SINTHIA EMILLY ARAUJO PEREIRA

TINA ALICE SILVA MOTA

A NORMA PENAL NO ENFRENTAMENTO À CIBERCRIMINALIDADE NO BRASIL: efetividade e desafios da legislação brasileira no ambiente virtual

TERESINA – PI

2025

SINTHIA EMILLY ARAUJO PEREIRA
TINA ALICE SILVA MOTA

A NORMA PENAL NO ENFRENTAMENTO À CIBERCRIMINALIDADE NO BRASIL: efetividade e desafios da legislação brasileira no ambiente virtual

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

Orientadora: Profª Ma. Dione Cardoso de Alcântara

TERESINA – PI
2025

FICHA CATALOGRÁFICA

P436n Pereira, Sinthia Emilly Araujo

A norma penal no enfrentamento à cibercriminalidade no brasil: efetividade e desafios da legislação brasileira no ambiente virtual / Sinthia Emilly Araujo Pereira; Tina Alice Silva Mota. –– Teresina: UNINOVAFAPI, 2025.

Orientador (a): Profº. Ms. Dione Cardoso de Alcântara. – UNINOVAFAPI, 2025.

28.p.; 23cm.

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

1. Efetividade da norma penal. 2. Crimes cibernéticos. 3. Provas digitais. 4. Cooperação internacional. 5. Perícia forense I. Título. II. Mota, Tina Alice Silva.

CDD 345

Catalogação na publicação
Francisco Renato Sampaio da Silva – CRB/1028

SINTHIA EMILLY ARAUJO PEREIRA

TINA ALICE SILVA MOTA

A NORMA PENAL NO ENFRENTAMENTO À CIBERCRIMINALIDADE NO BRASIL:
efetividade e desafios da legislação brasileira no ambiente virtual

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: 12/11/2025.

BANCA EXAMINADORA

Dione Cardoso de Alcântara

Professora Mestra Dione Cardoso de Alcântara

Afya Centro Universitário Uninovafapi

(Orientadora)

Amanda Fernandes Leal

Professora Mestra Amanda Fernandes Leal

Afya Centro Universitário Uninovafapi

(1º Examinadora)

Sara M S C Lopes

Professora Mestra Sara Morgana Silva Carvalho Lopes

Afya Centro Universitário Uninovafapi

(2º Examinadora)

À Deus, que nos sustentou com fé, coragem e esperança até aqui, e às nossas famílias que sempre nos apoiaram e caminharam nessa jornada conosco e fizeram de cada obstáculo uma oportunidade de aprendizado, sendo nossa base e que sempre sonharam e torceram por nós!

RESUMO

A crescente incidência de crimes cibernéticos no Brasil, especialmente aqueles que envolvem golpes virtuais e manipulação indevida de dados sensíveis no âmbito do Poder Judiciário, tem evidenciado as limitações da norma penal tradicional diante da complexidade do ambiente digital. A dificuldade de rastreamento da autoria, a volatilidade das provas eletrônicas e a sofisticação dos meios tecnológicos utilizados pelos infratores tornam o combate a essas práticas um desafio constante para o sistema de justiça criminal. Nesse cenário, observa-se uma evolução legislativa contínua que busca acompanhar o avanço tecnológico, integrando normas regulatórias gerais, instrumentos penais específicos, mecanismos de proteção de dados pessoais, como os previstos na Lei Geral de Proteção de Dados e na Lei nº 14.155/2021. Apenas criar tipos penais não garante a efetividade da resposta criminal, é preciso implementar medidas estruturais e institucionais que fortaleçam a capacidade investigativa do Estado. Assim, este trabalho analisa em que medida os crimes digitais, com ênfase na fraude e no estelionato digital, comprometem a efetividade da norma penal brasileira, ressaltando as lacunas normativas e operacionais que dificultam a punição e a prevenção dessas condutas. A presente pesquisa adotou, em um primeiro momento, o método de revisão bibliográfica, complementado por uma abordagem qualitativa de análise. Embora os crimes cibernéticos representem uma ameaça significativa, os mecanismos existentes têm contribuído parcialmente para a efetividade da norma penal. Contudo, ainda é necessário aprimorar essa resposta por meio de estratégias integradas, com cooperação entre Estado, setor privado e sociedade civil, promovendo capacitação contínua, inovação tecnológica e maior articulação institucional.

Palavras-chave: efetividade da norma penal; crimes cibernéticos; provas digitais; cooperação internacional; perícia forense; cadeia de custódia.

ABSTRACT

The increasing incidence of cybercrimes in Brazil, especially those involving virtual scams and the improper manipulation of sensitive data within the Judiciary, has highlighted the limitations of traditional criminal law in the face of the complexity of the digital environment. The difficulty in tracing the perpetrators, the volatility of electronic evidence, and the sophistication of the technological means used by offenders make combating these practices a constant challenge for the criminal justice system. In this context, there is a continuous legislative evolution seeking to keep up with technological advancement, integrating general regulatory norms, specific criminal instruments, and personal data protection mechanisms, such as those provided in the General Data Protection Law and Law No. 14,155/2021.
Simply creating criminal offenses does not guarantee the effectiveness of the criminal response; it is necessary to implement structural and institutional measures that strengthen the State's investigative capacity. Thus, this paper analyzes to what extent digital crimes, with an emphasis on digital fraud and scams, compromise the effectiveness of Brazilian criminal law, highlighting the normative and operational gaps that hinder the punishment and prevention of such conduct.This research initially adopted the method of literature review, complemented by a qualitative analysis approach. Although cybercrimes represent a significant threat, existing mechanisms have only partially contributed to the effectiveness of criminal law. However, it is still necessary to enhance this response through integrated strategies, with cooperation between the State, the private sector, and civil society, promoting continuous training, technological innovation, and greater institutional coordination.

Keywords: effectiveness of the criminal norm; cybercrimes; digital evidence; international cooperation; forensic expertise; chain of custody.

