CRIMES VIRTUAIS: OS DESAFIOS JURÍDICOS, A EFETIVIDADE NORMATIVA E A URGÊNCIA DE ATUALIZAÇÃO LEGAL NO BRASIL, FRENTE A ERA DIGITAL

Gesson Eliésio Aguiar de Sousa[1]
http://lattes.cnpq.br/5965100253725484
https://orcid.org/0009-0009-7523-4681
Maria Cristina Ferreira Marques[2]
http://lattes.cnpq.br/5916761448356919
https://orcid.org/0009-0009-0268-4315
Alcirene Maria da Silva Cursino[3]
http://lattes.cnpq.br/2230131687476437
https://orcid.org/0009-0006-3693-0500
Cesar Maurício de Abreu Mello[4]
http://lattes.cnpq.br/2079368341132335
https://orcid.org/0000-0003-3086-2624

Resumo

Os crimes cibernéticos constituem uma ameaça crescente à segurança digital, afetando empresas e indivíduos em escala global, e o combate a estes tipos de crimes é, por vezes, de alta complexidade, tendo em vista a necessidade de um arcabouço jurídico prevendo este crescimento exponencial, sendo, portanto, este estudo de grande relevância jurídica e social diante desta era tecnológica. Este estudo teve como objetivo central analisar a eficácia do ordenamento jurídico brasileiro no enfrentamento dos crimes virtuais, identificando lacunas legislativas que comprometam a segurança jurídica e a persecução penal. A justificativa para esta pesquisa reside na alarmante escalada dos crimes cibernéticos, que representam uma ameaça crescente à sociedade, às instituições e à economia. A defasagem entre a velocidade das transformações tecnológicas e a morosidade da adaptação legal cria um ambiente propício à impunidade, demandando uma análise crítica e propositiva sobre a adequação normativa vigente. A metodologia empregada é de natureza qualitativa e exploratória, fundamentada em revisão bibliográfica de doutrina nacional e internacional sobre direito penal informático, criminologia digital e direito comparado. Realiza-se, ainda, análise documental da legislação brasileira pertinente aos crimes virtuais. Os resultados preliminares indicam que o atual arcabouço legal brasileiro apresenta limitações significativas na tipificação de novas condutas criminosas, na delimitação de

[1] Mestrando do Curso de Mestrado Profissional em Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas – UEA. E-mail: gesson@policiacivil.am.gov.br
[2] Mestranda do Curso de Mestrado Profissional em Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas – UEA. E-mail: mcfm.msp25@uea.edu.br
[3] Pós Doutora em Filosofia, Ciências Humanas e Sociais, vice coordenadora e docente da Universidade do Estado do Amazonas. E-mail: acursino@uea.edu.br .
[4]Doutor em Desenvolvimento Sustentável do Trópico Úmido, docente do Programa de Pós-graduação em Segurança Pública da Universidade Federal do Pará. E-mail: mello.cesar@gmail.com

competências e nos obstáculos à coleta de evidências digitais. A pesquisa aponta para a necessidade imperativa de uma reforma legislativa abrangente, acompanhada de investimentos em capacitação tecnológica para as forças policiais, visando maior efetividade no combate aos crimes virtuais e a construção de um ambiente digital mais seguro.

Palavras-chave: Crimes Virtuais; Legislação Cibernética; Segurança Pública; Persecução Penal; Era Digital.

Abstract

Cybercrimes constitute a growing threat to digital security, affecting businesses and individuals on a global scale. Combating these types of crimes is often highly complex given the necessity of a legal framework capable of anticipating this exponential growth. Therefore, this study holds great legal and social relevance in this technological era. The central objective of this study was to analyze the efficacy of the Brazilian legal system in confronting virtual crimes, identifying legislative gaps that compromise legal security and criminal prosecution. The justification for this research lies in the alarming escalation of cybercrimes, which represent a growing threat to society, institutions, and the economy. The disparity between the rapid pace of technological transformations and the sluggishness of legal adaptation creates an environment conducive to impunity, thus demanding a critical and proactive analysis of the adequacy of current regulations. The methodology employed is qualitative and exploratory in nature, grounded in an extensive bibliographical review of national and international doctrine on cybercriminal law, digital criminology, and comparative law. Furthermore, a documentary analysis of pertinent Brazilian legislation concerning virtual crimes is conducted. Preliminary results indicate that the current Brazilian legal framework presents significant limitations in typifying new criminal behaviors, delimiting jurisdictions, and facilitating the collection of digital evidence. The research points to the imperative need for comprehensive legislative reform, accompanied by investments in technological training for law enforcement agencies, aiming for greater effectiveness in combating virtual crimes and fostering the creation of a safer digital environment.

Keywords: Cybercrime; Cyber Law; Information Security; Cybersecurity Governance; Legal Liability.

Introdução

Os crimes cibernéticos constituem uma ameaça crescente à segurança digital, afetando empresas e indivíduos em escala global. A complexidade crescente dessas atividades criminosas demanda uma resposta eficaz do sistema jurídico e das forças de segurança pública para salvaguardar os interesses e a privacidade das organizações, bem como a segurança dos cidadãos. A delimitação temática deste estudo aborda os crimes virtuais, os desafios jurídicos, a efetividade normativa e a urgência de atualização legal no Brasil, frente à era digital.

Conforme estudos de Sousa (2024) e França (2024), a problemática central desta pesquisa será como a atual legislação mostra-se insuficiente para enfrentar os crimes virtuais de forma eficaz em razão da rápida evolução tecnológica e da complexidade das infrações digitais o que compromete a

efetividade normativa e evidencia a necessidade urgente de atualização legal específica e adequada à era digital.

O objetivo geral desta pesquisa foi analisar a eficácia do ordenamento jurídico brasileiro no enfrentamento dos crimes virtuais, identificando lacunas legislativas que comprometam a segurança jurídica e a persecução penal. Adicionalmente, os objetivos específicos foram assim definidos: 1. Estudar o contexto histórico e a evolução dos crimes virtuais no Brasil; 2. Descrever a atual legislação brasileira referente ao combate aos crimes virtuais, incluindo leis específicas e dispositivos do Código Penal. 3. Identificar as principais lacunas na aplicação das normas brasileiras diante da complexidade e dos crescentes delitos cibernéticos.

