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

OPEN ACCESS

doi.org/10.51891/rease.v12i6.27553

PHISHING E ESTELIONATO ELETRÔNICO: DESAFIOS DA INVESTIGAÇÃO E DA RESPONSABILIDADE PENAL APÓS A LEI 14.155/2021

Rafaele Louise de Souza silva oliveira[1]
Rosana Reis de Melo Silva[2]

RESUMO: O presente artigo examina o fenômeno do phishing e do estelionato eletrônico à luz do ordenamento jurídico brasileiro, com ênfase nas inovações introduzidas pela Lei nº 14.155/2021. Por meio de pesquisa bibliográfica e documental de natureza qualitativa, analisam-se as características e a evolução dessas condutas criminosas, os instrumentos normativos disponíveis para sua repressão e os principais desafios enfrentados pelas autoridades na investigação e na responsabilização penal dos agentes. Os resultados demonstram que, apesar dos avanços legislativos representados pela qualificadora da fraude eletrônica e pela nova regra de competência jurisdicional, persistem lacunas normativas e deficiências estruturais que comprometem a efetividade da tutela penal. Conclui-se que o enfrentamento eficaz ao phishing exige uma abordagem sistêmica, que articule aprimoramento legislativo, modernização investigativa, cooperação internacional e educação digital da população.

Palavras-chave: Phishing. Estelionato Eletrônico. Lei 14.155/2021. Crimes Cibernéticos. Investigação Criminal.

ABSTRACT: This article examines the phenomenon of phishing and electronic fraud in light of the Brazilian legal system, with emphasis on the innovations introduced by Law No. 14.155/2021. Through qualitative bibliographic and documentary research, it analyzes the characteristics and evolution of these criminal conducts, the normative instruments available for their repression, and the main challenges faced by authorities in the investigation and criminal accountability of perpetrators. The results demonstrate that, despite the legislative advances represented by the electronic fraud qualifying circumstance and the new jurisdictional competence rule, normative gaps and structural deficiencies persist that undermine the effectiveness of criminal protection. It is concluded that the effective confrontation of phishing requires a systemic approach, articulating legislative improvement, investigative modernization, international cooperation and digital education of the population.

Keywords: Phishing. Electronic fraud. Law 14.155/2021. Cybercrime. Criminal investigation.

[1]Graduanda do curso de Bacharelado em Direito, no Centro Universitário Fametro. Manaus, Amazonas, Brasil.
[2]Prof.ª Orientadora e Coordenadora do TCC II, no Centro Universitário FAMETRO: Prof.ª Esp. Rosana Reis de Melo Silva. Manaus, Amazonas, Brasil.

1 INTRODUÇÃO

A expansão acelerada das tecnologias digitais nas últimas décadas transformou profundamente as relações sociais, econômicas e jurídicas no Brasil e no mundo. O acesso massivo à internet, a popularização dos dispositivos móveis e a intensificação das transações financeiras realizadas em ambiente virtual criaram um campo fértil para o surgimento e a proliferação de novas modalidades criminosas, entre as quais o phishing e o estelionato eletrônico ocupam posição de destaque pela sofisticação dos métodos empregados e pela extensão dos danos causados às vítimas. Nesse cenário, o ordenamento jurídico brasileiro foi instado a responder com instrumentos normativos mais eficazes, culminando na promulgação da Lei nº 14.155, de 27 de maio de 2021, que representou um marco legislativo relevante ao agravar as penas dos crimes praticados por meios eletrônicos e fixar novas regras de competência processual (Brasil, 2021).

Apesar dos avanços introduzidos pela legislação, a realidade prática demonstra que a simples majoração das sanções penais não é suficiente para conter o crescimento exponencial das fraudes eletrônicas. Segundo dados do Anuário Brasileiro de Segurança Pública de 2025, somente no ano de 2024 foram registrados 281 mil casos de estelionato eletrônico no país, o que representa um aumento de 17% em relação ao ano anterior, evidenciando que os desafios impostos pela criminalidade digital transcendem o campo legislativo e alcançam as esferas da investigação criminal, da produção de provas digitais e da cooperação internacional (Souza; Rodrigues, 2025). Diante desse quadro, a problemática central deste artigo reside em compreender em que medida a Lei nº 14.155/2021 contribuiu para o aprimoramento da responsabilização penal dos autores de phishing e estelionato eletrônico, e quais são os principais obstáculos enfrentados pelas autoridades na investigação e na persecução penal dessas condutas.