SUMÁRIO

1 INTRODUÇÃO

No contexto digital contemporâneo, as modalidades de crimes cibernéticos têm se diversificado e ganhado relevância tanto no campo jurídico quanto no social. os crimes de invasão de dispositivo informático, conforme elucidado por Souza (2021, apud Alexandre; Araújo, 2023), têm aumentado sua prevalência, dada a profunda integração de tecnologias no cotidiano das pessoas. a invasão de sistemas privados, seja para obtenção de dados pessoais ou para outros fins maliciosos, constitui uma grave violação à privacidade e à segurança das informações.

Nesse panorama, o crime virtual vem crescendo no âmbito judicial e se tornando uma grande problemática quanto à materialidade das provas e à eficácia das normas. à medida que a sociedade adotava o uso da internet em suas atividades diárias, surgiam novos desafios para o direito. Dornelas (2019, apud Alexandre; Araújo, 2023) destaca que a resposta estatal frente a esse fenômeno é fundamental, sendo a lei nº 12.735/2012 é um marco legal importante na tentativa de coibir tais práticas.

De igual modo, no ambiente digital, novas formas de criminalidade emergem com velocidade proporcional ao avanço tecnológico, desafiando os instrumentos jurídicos tradicionais que, em muitos casos, ainda estão ancorados em paradigmas analógicos. o chamado "crime virtual" não apenas transcende fronteiras físicas, como também opera em camadas de anonimato e volatilidade que dificultam a identificação de agentes, a preservação de dados probatórios e a aplicação efetiva da justiça.

O artigo 154-a do código penal, introduzido na Lei 12.737/2012 - Lei Carolina Dieckmann, foi a primeira norma a tipificar penalmente condutas de invasão de dispositivos eletrônicos no Brasil, incluindo o acesso não autorizado a computadores, celulares e contas digitais. essa lei passou a proteger a intimidade e os dados pessoais dos indivíduos em ambiente virtual.

Sua importância para o judiciário está em permitir a responsabilização penal de condutas que antes eram tratadas apenas no âmbito civil. além disso, serviu de base para a concessão de medidas protetivas, como retirada de conteúdo da

internet e bloqueio de contas, quando a violação da intimidade digital representa risco à integridade da vítima.

O aumento e a complexidade desses delitos exige uma reinterpretação profunda sobre o conceito de materialidade probatória e a eficácia das normas processuais. Ferramentas jurídicas concebidas para lidar com crimes convencionais muitas vezes se mostram insuficientes diante de práticas como fraudes digitais, invasões de sistemas, disseminação de Fake News, assim como vazamentos de dados sensíveis.

Desse modo, não basta apenas a criação de leis para combater crimes cibernéticos. É necessário também que exista uma compreensão adequada sobre a materialidade da prova em crimes digitais (Alexandre; Araújo, 2023). Souza (2021, apud Alexandre; Araújo, 2023) analisa o caso específico do ataque cibernético na rede de informática do Superior Tribunal de Justiça em 2020, destacando a relevância da preservação e análise de evidências digitais para uma efetiva responsabilização dos agentes infratores.

Nessa perspectiva, a doutrina tem reconhecido que o enfrentamento eficaz dos crimes digitais exige uma reformulação estrutural no modo de produção e valoração das provas. Krieguer, Ceron e Marcondes (2021, apud Alexandre; Araújo, 2023) argumentam que o gap entre a evolução social e tecnológica global e a resposta legislativa tem permitido que crimes cibernéticos proliferam em um cenário de relativa impunidade. A falta de adequação a essas exigências não apenas compromete a eficiência investigativa, mas também ameaça à segurança jurídica e a própria credibilidade do sistema penal contemporâneo.

Seriam as atuais medidas de segurança digitais, suficientes para enfrentar a crescente complexidade das ameaças virtuais?

Diante disso, este artigo tem como objetivo analisar a evolução dos crimes cibernéticos e os desafios que a legislação brasileira enfrenta e demonstrar a efetividade da norma penal no combate à cibercriminalidade, em face dos desafios jurídicos, tecnológicos e estruturais que dificultam a punição e a prevenção desses crimes no cenário nacional, considerando a evolução da sociedade e dos meios de

comunicação, para proteção jurídica quanto para a preservação dos direitos fundamentais dos indivíduos.

Nesse contexto, foram realizadas pesquisas bibliográficas e análises de jurisprudências sobre a temática no combate à cibercriminalidade. Do ponto de vista social e jurídico, o estudo contribui para a proteção de direitos fundamentais, como a privacidade e a segurança digital, além de subsidiar o aprimoramento das políticas públicas e da legislação penal no combate às condutas ilícitas cibernéticas.

Assim, a pesquisa justifica-se pela necessidade de promover uma reflexão crítica acerca da efetividade da norma penal diante das inovações tecnológicas, buscando apontar caminhos para o fortalecimento do sistema de justiça e para a construção de estratégias mais eficientes de prevenção e repressão à cibercriminalidade no brasil.

2 NOÇÕES GERAIS E CLASSIFICAÇÕES DOS CRIMES VIRTUAIS

O avanço tecnológico e a massificação da internet trouxeram inúmeros benefícios à sociedade contemporânea, porém, também abriram espaço para novas modalidades de ilícitos penais, conhecidos como crimes virtuais ou cibernéticos. Esses delitos se diferenciam por terem como meio de execução ou como alvo o ambiente digital, caracterizando-se pela utilização de computadores, redes de comunicação e dispositivos eletrônicos para a prática de condutas ilícitas. Nesse contexto, torna-se indispensável compreender suas noções gerais e respectivas classificações, a fim de oferecer respostas adequadas no âmbito jurídico e social.

Em termos conceituais, os crimes virtuais podem ser definidos como todas as condutas típicas, antijurídicas e culpáveis cometidas no ambiente digital ou por meio de recursos tecnológicos. Eles podem se manifestar de forma direta, quando a tecnologia é o objeto imediato da infração, ou indireta, quando o crime tradicional se vale das ferramentas digitais para alcançar a vítima.

Sendo assim, a evolução dos crimes cibernéticos representa um dos maiores desafios do século XXI para o Direito Penal. As transformações tecnológicas, a velocidade de propagação da informação e a natureza global da internet exigem uma resposta rápida, integrada e eficiente por parte dos órgãos responsáveis por

garantir a segurança e a justiça. Hernandez e De Toledo (2021, apud Alexandre; Araújo, 2023) reiteram que, diante deste cenário, é imperativo que o ordenamento jurídico esteja em constante atualização, de forma a responder adequadamente aos novos desafios impostos pelos crimes cibernéticos.