A relevância deste tema reside na necessidade de aprofundar a compreensão das complexidades jurídicas dos crimes cibernéticos, considerando as rápidas transformações tecnológicas e suas consequências legais.

A pesquisa se justifica em razão da alarmante escalada dos crimes cibernéticos, que impuseram a todo o sistema de justiça brasileiro, um grande volume de demanda de tais crimes na segurança pública e no judiciário brasileiro quanto à resolução e ao combate a estes crimes na era digital (Uchôa, 2025).

Assim sendo, considerando a velocidade das transformações tecnológicas e a morosidade da adaptação legal, cria-se um ambiente propício à impunidade, demandando uma análise crítica e propositiva sobre a adequação normativa vigente.

Por fim, busca-se, ademais, identificar oportunidades para o aprimoramento das estruturas legais, visando um enfrentamento mais eficaz e justo dos delitos cometidos no ambiente digital, contribuindo, assim, para a construção de uma abordagem jurídica mais adequada aos desafios emergentes da sociedade digital.

Metodologia

No intuito de alcançar os objetivos propostos, utilizou-se uma metodologia, qualitativa quanto à abordagem, a fim de fornecer melhor compreensão a determinados fenômenos jurídicos e sociais. Possui pesquisa bibliográfica quanto aos procedimentos técnicos. Básica quanto à natureza metodológica, pois se justifica por gerar conhecimentos novos, uteis para o avanço da ciência, porém sem aplicação prática prevista, assim como defende Gerhardt (2009), haja vista o que se busca nesse estudo é estabelecer um entendimento e reflexão, entre a eficiência e eficácia legislativa brasileira em contrapartida ao combate aos crimes virtuais no Brasil. Em relação às referências legislativas estrangeiras utilizadas neste estudo, todas foram traduzidas para o português na sua integra por inteligência artificial

Quanto aos objetivos a pesquisa é exploratória, por envolver levantamento bibliográfico, com fulcro nos estudos de (Gil, 1987): “[...] a pesquisa bibliográfica se utiliza fundamentalmente das contribuições dos diversos autores sobre determinado assunto[...]”, sendo assim, cabe esclarecer que esta pesquisa se propõe a estudar outros autores e estudos em doutrinas, leis, jurisprudências, artigos acadêmicos acerca da matéria, na busca de identificar qual entendimento têm-se das leis e normas brasileiras no que se refere ao combate dos crimes virtuais, e sua aplicabilidades no meio jurídico.

Resultados e discussões

A criminalidade no ciberespaço, fenômeno indissociável da expansão tecnológica, evoluiu das primeiras interferências experimentais para a atual industrialização dos crimes on-line. Esse processo de contínua sofisticação técnica e organizacional dos agentes ilícitos, analisado em perspectiva global e brasileira, culmina na constatação de insuficiências normativas que dificultam o enfrentamento efetivo da delinquência virtual. Conforme o que será estabelecido a partir da fundamentação teórica, a sofisticação da criminalidade no ciberespaço impõe desafios significativos à estrutura jurídica brasileira. As insuficiências normativas, apontadas como entrave central, são o foco dos **Resultados e Discussões** a seguir.

Não obstante, conforme estudos de Sousa (2024), o surgimento dos crimes virtuais é intrínseco ao desenvolvimento das redes de computadores, tendo suas raízes nas décadas de 1970 e 1980. Inicialmente, a interação com sistemas computacionais por indivíduos não autorizados era, em grande medida, motivada pela exploração intelectual e pela curiosidade tecnológica, característica da chamada *cultura hacker* primária. Nessas primeiras fases, observavam-se intrusões em redes acadêmicas e governamentais, como as pioneiras da Arpanet, a primeira rede de computadores de longa distância criada nos EUA em 1960, sem necessariamente um intuito de dano ou lucro financeiro, mas sim de demonstração de habilidade e superação de barreiras de segurança.

Ademais, com a popularização comercial da internet na década de 1990, e a consequente expansão do comércio eletrônico e dos serviços bancários online, o perfil da criminalidade cibernética começou a migrar decisivamente para o escopo lucrativo. Fraudes eletrônicas, clonagem de cartões de crédito e roubos de identidade passaram a ser perpetrados em escala crescente, demonstrando que o ambiente digital oferecia um vasto campo para a obtenção de ganhos ilícitos, superando, em muitos casos, os retornos de atos de vandalismo digital desprovidos de intenção financeira.

Sobretudo, o advento do novo milênio marcou uma nova fase na evolução dos crimes cibernéticos, caracterizada pela consolidação e complexidade das táticas criminosas, impulsionadas por três vetores principais. Em primeiro lugar, a explosão de plataformas e serviços online, como redes sociais, aplicativos de mensageria e sistemas bancários digitais, ampliou exponencialmente a *superfície de ataque* para os criminosos. Este cenário facilitou a disseminação de fraudes, campanhas de *phishing* e o roubo de credenciais em uma escala sem precedentes.

Igualmente, em segundo lugar, a atividade criminosa no ciberespaço assistiu a uma notável profissionalização e à crescente integração com organizações criminosas transnacionais. Grupos especializados passaram a operar com uma estrutura empresarial, dotados de divisão de tarefas, infraestrutura para apoio operacional como *call centers* para aplicar golpes e até mesmo mercados clandestinos como a *dark web* para a comercialização de ferramentas e serviços ilícitos.

Desse modo, o avanço tecnológico em áreas como criptografia, criptomoedas e inteligência artificial, forneceu aos criminosos ferramentas

poderosas para aprimorar suas operações. A criptografia ponta a ponta, *end-to-end* e o uso de criptomoedas, por exemplo, conferem um alto grau de anonimato aos agentes, dificultando o rastreamento e a identificação. A inteligência artificial, por sua vez, tem sido empregada para potencializar técnicas de conteúdos falsos produzidos com um alto grau de elaboração, *deepfakes,* e automatizar campanhas de *phishing* e engenharia social, tornando os golpes mais críveis e eficazes.