A justificativa para a realização desta pesquisa repousa na urgência social e acadêmica de se debater o fenômeno da criminalidade cibernética de forma sistemática, considerando que os operadores do direito, delegados, promotores, juízes e advogados, deparam-se cotidianamente com demandas para as quais o arcabouço normativo ainda não oferece respostas plenamente satisfatórias. A dificuldade de rastreamento dos agentes delitivos, o anonimato proporcionado pelo ambiente virtual, a transnacionalidade dos crimes e as limitações técnicas dos órgãos de persecução penal constituem entraves concretos à efetividade da tutela penal, uma vez que, soma-se a isso a necessidade de interpretar a nova legislação à luz dos princípios constitucionais

e processuais penais, especialmente no que tange à competência jurisdicional e à produção de provas digitais (Wendt; Jorge, 2021).

O presente artigo está estruturado da seguinte forma: inicialmente, procede-se à caracterização do phishing e do estelionato eletrônico enquanto fenômenos criminais, abordando suas definições, ferramentas, técnicas de engenharia social e impactos econômicos e sociais. Em seguida, analisa-se o tratamento jurídico conferido a essas condutas pelo ordenamento brasileiro, com ênfase nas inovações trazidas pela Lei nº 14.155/2021. Por fim, examinam-se os principais desafios da investigação criminal e os problemas relacionados à responsabilização penal dos autores, à luz da doutrina e da jurisprudência mais recentes. A metodologia adotada é qualitativa e bibliográfica, com análise de dispositivos legais, doutrina especializada, artigos científicos e jurisprudência dos tribunais superiores.

2 PHISHING E ESTELIONATO ELETRÔNICO: CARACTERÍSTICAS E EVOLUÇÃO

2.1 Definição e evolução do phishing no contexto digital

O phishing constitui uma das modalidades mais antigas e persistentes de fraude eletrônica, cuja denominação deriva do inglês *fishing* (pescar), fazendo alusão à técnica de lançar iscas digitais para capturar dados e informações sigilosas das vítimas. Trata-se de uma conduta que se utiliza de mensagens fraudulentas, páginas falsas, correios eletrônicos enganosos e outros recursos do ambiente virtual para induzir o usuário ao erro, levando-o a fornecer voluntariamente seus dados bancários, senhas, números de documentos ou outros elementos que permitam ao agente obter vantagem ilícita em detrimento alheio. No ordenamento jurídico brasileiro, tal conduta encontra tipificação primordialmente no artigo 171, § 2º-A, do Código Penal, inserido pela Lei nº 14.155/2021, que qualificou o estelionato praticado mediante fraude eletrônica (Gomes; Medrado, 2023).

A evolução do phishing acompanhou o desenvolvimento das próprias tecnologias de comunicação digital. Em seus primórdios, os ataques se concentravam no envio massivo de e-mails simulando comunicações de instituições bancárias ou empresas idôneas, com o objetivo de redirecionar as vítimas a páginas falsas onde seus dados eram coletados. Com o tempo, os criminosos aprimoraram substancialmente suas técnicas, passando a personalizar os ataques a partir de informações prévias sobre os alvos, modalidade conhecida como *spear phishing*, além de diversificarem os canais de abordagem com o surgimento do *vishing*, realizado por ligações telefônicas, e do *smishing*, operacionalizado por meio de mensagens de texto, onde essa

progressiva sofisticação das práticas criminosas evidenciou a insuficiência das tipificações genéricas existentes no Código Penal e impulsionou as reformas legislativas que culminaram na Lei nº 14.155/2021 (Wendt; Jorge, 2021; Brasil, 2021).

No contexto brasileiro, o phishing ganhou contornos ainda mais preocupantes com a massificação do uso das redes sociais, aplicativos de mensagens instantâneas e plataformas de comércio eletrônico. Os criminosos passaram a explorar o ambiente digital para criar perfis falsos de pessoas e empresas, simular situações de urgência financeira e se apropriar de contas de comunicadores para fraudar contatos das vítimas, conduta que ficou popularmente conhecida como clonagem de WhatsApp. A Lei nº 14.155/2021 buscou alcançar exatamente essas hipóteses ao estabelecer, em seu artigo 2º, a seguinte previsão inserida no Código Penal:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se 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 (Brasil, 2021, art. 171).

