos apagados, depende de canais específicos e, em alguns casos, de acordos internacionais que o Brasil ainda não firmou ou operacionaliza com lentidão (PECK, 2021).

A falta de padronização nos procedimentos de coleta e preservação de provas digitais é outro fator que compromete a eficácia das investigações. Sem protocolos claros e uniformes, há risco de contaminação da prova, quebra da cadeia de custódia e invalidação de elementos essenciais para a responsabilização penal. A atuação dos peritos, embora fundamental, muitas vezes é prejudicada pela ausência de recursos tecnológicos adequados e pela sobrecarga de demandas, o que limita a capacidade de resposta do sistema de justiça (PIERITZ NETTO; PIERITZ, 2023).

Além disso, a cultura institucional ainda não está plenamente adaptada à realidade digital. Muitos delegados, promotores e magistrados não possuem formação específica em crimes cibernéticos, o que dificulta a compreensão da dinâmica dos delitos e a correta interpretação das provas técnicas. A falta de especialização compromete a tomada de decisões estratégicas durante a investigação, como a escolha do momento ideal para a quebra de sigilo ou a solicitação de medidas cautelares. A capacitação contínua dos operadores do Direito é, portanto, uma medida urgente e necessária.

A impunidade também é alimentada pela percepção social de que os crimes digitais são menos graves ou menos "reais" do que os delitos convencionais. Essa visão equivocada contribui para a subnotificação das infrações, especialmente aquelas que envolvem violência psicológica, exposição indevida ou perseguição virtual. Muitas vítimas não denunciam por medo, vergonha ou descrença na efetividade da justiça, o que reforça o ciclo de invisibilidade e reincidência. O reconhecimento da gravidade dos crimes digitais é essencial para que o sistema penal possa atuar com firmeza e legitimidade.

A superação da impunidade nos crimes digitais exige uma reestruturação profunda dos mecanismos investigativos, com foco na modernização tecnológica, na capacitação dos profissionais envolvidos e na criação de unidades especializadas em *cibercriminalidade*. A implementação de delegacias virtuais, laboratórios de perícia digital e sistemas integrados de

inteligência pode representar um avanço significativo na resposta penal, desde que acompanhada de investimentos contínuos e políticas públicas voltadas à segurança digital.

Em síntese, a fragilidade investigativa que marca os crimes digitais praticados em redes sociais é um dos principais fatores que alimentam a impunidade e comprometem a credibilidade da justiça penal. A ausência de estrutura técnica, a lentidão processual e a falta de cooperação internacional são obstáculos que precisam ser enfrentados com urgência. Somente por meio de uma atuação articulada entre tecnologia, legislação e capacitação institucional será possível garantir a efetividade da persecução penal e a proteção dos direitos fundamentais na era digital.

2.4. A Responsabilização Penal nas Redes Sociais: Desafios e Perspectivas

A ascensão das redes sociais como principal meio de comunicação interpessoal e difusão de informações trouxe consigo uma nova gama de condutas potencialmente criminosas, que desafiam os limites da legislação penal tradicional. A facilidade de acesso, o anonimato e a velocidade de propagação de conteúdos tornam o ambiente virtual propício à prática de ilícitos como calúnia, difamação, injúria, incitação ao crime, apologia ao nazismo, racismo, entre outros. No entanto, a responsabilização penal por tais condutas ainda encontra entraves significativos, tanto no plano normativo quanto no plano prático da investigação e da persecução penal (NUCCI, 2023; LOPES JR., 2021).

A legislação brasileira, embora tenha avançado com o *Marco Civil da Internet* (Lei nº 12.965/2014) e com a *Lei Geral de Proteção de Dados* (Lei nº 13.709/2018), ainda carece de dispositivos específicos que tratem de forma clara e objetiva os crimes cometidos em redes sociais. A ausência de uma tipificação penal adequada para condutas como o compartilhamento de *fake news*, o *cyberbullying* e o *discurso de ódio* dificulta a atuação dos órgãos de persecução penal e contribui para a sensação de impunidade. A jurisprudência, por sua vez, tem buscado suprir essas lacunas por meio de interpretações extensivas e sistemáticas, mas nem sempre consegue garantir segurança jurídica e uniformidade na aplicação da lei (PECK, 2021; TEIXEIRA, 2022).