Contudo, no Brasil, a trajetória dos crimes virtuais acompanhou, com certo atraso inicial, as tendências globais, mas desenvolveu características próprias em virtude do contexto socioeconômico e regulatório. A primeira fase, de 2000 a 2010, foi marcada pela incipiente popularização da banda larga e pela gradual bancarização digital. A ausência de legislação específica para essas condutas no Código Penal obrigava o enquadramento em tipos penais genéricos, o que dificultava sobremaneira as investigações e a aplicação da lei. (MPF, 2018).

Todavia, a partir do ano de 2011, o cenário nacional testemunhou uma aceleração e, mais notadamente, uma industrialização dos crimes cibernéticos. Facções criminosas tradicionais, atraídas pelo menor risco e pelo alto retorno financeiro do ambiente online, começaram a migrar suas operações para o ciberespaço, profissionalizando-as. O advento do PIX, por exemplo, embora seja uma ferramenta de grande inclusão financeira, foi rapidamente cooptado por criminosos, transformando-se em um vetor para golpes instantâneos.

Não obstante, diversos fatores estruturais contribuem para a proliferação da criminalidade digital no Brasil. A rápida expansão da conectividade móvel, muitas vezes desacompanhada de educação digital adequada, especialmente em faixas etárias mais vulneráveis, cria um ambiente fértil para a atuação de golpistas. Ademais, o lucro financeiro obtido com o cibercrime, frequentemente superior ao de atividades criminosas tradicionais, estimula a migração e a profissionalização de grupos organizados, que estabelecem verdadeiros *escritórios do crime* para operar suas fraudes, conforme (Uchôa, 2025).

Acrescenta-se, a isso a percepção de um *risco jurídico reduzido* por parte dos criminosos, decorrente da defasagem normativa e da morosidade do sistema de justiça, o que potencializa a reincidência e a impunidade. A despeito dos avanços, a legislação brasileira ainda demonstra fragilidades significativas no enfrentamento dos crimes cibernéticos contemporâneos.

Os impactos dos crimes cibernéticos no Brasil são multifacetados e de grande envergadura. Economicamente, os prejuízos anuais contabilizam bilhões de reais, afetando não apenas indivíduos, que sofrem perdas financeiras significativas em golpes como o do PIX, mas também pequenas e médias empresas, que frequentemente carecem de investimentos em cibersegurança, e até mesmo instituições públicas, que se tornam alvos de sequestro de dados sensíveis.

Para além disso, socialmente, a crescente onda de fraudes e invasões digitais destrói a confiança dos cidadãos nos serviços digitais, podendo comprometer iniciativas de inclusão financeira e o desenvolvimento da economia digital como um todo. Em síntese, a trajetória histórica dos crimes virtuais demonstra uma evolução constante, em que a capacidade adaptativa dos criminosos supera, muitas vezes, a resposta normativa e institucional.

Sobre essa ótica, essa assincronia brasileira entre a velocidade da inovação tecnológica e a atualização legislativa cria um vácuo regulatório que favorece a impunidade e a proliferação dessas atividades ilícitas. Para um enfrentamento eficaz, torna-se imperativa a revisão e complementação do arcabouço legal, com a tipificação de novas condutas e o endurecimento de penas. Paralelamente, dever ser feito investimentos em alfabetização digital e em cibersegurança, tanto no setor público quanto no privado, são medidas essenciais para construir uma sociedade mais resiliente e segura no ambiente digital. Sem ações coordenadas e robustas, a expectativa é que o ciberespaço continue a ser um território preferencial para a criminalidade organizada, com consequências cada vez mais severas para a segurança pública, o judiciário e o desenvolvimento nacional.

Panorama jurídico dos crimes virtuais no Brasil

Ademais, após a análise do panorama jurídico e das lacunas e inadequações da legislação brasileira em matéria de crimes cibernéticos, voltamos agora o olhar para as condutas que já possuem tipificação específica e consideramos, em grande parte, adequada. É fundamental entender que *adequada* não significa *perfeita* ou *exaustiva*, mas sim que o tipo penal existente consegue, com razoável clareza e abrangência, enquadrar o comportamento criminoso digital ao qual se propõe, permitindo a persecução penal. Mesmo nos casos considerados adequados, a rápida evolução tecnológica e os novos modus operandi de criminosos impõem desafios contínuos. A adequação é um conceito dinâmico, e o que é suficiente hoje pode não ser amanhã.

Dessa forma, para cada crime cibernético que possui uma lei específica no Brasil, será avaliada a eficácia do tipo penal em cobrir a conduta, a clareza de sua redação e os desafios práticos de sua aplicação. Serão incluídos comparativos internacionais para verificar se a abordagem brasileira se alinha com as melhores práticas globais ou se há oportunidades de aprimoramento.

De modo que, em relação à legislação brasileira e tipificação, o crime de invasão de dispositivo informático está previsto no Art. 154-A conduta de *invadir dispositivo informático alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita,* introduzido pela lei n.º 12.737/2012, conhecida como lei *Carolina Dieckmann*. Sendo que o § 3º, que aumenta a pena se a invasão resultar na obtenção de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais ou controle remoto não autorizado, foi adicionado pela lei n.º 14.155/2021 (Mendes, 2021).

Nesse sentido, os aspectos positivos do artigo 154-A é um marco, pois definiu de maneira explícita uma das ações mais fundamentais do cibercrime: o acesso não autorizado. A inclusão da *instalação de vulnerabilidades* e o reconhecimento da invasão em dispositivos conectados e não conectados são amplos. A lei n.º 14.155/2021 reforçou a tipificação ao estabelecer agravantes específicos para a obtenção de dados sensíveis, em consonância com a

preocupação com a privacidade e o sigilo das informações. A pena também é apropriada para o crime base, com possibilidade de agravamento em situações mais sérias (Mendes, 2021).

Apesar de, sobre as limitações e desafios na aplicação: a compreensão de *fim específico* e *com o fim de obter* pode levar a debates acerca da exigência de dolo específico, complicando a demonstração em situações em que o propósito não é tão evidente. Apesar de ser abrangente, a expressão "dispositivo informático" pode gerar discussões devido à variedade de aparelhos e ao uso de técnicas cada vez mais avançadas.