A amplitude da expressão "qualquer outro meio fraudulento análogo" revela a opção do legislador por uma fórmula aberta que permite a interpretação progressiva do tipo penal, de modo a alcançar as inovações tecnológicas que inevitavelmente surgirão no cenário da criminalidade digital (Pereira, 2021). Esse mecanismo interpretativo é essencial em um campo normativo em que a velocidade das transformações tecnológicas supera, em muito, a capacidade de resposta do processo legislativo (Marra, 2019).

2.2 Ferramentas e métodos utilizados pelos criminosos: como operam os ataques de phishing

A compreensão dos mecanismos técnicos empregados pelos criminosos é condição indispensável para a efetividade tanto da investigação criminal quanto da construção de uma resposta jurídica adequada. Os ataques de phishing valem-se de um conjunto diversificado de ferramentas e estratégias que vão desde a criação de páginas web falsas (tecnicamente denominadas *sites* de *spoofing*) até o emprego de programas maliciosos capazes de interceptar dados inseridos pelos usuários em seus dispositivos. Nesse sentido, o desvio de endereços eletrônicos, conhecido como *typosquatting*, constitui técnica frequentemente utilizada para confundir a vítima ao apresentar domínios quase idênticos aos legítimos, diferindo apenas em um caractere ou na extensão (Lai, 2021).

Outra ferramenta amplamente utilizada é o *malware*, categoria que abrange os chamados *keyloggers*, programas capazes de registrar todas as teclas digitadas pelo usuário, e os *trojans*, aplicações maliciosas que se disfarçam de softwares legítimos para capturar dados

sigilosos ou permitir o acesso remoto não autorizado ao dispositivo da vítima. A utilização dessas ferramentas pode implicar a incidência de mais de um tipo penal, gerando concurso entre o crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal, e o estelionato eletrônico, o que representa um dos desafios hermenêuticos mais relevantes trazidos pela reforma legislativa de 2021 (Wendt; Jorge, 2021).

A Lei nº 12.737/2012, ao tipificar a invasão de dispositivo informático, já havia antecipado a necessidade de proteção penal em face dessas condutas, prescrevendo em seu artigo 154-A:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa (Brasil, 2012, art. 154-A).

A intersecção entre o crime de invasão de dispositivo informático e o estelionato eletrônico gera, na prática, situações de difícil enquadramento típico, sobretudo quando o criminoso emprega recursos tecnológicos para capturar dados da vítima sem que esta perceba qualquer interação direta com o agente. A distinção doutrinária e jurisprudencial entre furto mediante fraude eletrônica e estelionato eletrônico torna-se, nesses casos, determinante para a correta imputação e para a fixação da competência jurisdicional (Lopes; Lopes, 2023).

Além disso, o emprego de servidores localizados fora do território nacional, prática rotineira entre os grupos criminosos mais sofisticados, dificulta sobremaneira a obtenção de registros digitais e dados de conexão necessários à identificação dos autores, impondo às autoridades brasileiras a necessidade de recorrer aos instrumentos de cooperação jurídica internacional (Dobler, 2023).

2.3 A engenharia social como base para o phishing: manipulação psicológica e técnicas de engano

A engenharia social constitui o substrato sobre o qual se assenta a maior parte das práticas de phishing, sendo definida como o conjunto de técnicas psicológicas destinadas a manipular o comportamento humano para que a vítima, de forma voluntária, mas enganada, realize ações que favorecem os interesses ilícitos do agente. Diferentemente dos crimes informáticos que dependem exclusivamente de vulnerabilidades técnicas dos sistemas, o phishing baseia-se primordialmente na exploração de fatores humanos, como a confiança, o medo, a urgência e a autoridade percebida. É justamente esse elemento de participação ativa e consentida da vítima, ainda que obtida por meio de engano, que distingue o estelionato eletrônico do furto mediante fraude eletrônica no plano jurídico-penal (Gomes; Medrado, 2023).

Entre as técnicas de engano mais frequentemente utilizadas, destacam-se a simulação de comunicações oficiais de bancos, órgãos públicos e operadoras de telefonia, a criação de situações de falsa urgência, como supostos bloqueios de contas ou pendências tributárias, a personificação de funcionários de suporte técnico e a promessa de prêmios, benefícios ou investimentos com rentabilidade anormalmente elevada. Tais estratégias visam a contornar a racionalidade crítica do usuário, levando-o a agir impulsivamente e a fornecer dados sensíveis antes que possa avaliar a legitimidade da comunicação recebida (Wendt; Jorge, 2021).