Observa-se que não se trata de um novo ramo do direito penal, mas de novas formas de incidência de tipos penais já previstos, adaptadas às particularidades do ciberespaço.

Quanto à classificação, a doutrina costuma dividi-los em duas categorias principais: os crimes virtuais próprios e os impróprios. Os crimes virtuais próprios são aqueles que somente podem ser praticados por meio eletrônico, como a invasão de dispositivos informáticos, a disseminação de vírus e os ataques de negação de serviço (DDoS). Já os crimes virtuais impróprios correspondem a delitos comuns, todavia, utilizam recursos tecnológicos como meio de execução, a exemplo da prática de estelionato por fraude eletrônica, da difamação em redes sociais e da pedofilia online. Essa distinção é essencial para compreender o alcance da responsabilização penal e a aplicação das normas vigentes.

Além disso, a globalização da internet trouxe desafios jurisdicionais. Cazaroti e Pinheiro (2021, apud Alexandre; Araújo, 2023) ressaltam a dificuldade em lidar com crimes que transcendem fronteiras nacionais, exigindo cooperação internacional para rastrear e punir responsáveis que podem estar atuando em qualquer canto do mundo. A transnacionalidade das condutas, a dificuldade de identificação dos agentes e a volatilidade das provas digitais exigem maior cooperação internacional, bem como investimentos em legislação especializada e em técnicas de investigação cibernética.

Hernandez e De Toledo (2021, apud Alexandre; Araújo, 2023) sublinham a maneira como, paralelamente ao desenvolvimento tecnológico, surgiu uma subcultura de hackers, que, motivados por diversas razões, desde a busca por reconhecimento até objetivos políticos ou financeiros, desafiavam constantemente as medidas de segurança existentes.

A virada do milênio marcou uma nova era para os crimes cibernéticos. Com o surgimento e popularização das redes sociais, e-commerce e serviços bancários online, os criminosos encontraram novos alvos. Souza e Cervinski (2021, apud Alexandre; Araújo, 2023) discorrem sobre como a crescente digitalização de serviços e informações pessoais tornou-se um chamariz para ações mal-

intencionadas Silva e Da Silva (2019, apud Alexandre; Araújo, 2023) destacam a urgente necessidade de novas ferramentas de investigação que sejam eficazes frente ao crescente número e sofisticação dos crimes cibernéticos. Mais do que isso, é essencial que o aparato legal também evolua, a fim de proporcionar o devido enquadramento e combate a tais delitos.

Além disso, observa-se que a expansão das interações sociais, econômicas e institucionais em ambientes digitais tem ampliado a complexidade das condutas criminosas e, consequentemente, a necessidade de respostas jurídicas mais estruturadas. Nesse cenário, o debate sobre criminalidade cibernética ultrapassa a esfera estritamente penal e envolve aspectos técnicos, institucionais e cooperativos, sobretudo no que se refere à harmonização de práticas de coleta, preservação e análise de evidências digitais, bem como à integração entre órgãos nacionais e cooperação internacional para o compartilhamento seguro e eficaz de informações.

3 A CIBERCRIMINALIDADE E OS DESAFIOS DA NORMA PENAL

No cenário contemporâneo, a crescente digitalização dos serviços públicos e privados ampliou significativamente as possibilidades de ocorrência de crimes informáticos, especialmente no âmbito do Poder Judiciário. Assim, torna-se essencial compreender como o Direito Penal e o Direito Processual Penal respondem a essa nova realidade digital, bem como analisar as lacunas existentes na legislação vigente.

Em primeiro lugar, é importante destacar que a legislação penal brasileira foi concebida em um contexto analógico, sendo, portanto, limitada diante da complexidade das práticas delituosas digitais. Sendo assim, a legislação penal tradicional não foi construída para lidar com os crimes cometidos no ambiente digital, onde o tempo é instantâneo, a autoria é difícil de rastrear e as fronteiras geográficas são irrelevantes.

Nogueira e Nolasco (2022, apud Alexandre; Araújo, 2023) argumentam que os crimes cibernéticos representam um desafio significativo para o Direito, uma vez que sua natureza e métodos de atuação são distintos dos crimes tradicionais, o que exige uma abordagem jurídica diferenciada e mais adaptada à realidade virtual. Agrava-se esse cenário pela questão da jurisdição internacional, uma vez que muitos delitos virtuais envolvem agentes ou servidores localizados em outros países.

Nesses casos, a cooperação jurídica internacional torna-se indispensável, mas ainda é limitada por entraves burocráticos e pela ausência de uniformidade legislativa entre os ordenamentos nacionais, o que reforça a importância do princípio da extraterritorialidade.

No âmbito do Poder Judiciário, a mera tipificação legal mostra-se insuficiente diante da natureza técnica e volátil dos elementos digitais. Conforme o Relatório de Justiça em Números (CNJ, 2024), houve um aumento de 37% nos processos envolvendo crimes cibernéticos entre 2022 e 2024, porém apenas 41% dos casos foram efetivamente concluídos, evidenciando dificuldades estruturais e periciais que comprometem a efetividade da resposta penal. Além disso, o mesmo relatório aponta que somente 18% dos magistrados brasileiros receberam treinamento específico sobre prova digital, o que reforça a carência de capacitação técnica entre os operadores do Direito.

Embora o Brasil possua um conjunto normativo relevante, a realidade demonstra que ainda há lacunas entre a previsão legal e sua efetividade prática.

Dados recentes reforçam essa necessidade de aprimoramento. Em 2024, foram registradas 100.077 novas ocorrências de crimes cibernéticos no Brasil, segundo a SaferNet, representando uma redução de cerca de 33% em relação a 2023, mas ainda refletindo números expressivos (Safernet, 2024). Deste total, 52.999 denúncias estavam relacionadas à disseminação de imagens de abuso e exploração sexual infantil, uma queda de 26% frente ao ano anterior (Istoé dinheiro, 2024). Apesar dessa aparente redução, outros levantamentos apontam um crescimento acentuado de crimes digitais ao longo do último quinquênio: entre 2020 e 2025, houve um aumento de aproximadamente 800% nas ocorrências desse tipo de delito, com 80% dos casos decorrentes de práticas de engenharia social, como golpes e fraudes virtuais (Baguete, 2025).