Desse modo, ao analisar o comparativo internacional, podemos observar que a tipificação brasileira está em conformidade com as disposições do Art. 2º da Convenção de Budapeste, que trata do "Acesso ilegal". Essa tipificação criminaliza o acesso intencional e não autorizado a um sistema de computador ou a qualquer parte dele. Leis como a CFAA, Computer Fraud and Abuse Act dos EUA e a Diretiva 2013/40/EU da União Europeia tratam de maneira semelhante o acesso não autorizado, enfatizando a intenção e a falta de autorização.

Ainda assim, a lei n.º 14.155/2021 trouxe mudanças significativas aos crimes de furto e estelionato quando cometidos por meio eletrônico. O furto foi qualificado pelo Art. 155, § 4º-B do Código Penal quando realizado *por meio de fraude eletrônica ou pela utilização de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou uso de programa malicioso*. Além disso, o Art. 171, § 2º-A e § 2º-B instituiu o estelionato eletrônico, prevendo ações realizadas *por meio de redes sociais, contatos telefônicos ou envio de e-mail fraudulento, ou por qualquer outro meio análogo*. Há agravantes se a prática for contra idoso/vulnerável ou se envolver servidor mantido fora do Brasil.

Ademais. entre os pontos fortes identificados, destaca-se que essa lei foi fundamental para modernizar o Código Penal e enfrentar o aumento de golpes virtuais, como *phishing*, *engenharia social* e *fraudes bancárias*. As recentes qualificadoras e causas de aumento de pena, particularmente em relação a idosos, evidenciam uma atenção voltada às vítimas mais vulneráveis e à natureza transnacional do delito. A diferença nítida entre furto, sem envolvimento da vítima na transferência, e estelionato, com indução ao erro da vítima, foi claramente definida para o contexto digital.

Desta feita, dentre as limitações e os desafios, destaca-se apesar de abrangente, a constante evolução das técnicas fraudulentas demanda uma interpretação jurídica que se ajuste de forma ágil. A evidência de *fraude eletrônica* e *uso de dispositivo eletrônico* pode ser complexa, principalmente ao distinguir entre a atuação do malware e a intervenção humana.

Além disso, no comparativo internacional, constatou-se que a maioria das legislações internacionais trata da fraude e do furto eletrônico, ajustando os crimes patrimoniais já existentes. O Art. 8º da Convenção de Budapeste, *Fraude informática*, tipifica como crime a causa de perda de propriedade alheia por meio da alteração de dados ou sistemas. Nações com economias digitais

desenvolvidas, como Reino Unido com o *Fraud Act 2006* e EUA com suas leis de *wire fraud* e *computer fraud*, contam com legislações sólidas que, em termos gerais, englobam essas formas de crime, muitas vezes utilizando definições mais amplas de *fraude* que se ajustam a qualquer meio.

Da mesma forma, a legislação brasileira trouxe a tipificação do Art. 147-A que foi incorporada pela lei n.º 14.132/2021. Como ato de *perseguir alguém*, *reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, perturbando-lhe a liberdade ou privacidade*. Há previsão de aumento de pena se o delito for praticado contra mulher em razão de sua condição de sexo feminino, ou contra crianças, adolescentes, idosos ou indivíduos com deficiência.

Assim como, os aspectos positivos, a tipificação do *stalking* representou um progresso importante, particularmente para combater a violência digital, que frequentemente se manifesta por meio de perseguição online, monitoramento de redes sociais e envio constante de mensagens. A expressão *por qualquer meio* é fundamental para incluir o contexto digital. É fundamental prever agravantes para a violência de gênero e contra pessoas vulneráveis.

Por outro lado, entre as limitações e desafios, destaca-se o fato de que a prova da *reiteração* e da *perturbação da liberdade* ou *privacidade* pode ser subjetiva e demandar um conjunto probatório sólido, como registros de mensagens, perfis falsos, etc. Distinguir uma perseguição criminosa de um comportamento importuno, que não é considerado crime, pode representar um desafio interpretativo.

Somado a isso, no Comparativo Internacional, muitas leis, principalmente na Europa e nos Estados Unidos, definem o *stalking*. A pioneira lei de *stalking* do Reino Unido, de 1997, inspirou muitos estados americanos a adotarem leis *anti-stalking*, que geralmente abrangem o *cyberstalking*. A adequação brasileira está em sintonia com as preocupações internacionais de proteger as vítimas de perseguição obsessiva, independentemente do meio.

Bem como, na legislação brasileira a tipificação do Art. 218-C do Código Penal, introduzido pela lei n.º 13.718/2018 e posteriormente aprimorado pela lei n.º 14.188/2021, que o incluiu na lista de crimes relacionados à violência de gênero, torna ilegal a divulgação não autorizada de *cena de sexo, nudez ou pornografia* quando se refere a conteúdo privado. A lei n.º 14.188/2021 expandiu o alcance para abranger a divulgação de cenas de estupro ou sexo ou pornografia envolvendo crianças e adolescentes.

Mas também, o ponto forte focou na criminalização da *pornografia de vingança*, o que foi um passo essencial para salvaguardar a dignidade e a privacidade das vítimas, que são principalmente mulheres. O tipo penal é explícito ao demandar a falta de consentimento e a natureza privada do conteúdo. A lei n.º 14.550/2023, que agrava as penas e inclui a violência digital na Lei Maria da Penha, fortalece o combate a essa forma de violência de gênero.

Por outro lado, existem limitações e desafios na aplicação. Nesse sentido, a rapidez com que o conteúdo se espalha na internet torna sua remoção

um desafio. Além disso, a demonstração do "consentimento" pode ser complicada, especialmente em situações de relacionamento anterior. Mesmo com ordem judicial, a ausência de mecanismos mais eficientes para a remoção rápida de conteúdo online representa uma limitação prática na proteção da vítima.