A Lei nº 14.155/2021, ao qualificar o estelionato praticado por meio de redes sociais, contatos telefônicos e correio eletrônico fraudulento, reconheceu expressamente a relevância penal dessas técnicas de manipulação psicológica, inserindo no Código Penal, por meio de seu artigo 2º, o seguinte dispositivo: "§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional" (Brasil, 2021, art. 171).

A previsão da causa de aumento para crimes praticados com uso de servidores estrangeiros reflete a preocupação do legislador com os obstáculos que essa circunstância impõe à investigação criminal, pois a obtenção de dados junto a provedores localizados em outros países exige a utilização dos mecanismos de cooperação jurídica internacional, processo que tende a ser moroso e que frequentemente inviabiliza a identificação tempestiva dos agentes delitivos (Gomes; Medrado; Gama, 2024).

No mais, averigua-se que a Convenção sobre o Crime Cibernético, promulgada no Brasil pelo Decreto nº 11.491/2023, conhecida como Convenção de Budapeste, representa um avanço significativo nesse sentido, ao estabelecer mecanismos padronizados de cooperação entre os países signatários para a preservação e o compartilhamento de dados digitais em investigações criminais (Brasil, 2023).

A engenharia social atinge com maior eficácia as parcelas mais vulneráveis da população, como idosos, pessoas com menor familiaridade com o ambiente digital e usuários que utilizam dispositivos sem as devidas proteções de segurança. A Lei nº 14.155/2021, atenta a essa realidade, estabeleceu causa especial de aumento de pena quando os crimes de furto e estelionato eletrônico são praticados contra idosos ou vulneráveis, reforçando a tutela penal em favor dos grupos historicamente mais expostos à vitimização digital (Santos, 2024).

2.4 O impacto econômico e social do phishing: consequências para as vítimas e para a confiança digital

Os efeitos do phishing e do estelionato eletrônico não se restringem ao plano individual das vítimas diretamente lesadas, mas se irradiam para dimensões coletivas que afetam a estabilidade das relações econômicas, a confiança nas instituições financeiras e a própria percepção de segurança no ambiente digital. Do ponto de vista econômico, as estimativas globais apontam para prejuízos bilionários anuais decorrentes de fraudes cibernéticas, com especial destaque para as perdas relacionadas a golpes bancários, clonagem de cartões, invasão de contas digitais e transferências fraudulentas realizadas por meio de plataformas de pagamento instantâneo (Marra, 2019). No Brasil, os dados do Anuário Brasileiro de Segurança Pública de 2025 revelam que somente o estelionato eletrônico respondeu por 281 mil registros em 2024, aumento expressivo que demonstra a incapacidade das medidas repressivas vigentes de reverter a tendência de crescimento dessas infrações (Souza; Rodrigues, 2025).

No âmbito das consequências individuais, as vítimas de phishing e estelionato eletrônico sofrem não apenas prejuízos patrimoniais diretos, mas também danos de natureza moral e psicológica. A sensação de violação da privacidade, a vergonha decorrente do engano sofrido e a dificuldade de recuperação dos valores indevidamente transferidos compõem um quadro de vitimização que frequentemente se prolonga muito além do evento criminoso em si. A esse cenário soma-se a constatação de que a maioria das vítimas desconhece os mecanismos legais disponíveis para a busca de reparação ou para a denúncia das condutas às autoridades competentes, o que contribui para a subnotificação dos crimes e para a sensação de impunidade que cerca o ambiente digital (Lima, 2024).

Do ponto de vista social, o phishing contribui para a erosão da confiança digital, fenômeno com implicações profundas para o desenvolvimento da economia digital e para a inclusão financeira de amplos segmentos da população. A desconfiança em relação aos canais digitais de comunicação e de realização de transações financeiras gera barreiras ao uso de serviços essenciais oferecidos em formato eletrônico, afetando especialmente as camadas menos favorecidas economicamente que mais dependem das plataformas digitais de acesso a serviços bancários e governamentais (Ribeiro; Lima, 2024). Nesse contexto, as políticas públicas de educação digital e de conscientização dos usuários sobre os riscos e as formas de identificação dos ataques de phishing assumem papel complementar e indispensável ao esforço repressivo do

Estado, pois a prevenção revela-se mais eficaz do que a punição posterior quando se trata de crimes que dependem fundamentalmente da indução ao erro da vítima (Araújo et al., 2025).