No aspecto econômico, os ataques cibernéticos causaram em 2024 um prejuízo estimado em R$2,3 trilhões, o equivalente a 18% do PIB brasileiro, com custo médio de R$15,4 milhões por violação de dados (Incc, 2024). Além disso, cerca de 41 milhões de brasileiros com mais de 16 anos, aproximadamente 24% da população dessa faixa etária, afirmaram já ter sido vítimas de golpes digitais, totalizando R$10,1 bilhões em perdas financeiras (Ceub, 2024). Tais números evidenciam não apenas a dimensão econômica do problema, mas também sua abrangência social.

Além das perdas financeiras diretas, os crimes cibernéticos também acarretam custos intangíveis para as empresas, como a perda da reputação, a desvalorização da marca e a perda de confiança dos clientes. Esse aspecto social é crítico, uma vez que a confiança é um dos pilares do comércio eletrônico e das interações online (Marra, 2019, apud Alexandre; Araújo, 2023).

Segundo dados da Federação Brasileira de Bancos (Febraban), as tentativas de golpes virtuais aumentaram 81% em 2024, gerando prejuízos superiores a R$2,5 bilhões apenas no setor bancário (Febraban, 2025). O Banco Central do Brasil (2024) complementa que 74% das fraudes financeiras reportadas no país decorreram de meios eletrônicos, demonstrando a predominância das práticas informacionais sobre os crimes patrimoniais tradicionais. Esses dados refletem a necessidade de um constante aperfeiçoamento normativo e de mecanismos técnicos capazes de acompanhar o dinamismo do ambiente digital.

No próprio âmbito institucional, o Superior Tribunal de Justiça (STJ) foi alvo, em 2020, de um ataque cibernético do tipo *ransomware* que paralisou seus sistemas por dias, comprometendo o acesso processual e evidenciando falhas estruturais na segurança digital do Poder Judiciário (Migalhas, 2023). Esse episódio ilustra a vulnerabilidade das instituições e reforça a necessidade de fortalecimento técnico e jurídico no combate à cibercriminalidade.

Dessa forma, não basta apenas adaptar os tipos penais já existentes, mas repensar a estrutura normativa e os instrumentos legais disponíveis, de modo a garantir respostas mais efetivas por parte do sistema penal.

O debate acerca da criminalidade cibernética e da efetividade das normas penais no ambiente digital, problematizam a insuficiência dos instrumentos jurídicos tradicionais diante da velocidade e da complexidade tecnológica.

O direito digital deve ser compreendido como um ramo transversal, que influencia diretamente na forma como os indivíduos exercem sua cidadania e como o Estado deve proteger direitos fundamentais em ambiente virtual, de modo que a tutela penal deve ser complementada por políticas públicas de prevenção e educação digital, de forma a enfatizar que a falta de atualização contínua da legislação compromete a eficácia da persecução penal e coloca em risco a proteção da intimidade digital e da segurança coletiva. Sua análise sustenta a relevância de reformulações legislativas, de modo que a aplicação da norma penal seja efetiva e compatível com a realidade tecnológica.

Assim, fica evidenciado que a proteção de dados pessoais e a segurança das interações virtuais tornaram-se dimensões essenciais do Estado Democrático de Direito. Para além da doutrina jurídica, relatórios técnicos de segurança digital evidenciam de forma concreta a sofisticação e o avanço dos delitos virtuais.

De acordo com dados divulgados pela Kaspersky, em 2023 foram registrados cerca de 33,8 milhões de ataques a dispositivos móveis em todo o mundo, representando um aumento de aproximadamente 50% em relação ao ano anterior. Ainda segundo a empresa, as ameaças do tipo adware corresponderam a cerca de 40,8% desses incidentes, evidenciando o crescimento e a diversificação das técnicas empregadas pelos cibercriminosos (Kaspersky, 2023).

Esses dados empíricos reforçam a urgência de um aperfeiçoamento legislativo e investigativo, diante de um cenário real e crescente, e não apenas de abstrações teóricas. No campo específico da persecução penal, a obra de Higor Vinícius Nogueira Jorge, Investigação Criminal Tecnológica (2018), assume relevância por tratar da aplicação de técnicas forenses e de inteligência digital na apuração de delitos cibernéticos. O autor evidencia que a volatilidade e a fragilidade das provas digitais impõem aos órgãos de investigação a adoção de protocolos técnicos rigorosos de coleta, preservação e análise de dados, sob pena de comprometer a validade jurídica das evidências. Além disso, Jorge destaca a necessidade de capacitação constante dos operadores do direito e da integração entre polícia, Ministério Público e perícia criminal, a fim de se evitar a impunidade decorrente da ineficiência investigativa.

Dessa forma, a obra contribui para reforçar a compreensão de que a efetividade da norma penal no ambiente digital depende não apenas da atualização legislativa, mas também da modernização dos mecanismos de investigação e integração normativa entre os países, a persecução penal no ciberespaço torna-se limitada, comprometendo a efetividade das normas e favorecendo a impunidade. Compreende-se que a criminalidade digital impõe à ciência penal múltiplos desafios, entre eles: (i) reinterpretar a legislação, para assegurar sua eficácia diante das novas condutas ilícitas; (ii) repensar a cidadania digital, de modo a equilibrar a proteção jurídica e o uso social da tecnologia; e (iii) fortalecer a cooperação e a investigação transnacional, possibilitando uma atuação estatal mais efetiva frente à dinamicidade e à volatilidade dos crimes virtuais.

4 DA EFETIVIDADE DA NORMA PENAL NO ENFRENTAMENTO A CIBERCRIMINALIDADE

A crescente incidência de crimes cibernéticos no cenário brasileiro evidencia a urgência de uma análise abrangente sob as perspectivas peculiares que desafiam tanto a estrutura do ordenamento jurídico quanto social em relação a esses delitos, caracterizados pela utilização de recursos tecnológicos para a prática de condutas ilícitas. Compreender as causas e as consequências desses crimes é fundamental para mensurar os impactos que vão além das vítimas individuais, alcançando também a coletividade, a economia e a própria credibilidade das instituições públicas.