Da mesma forma, em mais um comparativo internacional, vários países têm tornado o *revenge porn,* crime. Em 2014, Israel foi o primeiro a fazer isso. A divulgação de imagens íntimas é tratada pela lei de Justiça Criminal e Imigração de 2008 no Reino Unido. A maioria dos estados americanos tem leis específicas contra o *revenge porn*. A tipificação brasileira é sólida e está em sintonia com essa tendência mundial.

De outro modo, referente à tipificação brasileira, nos delitos de calúnia (Art. 138), difamação (Art. 139) e injúria (Art. 140), todos previstos no Código Penal Brasileiro, receberam um agravante específico para o ambiente digital com a lei n.º 13.964/2019, conhecida como *Pacote Anticrime*, que modificou o Art. 141 do Código Penal. O § 2º desse artigo determina que s*e o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, a pena é aumentada de 1/3 (um terço) a 2/3 (dois terços)*.

De igual modo, no que diz respeito aos pontos fortes, observa-se que o legislador reconheceu a capacidade de propagação e o agravamento dos danos que as redes sociais e a internet oferecem aos crimes contra a honra. O aumento da pena é uma resposta proporcional ao maior potencial de dano. A expressão *qualquer modalidade das redes sociais da rede mundial de computadores*" é suficientemente ampla para incluir diversas plataformas.

No entanto, existem algumas limitações e desafios na aplicação, especialmente em relação à obtenção de dados de autoria e identificação do agressor no ambiente digital. O uso de perfis falsos ou anonimato ainda representa um desafio prático, mesmo com a tipificação. Ainda é complicado diferenciar crítica, opinião e crime contra a honra no ambiente digital, onde os limites são tênues.

Para além disso, na pesquisa comparativa internacional, a maioria das jurisdições trata crimes contra a honra no ambiente digital ajustando suas legislações de difamação e calúnia, frequentemente utilizando agravantes semelhantes ou levando em conta a extensão da disseminação. A Convenção de Budapeste não estabelece um tipo penal específico para crimes contra a honra, delegando essa responsabilidade à legislação nacional.

Nesse viés, a legislação brasileira, conforme o Art. 266, § 1º do Código Penal, modificado pela lei n.º 12.737/2012, incorporaram os serviços. O delito é definido como impedir ou perturbar o funcionamento de serviço de comunicação de dados, informação ou de sistemas informatizados. Entre os pontos fortes, destaca-se a inclusão explícita de serviços informáticos e telemáticos, que foi fundamental para lidar com ataques de negação de serviço distribuída (DDoS) e outras formas de indisponibilidade de sistemas. A redação é suficientemente

abrangente para incluir várias técnicas destinadas a interromper ou perturbar o funcionamento de serviços digitais essenciais.

Ainda assim, na lista de limitações e desafios na aplicação, observa-se que a prova da autoria em ataques DDoS, que frequentemente envolvem redes de botnets e computadores zumbis, é extremamente complexa e requer cooperação internacional e rastreamento avançado. Em casos de interrupções momentâneas ou parciais, a definição precisa de *perturbar o funcionamento* pode ser interpretada de diferentes maneiras.

Igualmente, no Comparativo Internacional, é analisado que o Art. 5º *interferência no sistema* da Convenção de Budapeste tipifica como crime a interferência intencional no funcionamento de um sistema de computador, englobando ataques DDoS. Além disso, as leis de cibercrime de outros países geralmente incluem tipos penais específicos para a interrupção de serviços, reconhecendo o prejuízo econômico e social que isso causa.

Principais lacunas da norma brasileira sobre Cibercrimes

Nesse contexto, analisou-se a adequação dos tipos penais existentes, levando em conta a necessidade de ajustar as normas gerais do Código Penal e o perigo de interpretações amplas que comprometem a segurança jurídica. Simultaneamente, foram feitas comparações com legislações de outros países e tratados internacionais, como a Convenção de Budapeste sobre Cibercrime, a fim de identificar onde o Brasil pode melhorar sua abordagem. A análise incluiu várias áreas, como privacidade e crimes relacionados a novas tecnologias.

Contudo, o problema da tipificação na ascensão das criptomoedas, como Bitcoin e Ethereum, e de ativos digitais baseados em blockchain, como NFTs e tokens, trouxe novas formas de criminalidade que desafiam a tipificação convencional. Apesar de fraudes e furtos de criptoativos poderem, em princípio, ser classificados nos artigos 155, § 4º-B, furto mediante fraude eletrônica e 171, § 2º-A, estelionato mediante fraude eletrônica do Código Penal, a falta de um reconhecimento legal explícito de criptoativos como *dinheiro*, *valor mobiliário* ou *ativo financeiro* em todos os contextos gera ambiguidades.

Não obstante, a propriedade de uma criptomoeda é determinada pela detenção da chave privada. O *furto* dessa chave ou do ativo em si geralmente não se enquadra na definição de *coisa alheia móvel* do furto tradicional, a menos que se faça uma interpretação extensiva, a qual pode ser contestada. Ademais, esquemas complexos de manipulação de mercado envolvendo criptoativos e plataformas de investimento fraudulentas, bem como pirâmides financeiras disfarçadas de projetos de cripto, são geralmente abordados por leis mais abrangentes, como a Lei 1.521/51, que trata de crimes contra a economia popular. Isso ocorre em vez de serem considerados por tipificações específicas que reconheçam sua complexidade técnica e o modus operandi digital.

Outrossim, ao fazer uma comparação internacional, observa-se que muitos países e blocos econômicos estão mais avançados na regulamentação de criptoativos e na elaboração de leis penais específicas. Por exemplo, as

criptomoedas foram reconhecidas como forma de pagamento no Japão. A União Europeia está progredindo com a regulamentação MiCA, Markets in Crypto-Assets, que visa estabelecer um quadro jurídico claro para o setor, incluindo possíveis fundamentos para tipificações criminais mais específicas. Nos Estados Unidos, apesar de ser comum a aplicação de leis de fraude e valores mobiliários a criptoativos, existem debates sobre a necessidade de uma legislação mais clara para tratar das particularidades desses ativos.