A atuação da perícia digital forense tem se mostrado essencial para a identificação dos autores de crimes praticados em redes sociais. A análise de metadados, a rastreabilidade de endereços IP, a recuperação de conteúdos apagados e a verificação de autenticidade de perfis são ferramentas indispensáveis para a investigação criminal no ambiente virtual. Contudo, a escassez de profissionais capacitados, a limitação de recursos tecnológicos e a morosidade na

obtenção de dados junto às plataformas digitais ainda representam obstáculos à efetividade da persecução penal (PIERITZ NETTO; PIERITZ, 2023).

Outro ponto de destaque é a responsabilidade das plataformas digitais que hospedam conteúdos ilícitos. Embora o *Marco Civil da Internet* estabeleça que a retirada de conteúdo depende de ordem judicial, há discussões sobre a possibilidade de responsabilização civil e até penal das empresas em casos de omissão diante de denúncias reiteradas. A jurisprudência tem oscilado entre a proteção à liberdade de expressão e a necessidade de garantir a dignidade da pessoa humana, especialmente em casos que envolvem *discurso de ódio*, violência simbólica e violação de direitos fundamentais (BRASIL, 2014; BISPO; BINTO, 2023).

A responsabilização penal também enfrenta o desafio da territorialidade. A natureza transnacional da internet dificulta a aplicação das normas penais brasileiras quando os servidores estão localizados em outros países ou quando o autor do delito reside fora do território nacional. Essa complexidade exige cooperação jurídica internacional e acordos bilaterais que viabilizem a obtenção de provas e a responsabilização dos envolvidos. O Brasil, como signatário da *Budapest Convention on Cybercrime*, tem buscado ampliar sua capacidade de atuação internacional, mas ainda enfrenta limitações práticas e burocráticas que comprometem a eficácia das investigações (NUCCI, 2023; LOPES JR., 2021).

Além disso, a cultura da desinformação e da polarização política intensificada pelas redes sociais tem contribuído para a banalização de condutas criminosas, como a calúnia e a incitação à violência. A ausência de uma resposta penal célere e eficaz reforça a ideia de que o ambiente virtual é um espaço de impunidade, o que compromete a credibilidade das instituições e a proteção dos direitos fundamentais. A propagação de discursos extremistas, teorias conspiratórias e ataques coordenados a grupos vulneráveis exige uma atuação firme e articulada do sistema de justiça criminal (DAMÁSIO DE JESUS; MILAGRE, 2016).

A atuação do Ministério Público e das Defensorias Públicas também precisa se adaptar às especificidades dos crimes digitais. A capacitação de seus membros em tecnologia da informação e a criação de núcleos especializados são medidas que podem contribuir para uma atuação mais eficiente, tanto na acusação quanto na defesa, garantindo o devido processo legal e a ampla defesa. A complexidade técnica dos crimes digitais exige uma abordagem multidisciplinar, que envolva não apenas o conhecimento jurídico, mas também habilidades em informática, segurança cibernética e análise de dados (PIERITZ NETTO; PIERITZ, 2023).

A responsabilização penal nas redes sociais não pode se limitar à repressão. É necessário repensar o papel da educação digital como instrumento de prevenção. A conscientização sobre os limites da liberdade de expressão, o respeito à privacidade e a responsabilidade pelo conteúdo compartilhado são fundamentais para a construção de uma cultura digital mais ética e menos propensa à prática de ilícitos penais. Campanhas educativas, inserção de temas relacionados à ética digital nos currículos escolares e capacitação de professores e profissionais da educação são medidas que podem contribuir para a construção de um ambiente virtual mais seguro.