A evolução dos crimes eletrônicos e a consequente necessidade de um arcabouço legal específico para sua regulamentação e repressão são evidentes. No entanto, a implementação dessas leis enfrenta desafios, visto que a tecnologia evolui em um ritmo mais rápido do que as leis conseguem acompanhar (Almeida; de Oliveira, 2022, apud Alexandre; Araújo, 2023).

Sob o viés jurídico, o estudo da efetividade das normas penais revela-se indispensável para compreender se o aparato legislativo vigente é capaz de oferecer respostas adequadas às novas modalidades de criminalidade digital.

Na esfera social, a análise dos crimes cibernéticos permite observar como a vulnerabilidade digital afeta o exercício da cidadania e a garantia de direitos básicos, como a privacidade, a liberdade de expressão e a segurança digital.

A sociedade ainda se encontra despreparada para lidar com as complexidades da era digital, o que torna urgente o investimento em educação tecnológica, políticas públicas de conscientização e ampliação das estruturas institucionais de combate a esses delitos.

Ressalta-se que a promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi um marco inicial no processo de tipificação penal dos crimes informáticos, ao estabelecer sanções para a invasão de dispositivos eletrônicos e para a violação de dados pessoais, bem como a Lei 12.965/2014, conhecida como Marco Civil da Internet, representou uma ferramenta importante para regular a internet no Brasil, especialmente em relação ao direito à privacidade online. Entretanto, Calgaroto (2021, apud Alexandre; Araújo, 2023) ressalta que, apesar das inovações trazidas por esta lei, ainda há desafios pendentes em relação à

responsabilização civil e à proteção efetiva dos direitos dos usuários.

A Lei nº 12.735/2012, conhecida como Lei Azeredo, proposta pelo Senador Eduardo Azeredo, sucedendo os projetos de lei nº 89/2003, nº 76/2000 e 137/2000, sancionada em 30 de novembro de 2012, e teve como objetivo primordial tipificar condutas executadas por meio de sistemas eletrônicos digitais, ou similares, e aquelas perpetradas contra sistemas informatizados e seus equivalentes, representando um mecanismo jurídico relevante no combate aos crimes cibernéticos no Brasil.

Os primeiros artigos dessa lei, tratam da tipificação de delitos praticados no ambiente virtual, as condutas relacionadas à falsificação de cartão de crédito e ao delito em favor do inimigo, já previstas no Código Penal e no Código Penal Militar, respectivamente, foram inicialmente contempladas nos artigos 2º e 3º, porém vedadas na sanção final da lei. Bem como, contemplou aspectos processuais e penais na luta contra os crimes digitais, conforme o artigo 4º 34, no qual fundamentou a criação de órgãos especializados nesse combate, tendo em vista que a investigação desses delitos geralmente inicia com a localização e manuseio de equipamentos informáticos e dos dados ali armazenados, demandando assim profissionais tecnicamente preparados (Vieira, 2023).

Posteriormente, a Lei nº 14.155/2021 reforçou esse movimento ao endurecer as penas aplicáveis a crimes como o estelionato praticado por meios eletrônicos, refletindo a crescente preocupação do legislador com a sofisticação das fraudes digitais. Embora represente um avanço, a lei ainda deixa espaço para interpretações variadas e não abrange todas as modalidades possíveis desse crime.

Diz Galdino Siqueira (Oliveira, 2022) que, “se, no furto, há a tirada às mais das vezes, oculta e sempre invito domino se, no roubo e na extorsão, há o emprego de violência ou de meio intimidativo, no estelionato, o engano é o meio empregado pelo agente para determinar, em seu proveito que, outro, em prejuízo próprio, lhe transfira a coisa. Por isso mesmo que o engano é preordenadamente empregado para conseguir a disposição patrimonial, é um engano artificioso, engendrado e causativo da mesma disposição”.

É relevante destacar os esforços recentes para modernizar a legislação. Gomes e Medrado (2023, apud Alexandre; Araújo, 2023) trazem uma ponderação sobre a Lei 14.155 de 2021, que trata especificamente do crime de estelionato virtual, demonstrando um movimento legislativo em busca de respostas mais atuais

aos desafios impostos pelo ambiente digital.

No contexto de crimes cibernéticos, a determinação da responsabilidade e a identificação do autor são tarefas hercúleas. Com a globalização das redes e a multiplicidade de jurisdições envolvidas em um único ato delituoso, o princípio da extraterritorialidade torna se cada vez mais relevante, mas ao mesmo tempo, complexo (Lira; Salgado, 2021, apud Alexandre; Araújo, 2023).

Um passo relevante na esfera internacional foi a adesão do Brasil à Convenção de Budapeste, em 2023, a qual busca harmonizar legislações e fortalecer a cooperação entre Estados no combate à cibercriminalidade. Embora a Convenção de Budapeste tenha sido criticada por alguns países e organizações devido a preocupações sobre a privacidade e a liberdade de expressão, ela se tornou um referencial importante na luta contra o cibercrime em nível global. Assim, este marco representa o primeiro instrumento jurídico transnacional para a regulamentação da internet, fornecendo um modelo e parâmetro a ser adotado nas legislações dos países signatários e influenciando a doutrina e as decisões judiciais dos países não signatários, dada a sua importância no tema (Vieira, 2023).

Sob essa visão, a Convenção de Budapeste, e sua perspectiva jurídica, definem e categorizam cibercrimes em diversas infrações: contra sistemas e dados informáticos, delitos associados ao uso de computadores, infrações de conteúdo específico como pornografia infantil, e violações relacionadas, chegando até direitos autorais.

Com o Brasil se tornando signatário da Convenção, acabou por proporcionar às autoridades brasileiras um acesso mais amplo e ágil às provas eletrônicas e outros elementos informativos sob jurisdição estrangeira, além de tornar mais efetiva a cooperação jurídica internacional no combate a esses crimes, que transcende fronteiras.