De fato, a adaptação dos tipos penais de furto e estelionato é um paliativo. A especificidade do ativo digital e a natureza descentralizada exigem maior clareza para evitar arguições de atipicidade e garantir a segurança jurídica na aplicação da lei.

À luz do exposto, o problema da tipificação adequada se refere à proliferação de ferramentas de Inteligência Artificial, particularmente as generativas, que introduziram a habilidade de produzirem conteúdos falsos, porém altamente realistas, denominados *deepfakes*. Esses conteúdos altamente falsos podem ser empregados em fraudes de identidade, como imitação de voz ou imagem para obter acesso a contas bancárias, difamação, extorsão e até mesmo na propagação de desinformação em grande escala, capaz de afetar eleições ou gerar pânico social.

Todavia, apesar de o Código Penal já contemplar delitos como estelionato, difamação, extorsão e o Art. 218-C, a divulgação de cenas de sexo ou nudez sem consentimento, não existe um tipo penal que trate da criação e disseminação intencional e em massa de *deepfakes* com finalidade criminosa, nem que penalize a elaboração e a venda de ferramentas de IA desenvolvidas especificamente para atividades ilícitas. A tipificação vigente demanda um esforço interpretativo significativo para incluir o uso de IA.

Em um estudo comparativo internacional, observa-se um aumento global na regulamentação e criminalização do uso malicioso de *deepfakes*. Nos Estados Unidos, há leis estaduais, como a da Califórnia, que tornam crime a produção de *deepfakes* com o intuito de interferir em eleições ou divulgar conteúdo sexual explícito sem consentimento. Na Europa, debates sobre a Lei de inteligência artificial da União Europeia incluem medidas para lidar com os riscos de *deepfakes*, enquanto a Alemanha considera a modificação de seu Código Penal para tratar da questão.

De igual modo, sobre a adequação ao tipo penal aplicado, observa-se que os tipos existentes são genéricos e podem não abranger completamente o dano ou a modalidade da conduta. A particularidade da inteligência artificial, sua habilidade de escalabilidade e o dano possível justificariam um tipo penal mais direto e amplo, voltado para a falsidade ideológica digital e a manipulação da realidade por meio da inteligência artificial.

No entanto, o problema da tipificação adequada surge na extensa e em expansão rede de dispositivos internet das coisas (IoT), como câmeras de segurança, assistentes virtuais, eletrodomésticos inteligentes e veículos conectados, constituindo uma nova fronteira de vulnerabilidades. A invasão de um dispositivo IoT pode comprometer a privacidade do usuário, permitindo

acesso a câmeras domésticas, sendo usada para criar grandes redes de botnets que realizam ataques DDoS em larga escala, ou até mesmo afetando a segurança física ao controlar sistemas veiculares ou infraestruturas críticas.

Contudo, apesar do Art. 154-A do Código Penal, que trata da invasão de dispositivo informático, pode ser aplicado à Internet das Coisas (IoT), considerando a particularidade de que os dispositivos possuem segurança geralmente frágil e em grande escala, além do uso em ataques distribuídos, o que ainda não está claramente especificado na lei. A criminalização da formação, manutenção ou aluguel de *botnets*, redes de dispositivos zumbis que servem como base para diversos ataques cibernéticos, ainda é incerta e necessita ser ajustada a tipos penais como associação criminosa ou perturbação de serviço.

Além disso, no comparativo internacional à Convenção de Budapeste sobre cibercrime, em seus artigos 2º, acesso ilegal, 4º, interferência de dados e 5º, interferência de sistema, fornece um fundamento para abordar a invasão e o uso indevido de dispositivos. Muitos países com legislações cibernéticas mais avançadas têm disposições mais detalhadas para criminalizar comportamentos associados à criação e utilização de *botnets*.

Outrossim, poderia analisar a adequação do tipo penal, observando-se que a aplicação do artigo 154-A é viável, porém a variedade de riscos e o uso malicioso da rede de dispositivos IoT exigiriam uma tipificação mais sólida, voltada para a infraestrutura do crime cibernético.

Sobre essa ótica, o problema da tipificação adequada aos ataques de ransomware, que consistem na criptografia de dados e sistemas com a demanda de resgate, geralmente em criptomoedas, para sua liberação, representa uma das maiores ameaças cibernéticas no mundo. No Brasil, esses ataques são classificados como extorsão, conforme o Art. 158 do CP. No entanto, a retenção de dados e a ameaça de divulgação pública de informações confidenciais, caracterizando uma *dupla extorsão*, ou a comercialização dessas informações no mercado negro, poderiam justificar uma tipificação própria. Uma lei mais abrangente poderia considerar a complexidade técnica e as diversas etapas do ataque, desde a infecção inicial até a negociação do resgate, além de prever agravantes específicos para ataques a infraestruturas críticas, hospitais ou grandes empresas.

De igual modo, no comparativo internacional, a maioria dos países e a Convenção de Budapeste aplicam seus tipos gerais de extorsão ao ransomware. Entretanto, algumas leis têm abordado ou adotado tipos penais mais diretos para *extorsão de dados* ou *sequestro de dados*, levando em consideração a particularidade do bem jurídico afetado e do modus operandi (Clearsale, 2023).

Para além disso, em relação à adequação do tipo penal, se aplica o Art. 158, porém uma tipificação mais específica para ransomware poderia tornar a persecução mais eficiente, ao prever agravantes específicos para a modalidade digital e ao lidar de forma mais eficaz com as particularidades da negociação e pagamento em criptoativos.

Do mesmo modo, o problema da tipificação adequada de vazamentos massivos de dados pessoais tornou-se comum, colocando milhões de cidadãos em risco de fraude e outros delitos. Frequentemente, esses vazamentos não decorrem de uma *invasão de dispositivo informático*, conforme o Art. 154-A, mas sim de descuido por parte do encarregado do tratamento dos dados, falhas de segurança internas, acesso não autorizado por funcionários com permissão, que não se encaixam perfeitamente nos crimes de administração pública Art. 313-A e B do Código Penal, ou até mesmo de bases de dados que já estavam expostas sem segurança.