A resposta do Estado brasileiro a esse cenário tem sido progressiva, ainda que ainda insuficiente. A edição da Lei nº 12.737/2012, do Marco Civil da Internet - Lei nº 12.965/2014, da Lei Geral de Proteção de Dados; Lei nº 13.709/2018 e, mais recentemente, da Lei nº 14.155/2021 demonstram uma trajetória de amadurecimento legislativo orientada pelo reconhecimento da gravidade dos crimes cibernéticos e pela necessidade de adequação do sistema penal às demandas da sociedade digital (Belinotte et al., 2024). Contudo, como apontam os pesquisadores da área, a efetividade dessa trajetória legislativa depende não apenas da qualidade das normas editadas, mas também do investimento em estrutura investigativa especializada, em formação técnica dos profissionais da persecução penal e no aprofundamento dos mecanismos de cooperação jurídica internacional (Calixto; Facuri; Teles, 2023).

3 O DIREITO PENAL E A LEI 14.155/2021: UM NOVO ENFOQUE PARA O ESTELIONATO ELETRÔNICO

3.1 A adaptação do Código Penal ao estelionato eletrônico: a Lei 14.155/2021 e suas implicações

A promulgação da Lei nº 14.155, de 27 de maio de 2021, representou uma inflexão significativa na trajetória do direito penal brasileiro diante da criminalidade cibernética. Até então, os crimes patrimoniais praticados por meios eletrônicos eram enquadrados nas tipificações genéricas do Código Penal de 1940, instrumento normativo concebido em um contexto histórico radicalmente distinto do ambiente digital contemporâneo. A inadequação dessas tipificações ao fenômeno da fraude eletrônica gerava insegurança jurídica, divergências interpretativas na jurisprudência e dificuldades práticas na fixação das penas e da competência jurisdicional, criando um cenário de relativa impunidade que favorecia a proliferação dos golpes digitais (Gomes; Medrado, 2023).

A reforma introduzida pela Lei nº 14.155/2021 operou em três eixos principais. No primeiro, agravou as penas do crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal, ampliando a abrangência da conduta típica e aumentando os patamares mínimo e máximo das sanções cominadas. No segundo eixo, criou a figura qualificada do furto mediante fraude eletrônica, inserindo o § 4º-B no artigo 155 do Código Penal, com pena de reclusão de quatro a oito anos. No terceiro e mais relevante para os fins deste estudo, instituiu a qualificadora da fraude eletrônica no crime de estelionato, adicionando o § 2º-A ao artigo 171

do Código Penal (Brasil, 2021). Ao lado dessas alterações de direito material, a lei promoveu ainda importante modificação processual, inserindo o § 4º no artigo 70 do Código de Processo Penal, que assim passou a dispor:

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (Brasil, 2021, art. 70, § 4º).

A fixação da competência no domicílio da vítima representou uma mudança sensível em termos de política criminal, pois facilitou o acesso das pessoas lesadas ao sistema de justiça, evitando que precisassem se deslocar para o local de consumação do delito ,frequentemente desconhecido em razão do anonimato digital do agente. Contudo, essa inovação também gerou controvérsias jurisprudenciais, particularmente em razão da tensão entre a nova regra de competência e o entendimento tradicional sobre o momento consumativo do estelionato, questão que o Superior Tribunal de Justiça tem enfrentado em sucessivos conflitos de competência (Souza; Rodrigues, 2025). No plano doutrinário, critica-se ainda o viés excessivamente punitivista da reforma, que priorizou o agravamento das penas sem o correspondente investimento em capacidade investigativa e em mecanismos processuais eficazes para a produção de provas digitais (Lai, 2021).

3.2 O phishing no contexto do crime de estelionato (Art. 171, CP)

O crime de estelionato, tipificado no artigo 171 do Código Penal, é estruturado sobre quatro elementos essenciais: a fraude como meio executivo, o erro da vítima como resultado da fraude, a vantagem ilícita auferida pelo agente e o prejuízo alheio como consequência. A participação ativa da vítima , ainda que obtida mediante engano, é o traço que historicamente distingue o estelionato do furto, e é exatamente esse elemento que posiciona o phishing como modalidade prototípica do estelionato eletrônico, dado que nessa conduta o criminoso obtém os dados e os recursos financeiros da vítima com a colaboração involuntária desta, induzida ao erro pelos artifícios fraudulentos empregados (Pereira, 2021).