Em julho de 2020, o Brasil submeteu ao Congresso Nacional a Convenção de Budapeste sobre Cibercrime para apreciação e possível ratificação, passando, desde então, a participar das reuniões internacionais como país observador até a conclusão do processo legislativo. Tal iniciativa está alinhada aos princípios estabelecidos pelo Marco Civil da Internet e demonstra o reconhecimento da necessidade de aprimorar os instrumentos de persecução penal diante das especificidades dos delitos praticados no ambiente virtual, cuja dinâmica exige respostas ágeis e eficientes para prevenir, identificar e reprimir condutas ilícitas.

Ainda que o país disponha de dispositivos legais voltados ao combate dos crimes cibernéticos, a dimensão transnacional dessas práticas revela limitações da atuação isolada do Estado brasileiro. Nesse sentido, a adesão à Convenção constitui medida indispensável para reforçar o arcabouço jurídico nacional, ampliando a cooperação internacional e estabelecendo diretrizes mais eficazes para o enfrentamento penal no meio digital.

Entretanto, a eficácia dessa integração internacional depende da internalização efetiva de seus preceitos, com a implementação de estruturas normativas, técnicas e institucionais capazes de assegurar a cooperação entre autoridades e a execução rápida de medidas investigativas que extrapolam fronteiras nacionais.

Observa-se que, apesar dos avanços normativos e institucionais, a realidade prática ainda impõe obstáculos significativos à persecução penal dos crimes cibernéticos. A prova digital, por sua natureza instável e suscetível a alterações, demanda procedimentos técnicos rigorosos de coleta, preservação e análise, recursos que nem sempre estão plenamente disponíveis às autoridades brasileiras.

A identificação dos responsáveis também enfrenta entraves decorrentes do uso de mecanismos de anonimização, como redes privadas virtuais (VPNs) e navegadores que ocultam o endereço de origem, o que dificulta o rastreamento das ações ilícitas. A sensação de impunidade é outro fator que potencializa os crimes cibernéticos. Essa sensação é muitas vezes decorrente da dificuldade em identificar e punir os perpetradores e também da falta de conhecimento por parte das vítimas sobre seus direitos e as medidas legais que podem adotar (Cruz; Rodrigues, 2018, apud Alexandre; Araújo, 2023).

A norma existe, mas sua concretização se enfraquece quando as limitações probatórias impedem a responsabilização dos agentes.

O combate aos crimes cibernéticos também demanda ferramentas de investigação avançadas e adaptadas à natureza volátil do mundo digital. É essencial que as autoridades estejam equipadas não apenas para identificar e punir os criminosos, mas também para coletar e preservar evidências digitais que possam ser usadas em processos judiciais (Silva; da Silva, 2019, apud Alexandre; Araújo, 2023).

Bonini et al. (2018, apud ALexandre; Araújo, 2023) analisam os crimes cibernéticos de forma ampla e identificam que a velocidade das mudanças

tecnológicas exige uma atualização constante da legislação. Muitas vezes, quando uma lei é finalmente promulgada, os criminosos já desenvolveram novas formas de atuação, tornando a legislação rapidamente obsoleta ou insuficiente.

De acordo com pesquisa recente do Instituto Da taSenado (2024), quase um quarto da população brasileira (24%) afirmou ter sido vítima de golpes digitais no último ano, o que representa mais de 40 milhões de pessoas. Esses números revelam que o avanço tecnológico tem sido acompanhado por um crescimento expressivo das práticas criminosas virtuais, exigindo respostas mais eficazes do sistema penal.

Nessa mesma linha, as fraudes eletrônicas, no qual buscam obter ganhos financeiros ilegítimos através de técnicas de engenharia social, como phishing e spoofing, por meio de envio de mensagens falsas que se passam por comunicações autênticas de empresas conhecidas, como bancos ou lojas online (Vieira, 2023).

Sob essa perspectiva, evidencia-se que computadores e a internet não se limitam a instrumentos de utilidade e produtividade, mas também podem ser utilizados para práticas ilícitas. A ausência de proteção adequada e a vulnerabilidade das redes tornam os crimes cibernéticos um desafio global, muitas vezes configurando adaptações digitais de delitos já conhecidos no meio tradicional. Diante disso, é essencial compreender essas condutas e suas particularidades, adotando estratégias eficazes de prevenção e investigação.

Uma das maiores inquietações reside na efetivação da instrução probatória em ações penais relacionadas a crimes virtuais. A natureza intangível e volátil dos dados digitais e a falta de capacitação técnica muitas vezes limitam a ação do judiciário. Não raro, evidências cruciais se perdem ou se tornam inacessíveis antes que possam ser adequadamente coletadas e analisadas (Santana, 2019, apud Alexandre; Araújo, 2023).

A efetividade da norma penal no enfrentamento da cibercriminalidade não se esgota na criação de tipos penais específicos. Ao contrário, depende de uma estrutura integrada que envolva o aprimoramento técnico dos profissionais da área, a consolidação de unidades especializadas em investigação digital, o fortalecimento da cooperação com provedores e empresas de tecnologia, bem como a ampliação da conscientização social acerca dos riscos e das formas de prevenção no ambiente virtual.

5 O PAPEL DA JURISPRUDÊNCIA NO COMBATE À CIBERCRIMINALIDADE

A análise jurisprudencial permite avaliar em que medida a norma penal tem sido efetiva no enfrentamento da cibercriminalidade, de modo que sua eficácia depende menos da positivação abstrata e mais da concretização prática. Essa perspectiva se torna crucial diante da criminalidade digital, cujas condutas desafiam os meios tradicionais de persecução penal e, em alguns casos, atingem o Poder Judiciário.

Assim, a jurisprudência atua como instrumento de interpretação e adaptação do ordenamento jurídico às novas realidades digitais. Nos crimes cibernéticos, como fraudes eletrônicas, invasões de dispositivos, e golpes por aplicativos de mensagens, os tribunais exercem função hermenêutica e integrativa, aplicando normas penais tradicionais, como o art. 171 do Código Penal que trata do estelionato e as condutas praticadas por meio eletrônico. No caso da Apelação Criminal nº 0724838-25.2022.8.07.0001, o TJDFT confirmou a configuração do estelionato qualificado pela fraude eletrônica, contemplado no art. 171, §2º-A do Código Penal, demonstrando como o Judiciário tem adaptado o tipo penal às novas modalidades de golpe praticadas em ambientes virtuais, como no caso, via WhatsApp.