A evolução da Justiça Penal frente aos crimes digitais exige uma reforma legislativa que contemple as especificidades do ambiente virtual. A criação de tipos penais próprios, a regulamentação da atuação das plataformas digitais e o fortalecimento da cooperação internacional são medidas urgentes para garantir a efetividade da responsabilização penal. Além disso, é necessário investir em tecnologia, capacitação e estrutura para que os órgãos de persecução penal possam atuar com eficiência diante dos desafios impostos pela criminalidade informacional (NUCCI, 2023; PECK, 2021).

A responsabilização penal nas redes sociais deve ser vista como parte de um processo mais amplo de adaptação do sistema de justiça à realidade digital. A impunidade não decorre apenas da ausência de normas, mas também da dificuldade de aplicação das leis existentes diante das novas formas de interação social. É preciso reconhecer que o ambiente virtual não está à margem do ordenamento jurídico, e que a proteção dos direitos fundamentais deve ser garantida também no *ciberespaço* (LOPES JR., 2021).

Em suma, a construção de uma Justiça Penal eficaz no enfrentamento dos crimes digitais passa pela integração entre repressão, prevenção e educação. A responsabilização dos autores, a atuação das plataformas, a capacitação dos operadores do Direito e a conscientização da sociedade são pilares fundamentais para que o ambiente virtual deixe de ser um espaço de impunidade e se torne um território de respeito à legalidade e à dignidade humana.

3 A IMPORTÂNCIA DA PERÍCIA DIGITAL FORENSE NA INVESTIGAÇÃO DE CRIMES DIGITAIS

A crescente digitalização das relações sociais, econômicas e institucionais tem ampliado significativamente o campo de atuação da perícia digital forense. Diante da complexidade dos crimes informáticos, a perícia se tornou um instrumento indispensável para a produção de provas técnicas, a identificação de autores e a reconstrução de condutas ilícitas praticadas no

ambiente virtual. A atuação pericial, nesse contexto, não apenas complementa a investigação criminal, mas também contribui para a efetividade da justiça penal e para a proteção dos direitos fundamentais.

A perícia digital forense envolve a aplicação de técnicas especializadas para a coleta, preservação, análise e interpretação de evidências digitais. Entre os procedimentos mais comuns estão a recuperação de arquivos apagados, a análise de *logs* de acesso, a identificação de endereços IP, a verificação de autenticidade de documentos eletrônicos e a análise de dispositivos móveis e redes. Esses elementos são essenciais para a construção de uma narrativa probatória sólida, especialmente em casos que envolvem crimes como *phishing*, *ransomware*, invasão de dispositivos, divulgação não autorizada de dados e crimes contra a honra em redes sociais (PIERITZ NETTO; PIERITZ, 2023).

A confiabilidade da prova digital depende diretamente da observância de protocolos técnicos e jurídicos, como a preservação da cadeia de custódia, o uso de ferramentas certificadas e a atuação de profissionais qualificados. A ausência desses cuidados pode comprometer a validade da prova e gerar nulidades processuais. Por isso, é fundamental que os peritos atuem em conformidade com os princípios do devido processo legal, da legalidade e da imparcialidade, garantindo que a prova digital seja admissível e eficaz no âmbito judicial (LOPES JR., 2021).

Além de sua função probatória, a perícia digital forense também desempenha papel estratégico na prevenção e repressão de crimes cibernéticos. A análise de padrões de comportamento, a identificação de vulnerabilidades em sistemas e a produção de laudos técnicos contribuem para o aprimoramento das políticas públicas de segurança digital. A integração entre os órgãos de segurança, os laboratórios forenses e as plataformas tecnológicas é essencial para que a resposta estatal seja rápida, precisa e proporcional à gravidade dos delitos.