Por conseguinte, a Lei Geral de Proteção de Dados (LGPD) estabelece penalidades administrativas e multas. No entanto, *há uma lacuna penal evidente*: não existe um tipo penal geral para acesso não autorizado ou vazamento de dados não públicos em larga escala, nem para a venda de bases de dados roubadas ou vazadas. Isso ocorre quando não é possível caracterizar o acesso como furto ou invasão.

Do mesmo modo, em termos de comparação internacional, o Regulamento Geral de Proteção de Dados (GDPR) europeu, apesar de se concentrar em sanções administrativas, impõe um padrão de proteção de dados bastante rigoroso. Numerosos países europeus têm legislações específicas que tornam crime a violação de segredos comerciais ou o acesso ou a divulgação não autorizada de dados pessoais em grande escala, reforçando assim a regulamentação de proteção de dados. O Art. 32 da Convenção de Budapeste aborda a proteção de dados pessoais, porém não estabelece uma tipificação penal direta.

Deste modo, no âmbito da Adequação do tipo penal, existe uma lacuna na legislação penal para casos de vazamento de dados que não envolvem invasão clássica, assim como para a venda de dados obtidos de forma ilícita. Isso restringe a atuação das autoridades policiais e judiciais, limitando a resposta às penalidades administrativas da LGPD, que, apesar de relevantes, não têm a natureza de repressão criminal.

Desafios Processuais e de Prova

Nesse contexto, na análise crítica da Jurisdição e Cooperação Internacional, a característica transnacional dos delitos cibernéticos gera desafios tanto na definição de jurisdição quanto na obtenção de evidências em servidores situados em outros países. Apesar de o Brasil ter acordos de cooperação jurídica internacional, um ponto crítico é a não ratificação completa da Convenção de Budapeste sobre Cibercrime pelo Brasil. Essa Convenção proporciona uma estrutura sólida para a cooperação internacional, acesso a dados transfronteiriços e assistência mútua, simplificando a troca de informações e a obtenção de provas em tempo real entre os países signatários. A ausência dessa ratificação restringe a rapidez da cooperação brasileira.

Ainda, no que diz respeito à *Cadeia de Custódia* e preservação de provas digitais, observa-se que a volatilidade e a facilidade de manipulação de provas

digitais, como logs, metadados e imagens de sistemas, demandam protocolos estritos de cadeia de custódia e perícia forense digital. Apesar dos esforços da Polícia Federal e das Polícias Civis em capacitação, a uniformização e a propagação desse conhecimento em grande escala ainda representam desafios. A validade jurídica de provas digitais adquiridas por métodos não explicitamente estabelecidos em lei ainda é passível de questionamento, o que pode resultar em fragilidade processual.

Em resumo, apesar da legislação brasileira ter avançado significativamente na tipificação de crimes cibernéticos, ela ainda é reativa e fragmentada diante da evolução tecnológica. A insegurança jurídica e a possibilidade de comprometer a eficácia da persecução penal são consequências da necessidade de ajustar os tipos penais tradicionais ou de usar interpretações extensivas para incluir novas formas de criminalidade.

Proposta de aprimoramento legislativo ao sistema legal

À luz do exposto, embora haja um conjunto de leis que trata dos crimes cibernéticos no Brasil, conforme explicado na seção anterior, é comum que a população e alguns profissionais do direito sintam que o país precisa de uma legislação mais abrangente e eficaz para lidar com esse tipo de crime. Essa visão, apesar de não indicar a inexistência completa de normas, evidencia os grandes desafios enfrentados na implementação e na adaptação do sistema jurídico brasileiro às particularidades do ciberespaço.

Desafios na investigação e aplicação da lei

Portanto, além da fragmentação, a sensação de que a lei brasileira é ineficaz também está relacionada às dificuldades práticas na investigação e implementação das normas vigentes. As autoridades enfrentam desafios consideráveis devido à natureza transnacional dos crimes cibernéticos, à velocidade com que acontecem e à complexidade em rastrear os criminosos no ambiente digital. O Brasil ainda enfrenta deficiências nesse aspecto quando comparado a países que investem significativamente em unidades especializadas e treinamento tecnológico para suas forças policiais e judiciárias.

Sendo que, a baixa taxa de resolução na complexidade técnica e a falta de recursos adequados podem levar a uma baixa taxa de resolução de crimes cibernéticos, o que reforça a sensação de impunidade e a percepção de que a lei não é eficaz.

Somado a isso, a falta de especialização *na* ausência de profissionais do direito e da segurança pública com conhecimento aprofundado em tecnologia e direito digital pode comprometer a qualidade das investigações e dos processos judiciais.

E por fim, a cooperação internacional limitada com o Brasil, embora seja signatário da Convenção de Budapeste, a efetividade da cooperação internacional depende da capacidade interna de cada país em lidar com as

demandas e da agilidade dos trâmites burocráticos, que muitas vezes são lentos.

Considerações finais

De todo modo, a pesquisa buscou analisar a capacidade do sistema jurídico brasileiro de lidar com a complexidade dos crimes virtuais, avaliando a eficácia das normas existentes e identificando lacunas que demandam atualização legislativa urgente para garantir a segurança jurídica e a persecução penal eficaz. Observou-se que o Brasil tem feito progressos significativos na tipificação de diversas modalidades de crimes cibernéticos, como invasão de dispositivo informático, fraudes eletrônicas, stalking, divulgação de conteúdo íntimo sem consentimento e crimes contra a honra no ambiente digital, além de perturbação de serviço informático. Essas leis, embora muitas vezes reativas e com desafios práticos na aplicação devido à complexidade da prova digital e da autoria, demonstram uma base estabelecida para o combate ao cibercrime, alinhando-se em vários aspectos com padrões internacionais, como a Convenção de Budapeste.