O Superior Tribunal de Justiça (STJ) já enfrentou casos de clonagem de cartões e transferências eletrônicas fraudulentas Todavia, ressaltou a dificuldade de apuração da autoria devido à ausência de rastreamento confiável dos sistemas bancários. Esse julgado evidencia a crítica de Ferrajoli (2002, p. 95), para quem a legitimidade da pena depende da previsibilidade e da efetividade da resposta estatal.

A vulnerabilidade do Judiciário frente às manipulações digitais reitera que a norma penal perde força, tanto simbólica quanto prática. Podemos ver isso com a popularização do sistema de pagamentos instantâneos (PIX), que resultou no aumento expressivo dos golpes digitais. No AgRg no REsp 1.985.490/SP (2022), o STJ enquadrou a conduta como estelionato, mas ressaltou a importância da cooperação entre o Judiciário e as instituições financeiras para o rastreamento das operações. A decisão evidencia que a resposta estatal depende da integração tecnológica e da cooperação internacional, sob pena de a norma penal permanecer apenas no plano simbólico. Em suma, a fraude no Judiciário compromete a legitimidade da jurisdição, transformando a vulnerabilidade tecnológica em obstáculo

à efetividade da norma penal. Com a promulgação da Lei nº 14.155, de 27 de maio de 2021, o ordenamento jurídico brasileiro avançou no enfrentamento do estelionato praticado por meios eletrônicos ou digitais. Essa lei introduziu, no Código Penal, Decreto-Lei nº 2.848/1940, o § 2º-A do art. 171, qualificando a fraude eletrônica e estabelecendo pena de reclusão de 4 a 8 anos e multa quando “a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo”.

Além disso, a mesma lei alterou o Código de Processo Penal, acrescentando o § 4º ao art. 70, que determina que, nos casos de estelionato praticados mediante depósito, emissão de cheques sem fundos ou com pagamento frustrado, ou mediante transferência de valores, a competência territorial será do domicílio da vítima. Em situações envolvendo múltiplas vítimas, aplica-se a prevenção. Tal medida facilita o acesso à Justiça, evitando deslocamentos e litígios territoriais complexos.

Diante desse cenário, torna-se evidente que o enfrentamento do estelionato digital e da fraude eletrônica exige não apenas normas específicas, mas também capacitação técnica dos operadores do Direito, padronização de procedimentos investigativos e cooperação internacional efetiva. Somente a conjugação desses fatores permite proteger adequadamente as vítimas, preservar a integridade das provas e garantir a efetividade da persecução penal no ambiente digital.

6 CONSIDERAÇÕES FINAIS

No contexto dos crimes cibernéticos, observa-se que, apesar dos avanços normativos alcançados nas últimas décadas, o ordenamento jurídico brasileiro ainda enfrenta significativas limitações diante da velocidade das transformações tecnológicas e das condutas ilícitas praticadas no ambiente digital. A sensação de impunidade, frequentemente alimentada pela dificuldade de identificação e responsabilização dos agentes, evidencia a urgência de fortalecer os mecanismos de investigação e de ampliar a cooperação internacional para o enfrentamento efetivo dessas práticas delitivas.

Nessa perspectiva, a garantia da integridade das evidências digitais, bem como o respeito à cadeia de custódia e à sua correta admissibilidade processual,

demandam aprimoramentos tanto de natureza legal quanto técnica, a fim de assegurar decisões judiciais justas, seguras e eficazes. A dinâmica própria do ciberespaço impõe, portanto, uma abordagem jurídica adaptada, capaz de harmonizar os recursos tecnológicos disponíveis com as garantias processuais inerentes ao Estado Democrático de Direito.

A compreensão de suas noções gerais e classificações não apenas contribui para uma aplicação mais adequada do Direito Penal, como também fortalece a proteção da sociedade em um ambiente digital cada vez mais presente no cotidiano. Dessa forma, os crimes virtuais configuram um dos maiores desafios contemporâneos para o sistema de justiça, exigindo uma reflexão interdisciplinar e respostas jurídicas concretas. Sem a devida adaptação do Direito Penal à realidade digital, a norma perde sua efetividade, sobretudo diante de fraudes e delitos que ocorrem, paradoxalmente, no próprio ambiente institucional encarregado de combatê-los.

Conclui-se, que se torna imprescindível reavaliar os fundamentos da legislação penal brasileira à luz das inovações tecnológicas, buscando assegurar um sistema de justiça eficiente, legítimo e alinhado às demandas da era digital.

Somente por meio da integração entre tecnologia, políticas públicas, capacitação técnica dos operadores do Direito e atuação coordenada do sistema de justiça será possível tornar o enfrentamento da cibercriminalidade mais efetivo, garantindo a autonomia e a efetividade das medidas protetivas e, consequentemente, fortalecendo a confiança social na tutela penal em um mundo cada vez mais conectado.

REFERÊNCIAS

ALEXANDRE, Brenda Cristina; ARAÚJO, Giulianna Martins. **A evolução dos crimes cibernéticos e os desafios da legislação brasileira**. Revista FT – Ciências Humanas, Rio de Janeiro, v. 27, n. 128, nov. 2023. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 18 out. 2025.

BAGUETE. **Crimes digitais crescem 800% em cinco anos**. 2025. Disponível em:

https://www.baguete.com.br/noticias/crimes-digitais-crescem-800-em-cinco-anos. Acesso em: 28 out. 2025.

BANCO CENTRAL DO BRASIL. **Relatório de fraudes eletrônicas 2024**. Brasília, 2024. Disponível em: https://www.bcb.gov.br. Acesso em: 28 out. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências**. Diário Oficial da União: Seção 1, Brasília, DF, 3 dez. 2012.