A perícia digital forense também enfrenta desafios relacionados à obtenção de dados junto às plataformas digitais. Muitas empresas de tecnologia operam sob legislações estrangeiras e possuem políticas próprias de privacidade, o que dificulta o acesso a informações essenciais para a investigação criminal. A ausência de acordos internacionais eficazes e a morosidade na tramitação de pedidos de cooperação jurídica internacional comprometem a celeridade e a efetividade da produção da prova digital. A adesão do Brasil à *Budapest Convention on Cybercrime* representa um avanço nesse sentido, mas ainda há entraves práticos que precisam ser superados (NUCCI, 2023; LOPES JR., 2021).

A perícia digital forense também se destaca pela sua capacidade de atuar em tempo real, especialmente em operações que envolvem monitoramento de redes, interceptações telemáticas e análise de tráfego de dados. O uso de *real-time monitoring systems* permite a identificação de condutas criminosas em andamento, possibilitando ações preventivas e repressivas mais eficazes. Essa atuação dinâmica é especialmente relevante em casos de crimes contra crianças e adolescentes, terrorismo digital e fraudes financeiras.

Outro aspecto relevante é a necessidade de padronização dos procedimentos periciais. A ausência de protocolos técnicos uniformes para a coleta, preservação e análise de evidências digitais pode gerar inconsistências na produção da prova e comprometer sua validade jurídica. A adoção de boas práticas internacionais, como o uso de ferramentas certificadas e a documentação rigorosa da cadeia de custódia, é fundamental para garantir a integridade e a confiabilidade dos laudos periciais (PIERITZ NETTO; PIERITZ, 2023).

A capacitação contínua dos profissionais que atuam na perícia digital forense é igualmente essencial. Diante da constante evolução tecnológica, é necessário que peritos, delegados, promotores e magistrados estejam atualizados quanto às novas ferramentas, técnicas e vulnerabilidades digitais. A formação multidisciplinar, que envolva conhecimentos em informática, segurança da informação, criptografia e legislação penal, contribui para uma atuação mais eficaz e alinhada às exigências do processo penal contemporâneo.

Além da função repressiva, a perícia digital forense pode atuar de forma preventiva, identificando padrões de comportamento criminoso, vulnerabilidades em sistemas e riscos à segurança da informação. A integração entre os órgãos de segurança pública, os laboratórios forenses e as instituições acadêmicas pode fomentar a produção de conhecimento técnico e o desenvolvimento de soluções inovadoras para o enfrentamento da criminalidade digital.

No âmbito da prova pericial, é fundamental que os profissionais envolvidos dominem não apenas os aspectos técnicos, mas também os fundamentos jurídicos que regem a admissibilidade e a valoração da prova. A interdisciplinaridade entre Direito e Tecnologia é uma exigência cada vez mais presente na formação dos peritos, que devem compreender os limites legais da atuação investigativa, especialmente no que diz respeito à privacidade, ao sigilo de comunicações e à proteção de dados pessoais.

A valorização da perícia digital forense passa também pela sua institucionalização como função essencial à justiça. A criação de laboratórios forenses especializados, vinculados aos institutos de criminalística, e a regulamentação da atividade pericial digital são medidas que

podem fortalecer a atuação técnica e garantir maior segurança jurídica aos processos que envolvem crimes digitais. A padronização de procedimentos e a certificação de profissionais são passos importantes nesse sentido.

Finalizando, é preciso reconhecer que a perícia digital forense não é apenas uma ferramenta auxiliar, mas um elemento central na construção da verdade processual em casos que envolvem crimes digitais. Sua atuação técnica, precisa e imparcial contribui para a efetividade da justiça penal e para a proteção dos direitos das vítimas, especialmente em um ambiente marcado pela complexidade e pela volatilidade das informações.

A evolução da criminalidade digital exige que o sistema de justiça acompanhe as transformações tecnológicas, investindo em capacitação, estrutura e integração institucional. A perícia digital forense representa a resposta técnica mais adequada aos desafios impostos pela nova realidade informacional, sendo indispensável para a responsabilização penal e para a garantia da legalidade no ambiente virtual.