Contudo, o estudo revelou lacunas críticas na legislação brasileira que comprometem sua efetividade. Áreas como crimes envolvendo criptoativos e tecnologia blockchain, abuso de ferramentas de Inteligência Artificial e deepfakes maliciosos, crimes relacionados à Internet das Coisas (IoT) e dispositivos conectados, ciberextorsão e ransomware, e vazamentos em massa de dados carecem de tipificações penais específicas, forçando interpretações extensivas de leis existentes que geram insegurança jurídica. Além disso, desafios processuais e de prova, como a volatilidade da prova digital, a complexidade da jurisdição transnacional e a lentidão da cooperação internacional, apesar da promulgação da Convenção de Budapeste, persistem como entraves significativos à efetividade da lei. A fragmentação legal, sem um código cibernético unificado, contribui para a dificuldade de compreensão e a sensação de impunidade, reforçando a urgência de uma abordagem mais estratégica e menos reativa a casos específicos.

De forma objetiva, as limitações da pesquisa incluem sua natureza qualitativa e exploratória, que não se aprofundou em dados empíricos de efetividade de condenações, e o dinamismo inerente à área, que faz da *adequação* legislativa um alvo em constante movimento. Apesar disso, os achados são de suma importância, pois fornecem um diagnóstico preciso para aprimorar a atuação policial e judicial, subsidiar futuras reformas legislativas e fortalecer a cooperação internacional. Este conhecimento é vital para direcionar esforços na segurança pública e no direito penal, combatendo a impunidade e protegendo a sociedade no ambiente digital.

Nesse contexto, sugere-se para futuras pesquisas, a realização de estudos empíricos sobre a taxa de resolução de crimes cibernéticos, análises comparativas aprofundadas de modelos legislativos internacionais, especialmente em áreas como IA, criptoativos e IoT, investigações sobre os

desafios forenses e a cadeia de custódia digital, bem como propostas de regulamentação específica para novas tecnologias. Fomentar a pesquisa sobre educação digital e o papel das plataformas online na prevenção e combate a esses crimes também é crucial para construir um arcabouço jurídico e social mais resiliente e proativo.

Referências

BRASIL. **Lei Caroline Dieckmann. nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 9 jun. 2025.

BRASIL. **Lei do Marco Civil da Internet. nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 14.550, de 19 de abril de 2023**. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha) [...]. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil03/ato2023-2026-2026/2023/lei/l14550.htm. Acesso em: 15 out. 2025.

CLEARSALE. **Panorama do Ransomware no Brasil**: Tendências e Impactos. Relatório de Segurança Cibernética, 2023. Disponível em: https://www.clearsale.com.br/blog/panorama-do-ransomware-no-brasil/. Acesso em: 8 jun. 2025.

COUNCIL OF EUROPE. **Convenção sobre o Cibercrime (Convenção de Budapeste)**. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 20 jun. 2025.

ESTADOS UNIDOS DA AMÉRICA. **United States Code**. Title 18: Crimes and Criminal Procedure, Part I, Chapter 47, § 1030 - Fraud and related activity in connection with computers (Computer Fraud and Abuse Act). [Washington, D.C.]: U.S. Government Publishing Office, [s.d.]. Disponível em: https://www.govinfo.gov/app/details/USCODE-2021-title18/USCODE-2021-title18-partI-chap47-sec1030. Acesso em: 27 out. 2025.

ESTADOS UNIDOS. **Wire Fraud Statute, 18 USC § 1343**. Lei que criminaliza o uso do sistema de comunicações para fraudes. [Sl], 1948 (atualizado). Disponível em: https://www.law.cornell.edu/uscode/text/18/1343 . Acesso em: 27 out. 2025.

ESTADOS UNIDOS**. Lei de Fraude e Abuso de Computadores, 18 USC § 1030**. Lei que trata de fraudes e abusos relacionados a computadores. [Sl], 1986 (atualizado).

Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 27 out. 2025.

FRANÇA, Beatricia dos S. C. P. **Crimes Cibernéticos e a Legislação Brasileira**. **Revista FT**, 2024. Disponível em: https://revistaft.com.br/?s=Crimes+Cibern%C3%A9ticos+e+a+Legisla%C3%A7%C3%A3o+Brasileira. Acesso em: 20 jun. 2025.

GERHARDT, Tatiana E.; SILVEIRA, Denise T. (Org.). **Métodos de Pesquisa**. Porto Alegre: Editora da UFRGS, 2009.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 1987.

MACBARBOSA. **Invasão de Dispositivo Informático**: Análise do Art. 154-A do Código Penal. 2020. Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020.

MENDES, F. A. A Lei nº 14.155/2021 e o Combate aos Crimes Cibernéticos no Brasil. **Revista de Direito Penal e Criminologia**, v. 15, n. 1, p. 33-48, 2021.

MINISTÉRIO PÚBLICO FEDERAL (MPF). **Crimes cibernéticos**. Coletânea de artigos sobre criminalidade cibernética. Brasília, 2018. Disponível em: http://hdl.handle.net/11549/185404 . Acesso em: 27 out. 2025.

REINO UNIDO. **Lei de Fraude de 2006, c. 35**. Lei que prevê, e em conexão com, responsabilidade criminal por fraude e obtenção de serviços desonesta. [Sl], 8 nov. 2006. Disponível em: https://www.legislation.gov.uk/ukpga/2006/35/contents . Acesso em: 27 out. 2025.

SOUSA, Carlos Muryllo Rodrigues de; SANTOS, Guilherme Augusto Martins. Crimes cibernéticos e os desafios jurídicos na era digital: análise legislativa, doutrinária e jurisprudencial. **Revista JRG de Estudos Acadêmicos**, [S. l.], 30 nov. 2024. Disponível em: https://www.revistajrg.com/index.php/jrg. Acesso em: 27 out. 2025.

UCHÔA, Roberto. A metamorfose digital: como as facções brasileiras estão trocando o fuzil pelo phishing. **FONTESEGURA**, 2025. Disponível em: https://fontesegura.forumseguranca.org.br/a-metamorfose-digital-como-as-faccoes-brasileiras-estao-trocando-o-fuzil-pelo-phishing/. Acesso em: 20 jun. 2025.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. **Diretiva 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de agosto de 2013**, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. *Jornal Oficial da União Europeia*, Luxemburgo, L 218, p. 8-14, 14 ago. 2013. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32013L0040. Acesso em: 27 out. 2025.

Recebido em: 11/10/2025
Aprovado em: 27/10/2025
Publicado em: 31/10/2025