BRASIL. **Lei nº 14.132, de 31 de março de 2021. Altera o Código Penal para incluir o crime de perseguição (stalking)**. Diário Oficial da União: Seção 1, Brasília, DF, 1º abr. 2021.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para agravar penas de crimes patrimoniais praticados com uso de dispositivo eletrônico, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir competência em modalidades de estelionato**. Diário Oficial da União: Poder Legislativo, Brasília, DF, 28 maio 2021. ,Disponível em: https://legis.senado.leg.br/norma/34016289. Acesso em: 8 out. 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. **Apelação Criminal nº 0724838-25.2022.8.07.0001**, 1ª Turma Criminal, Rel. Des. Esdras Neves; Rev. Desª Leila Arlanch, Brasília, DF, julgado em 25 abr. 2025. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2025/abril/tjdft-mantem-condenacao-por-estelionato-praticado-contra-idosa-via-whatsapp. Acesso em: 9 nov. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **Agravo Regimental no Recurso Especial n. 1.985.490 – SP**. Relator: Ministro Reynaldo Soares da Fonseca. Jurisdição: Federal. Órgão julgador: Quinta Turma. Julgado em: 14 jun. 2022. Local: Brasília, DF. Publicação: Diário da Justiça Eletrônico, Brasília, DF, 20 jun. 2022.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012. Dispõe sobre a obrigatoriedade de os órgãos da polícia judiciária estruturarem setores e equipes especializadas no combate à ação de criminosos que utilizem a rede de computadores, ou meios de comunicação semelhantes, para a prática de delitos.** Diário Oficial da União: seção 1, Brasília, DF, 3 dez. 2012.

CEUB – AGÊNCIA DE NOTÍCIAS. **O DF registra 8.921 inquéritos para investigar crimes cibernéticos em 3 anos**. 2024. Disponível: https://agenciadenoticias.uniceub.br/destaque/df-registra-8-921-inqueritos-para-investigar-crimes-ciberneticos-em-3-anos/. Acesso em 29out.2025

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Justiça em números 2024**. Brasília: CNJ, 2024. Disponível em: https://www.cnj.jus.br . Acesso em: 28 out. 2025.

DATASENADO. **Pesquisa sobre golpes digitais no Brasil – 2024**. Brasília, DF: Senado Federal, 2024. Disponível em: https://www12.senado.leg.br/institucional/datasenado. Acesso em: 29 out. 2025.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Relatório de segurança bancária 2025**. São Paulo: Febraban, 2025. Disponível em: https://www.febraban.org.br . Acesso em: 28 out. 2025.

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME (INCC). **Relatório de impacto econômico dos ciberataques no Brasil 2024. 2024**. Disponível em: https://mpmt.mp.br/portalcao/news/1217/155587/ . Acesso em: 28 out. 2025.

ISTOÉ DINHEIRO. **Denúncias de crimes cibernéticos caem 33% no Brasil em 2024. 2024**. Disponível em: https://istoedinheiro.com.br/denuncias-de-crimes-ciberneticos-caem-33-no-brasil-em-2024 . Acesso em: 28 out. 2025.

JORGE, Higor Vinícius Nogueira. **Investigação criminal tecnológica**. v. 1. Rio de Janeiro: Brasport, 2018. ISBN 978-8574528977

KASPERSKY. **Relatório de ameaças na América Latina 2023**. Disponível em: https://www.kaspersky.com.br. Acesso em: 20 out. 2025.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA (MJSP**). Relatório nacional de enfrentamento aos crimes cibernéticos 2024**. Brasília: MJSP, 2024. Disponível em: https://www.gov.br/mj. Acesso em: 28 out. 2025.

MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO (MPRJ**). Lei nº 14.155/2021 dos crimes cibernéticos**. Rio de Janeiro: MPRJ, 2022. (Documento explicativo / parecer).

MIGALHAS. **Cibersegurança como pilar da justiça digital**. São Paulo, 2023. Disponível em: https://www.migalhas.com.br/depeso/428577. Acesso em: 29 out. 2025.

OAB NA MEDIDA. **Alterações importantes – Lei nº 14.155/2021**. [S. l.]: OAB, 2021. Disponível em: https://www.oabnamedida.com.br/alteracoes-importantes/lei-14-155-2021. Acesso em: 8 out. 2025.

OLIVEIRA, Wellington Antério de. **Os crimes cibernéticos e a prática do estelionato por meios eletrônicos**. 2022. Monografia (Graduação em Direito) – Universidade São Judas Tadeu (USJT), São Paulo, 2022. Disponível em: https://repositorio-api.animaeducacao.com.br/server/api/core/bitstreams/2cf07f88-c42b-4798-9f9e-3d701824f60f/content . Acesso em: 27 out. 2025.

SAFERNET BRASIL. **Relatório anual 2024: Central Nacional de Denúncias de Crimes Cibernéticos**. Disponível em: https://gmaisnoticias.com/denuncias-de-crimes-ciberneticos-caem-33-no-brasil-em-2024 . Acesso em: 28 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **HC 440.837/DF**, Rel. Min. Ribeiro Dantas, 2018.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Provas digitais devem ser colhidas com metodologia adequada – Quinta Turma não aceita como provas prints de**

celular extraídos sem metodologia adequada. Brasília: STJ, 2 maio 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/02052024-Quinta-Turma-nao-aceita-como-provas-prints-de-celular-extraidos-sem-metodologia-adequada.aspx . Acesso em: 8 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ); MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO. **STJ reconhece quebra da cadeia de custódia e anula provas digitais**. Cuiabá: MPMT, 7 mar. 2023. Disponível em: https://www.mpmt.mp.br/portalcao/news/722/122033/stj-reconhece-quebra-da-cadeia-de-custodia-e-anula-provas-digitais/9 . Acesso em: 8 out. 2025.

VIEIRA, Maria Eduarda Pereira. **A adesão do Brasil à Convenção de Budapeste e a correção das deficiências legislativas quanto aos crimes cibernéticos**. 2023. Monografia(Graduação em Direito) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Departamento de Direito, Florianópolis, 2023. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/248821/A%20ADES%C3%83O%20DO%20BRASIL%20A%20CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE%20E%20A%20CORRE%C3%87%C3%83O%20DAS%20DEFICI%C3%8ANCIAS.%20Vers%C3%A3o%20final%20-%20Documentos%20Google%20%281%29.pdf?sequence=1&isAllowed=y . Acesso em: 27 out. 2025.