Em suma, a importância da perícia digital forense transcende o aspecto técnico e alcança dimensões jurídicas, sociais e institucionais. Seu fortalecimento é condição essencial para que o Estado possa enfrentar, com eficiência e justiça, os crimes que se multiplicam nas redes digitais, protegendo os bens jurídicos fundamentais e promovendo a segurança da sociedade.

4 CONSIDERAÇÕES FINAIS

A crescente incidência de crimes digitais praticados em redes sociais tem revelado a urgência de uma resposta penal adequada, capaz de enfrentar os desafios impostos pela tecnologia e pela complexidade das novas formas de interação social. A legislação brasileira, embora tenha avançado em alguns aspectos, ainda apresenta lacunas significativas que dificultam a tipificação, a investigação e a responsabilização dos infratores. A ausência de normas específicas, a morosidade processual e a limitação estrutural dos órgãos de persecução penal contribuem para a sensação de impunidade e para a fragilização da justiça.

A perícia digital forense se destaca como ferramenta essencial na produção da prova técnica, permitindo a identificação de autores, a reconstrução de condutas e a validação de evidências digitais. Sua atuação, no entanto, depende de investimentos contínuos em tecnologia, capacitação e estrutura, além da integração entre os órgãos de segurança pública, o Poder Judiciário e as plataformas digitais. A adesão a tratados internacionais, como a *Budapest*

Convention on Cybercrime, também se mostra estratégica para ampliar a cooperação jurídica e fortalecer a atuação transnacional.

A responsabilização penal nas redes sociais não pode se limitar à repressão. É necessário promover uma cultura digital pautada na ética, na responsabilidade e no respeito aos direitos fundamentais. A educação digital, a conscientização da sociedade e a formação dos operadores do Direito são pilares indispensáveis para a construção de um ambiente virtual mais seguro e justo.

Em síntese, o enfrentamento dos crimes digitais exige uma abordagem multidisciplinar, que articule legislação, tecnologia, investigação e educação. Somente por meio de uma reforma legislativa eficaz, da valorização da prova digital e da atuação integrada entre os diversos agentes do sistema de justiça será possível garantir a proteção das vítimas, a responsabilização dos infratores e a efetividade da justiça penal na era digital.

Portanto, este estudo contribui para o debate jurídico sobre os limites e possibilidades do Direito Penal frente à criminalidade digital, destacando a importância da perícia digital forense como aliada da justiça na construção de um ambiente virtual mais seguro e responsável. A integração entre os operadores do Direito, os profissionais da tecnologia e os órgãos de segurança pública é essencial para garantir a proteção dos direitos fundamentais na era da informação.

REFERÊNCIAS

ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARÃES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais**. Revista Vertentes do Direito, v. 2, n. 1, p. 191–205, 2017.

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. **Crimes cibernéticos: da ineficácia da Lei Carolina Dieckmann na prática de crimes virtuais**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 11, p. 354–369, 2023.

BRASIL. **Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940.**

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Diário Oficial da União, Brasília, DF, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br>. Acesso em: 20 abr. 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>. Acesso em: 10 maio 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CUNHA, Rogério Sanches. **Direito Penal – Parte Especial**. 2. ed. ver. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2009.

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

LOPES JR., Aury. **Direito Processual Penal**. 19. ed. São Paulo: Saraiva, 2021.

NUCCI, Guilherme de Souza. **Curso de Direito Processual Penal**. 20. ed. Rio de Janeiro: Forense, 2023.

OLIVEIRA, Daiana Souza de; SANTIAGO, Vinícius Vale; COSTA, Adriana Vieira da. **Perícia forense computacional: a admissibilidade e a fragilidade das evidências coletadas via computação forense**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 5, p. 3978–3997, 2023.

PECK, Patrícia. **Direito Digital**. 7. ed. São Paulo: Saraiva, 2021.

PIERITZ NETTO, Alfredo; PIERITZ, Vera Lúcia Hoffmann. **Crimes Cibernéticos**. Livro Digital. UNIASSELVI, 2023.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 6. ed. São Paulo: SaraivaJur, 2022.