A qualificadora inserida pelo § 2º-A ao artigo 171 do Código Penal alcança especificamente as hipóteses em que a fraude é perpetrada por meio de redes sociais, contatos telefônicos ou correio eletrônico fraudulento, meios que coincidem com os principais vetores de disseminação dos ataques de phishing. Essa correspondência entre a técnica criminosa e a moldura típica é, ao mesmo tempo, um avanço e um desafio interpretativo, pois a lei exige que

a fraude seja cometida com a utilização de informações fornecidas pela própria vítima ou por terceiro induzido ao erro, o que pode excluir da qualificadora aquelas hipóteses em que o agente obtém os dados por outros meios, como a invasão direta de sistemas sem qualquer interação com a vítima (Lopes; Lopes, 2023). Para essas situações, o enquadramento adequado tende a ser o do furto mediante fraude eletrônica, previsto no § 4º-B do artigo 155, ou o concurso entre a invasão de dispositivo informático e o estelionato na forma simples. O artigo 171, caput, do Código Penal estabelece: "Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis" (Brasil, 1940, art. 171).

A amplitude da expressão "qualquer outro meio fraudulento" presente no caput do artigo 171, somada à fórmula genérica adotada pelo § 2º-A ,"qualquer outro meio fraudulento análogo" —, confere ao tipo penal a flexibilidade interpretativa necessária para alcançar as múltiplas e mutáveis formas pelas quais o phishing se manifesta no ambiente digital. Essa abertura normativa, entretanto, deve ser manejada com cautela pelos operadores do direito, em respeito ao princípio da legalidade e à vedação da analogia in malam partem no direito penal (Gomes; Medrado, 2023).

A jurisprudência dos tribunais superiores tem sido instada a delimitar com precisão as fronteiras entre as diversas figuras típicas envolvidas, produzindo precedentes que orientam a aplicação da lei nos casos concretos, ainda que as controvérsias interpretativas estejam longe de uma resolução definitiva (Santos, 2024).

3.3 A relação entre phishing e falsa identidade (Art. 307, CP): a adequação do tipo penal

O crime de falsa identidade, previsto no artigo 307 do Código Penal, consiste na atribuição a si mesmo ou a terceiro de falsa identidade com o objetivo de obter vantagem ou causar dano a outrem. Sua interface com o phishing é frequente e relevante, pois grande parte dos ataques dessa natureza envolve a personificação de pessoas físicas ou jurídicas ,bancos, órgãos governamentais, empresas de telecomunicação ,como artifício central para criar o ambiente de confiança necessário ao engano das vítimas. A questão que se coloca no plano jurídico-penal é a de saber se a conduta de se apresentar falsamente como representante de uma instituição legítima, para obter dados ou valores da vítima, configura autonomamente o crime

do artigo 307, em concurso com o estelionato eletrônico, ou se é absorvida por este na qualidade de meio de execução (Wendt; Jorge, 2021).

A doutrina majoritária inclina-se pela aplicação do princípio da consunção, segundo o qual o crime-meio é absorvido pelo crime-fim quando aquele constitui fase normal de execução deste. Nessa perspectiva, a falsa identidade utilizada como instrumento para a prática do estelionato eletrônico seria absorvida por este, respondendo o agente apenas pelo crime mais grave. Contudo, a hipótese de concurso formal ou material não pode ser descartada de plano quando a falsa identidade gera consequências autônomas que vão além da mera facilitação do estelionato, como ocorre nos casos em que o criminoso utiliza a identidade falsa para realizar múltiplas operações criminosas independentes (Lopes; Lopes, 2023). O artigo 307 do Código Penal dispõe: "Art. 307. Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena – detenção, de três meses a um ano, ou multa, se o fato não é elemento constitutivo de crime mais grave" (Brasil, 1940, art. 307).

A cláusula de subsidiariedade expressa contida na parte final do artigo 307 ,"se o fato não é elemento constitutivo de crime mais grave" ,resolve em grande medida a questão do concurso aparente de normas, confirmando que, nos casos em que a falsa identidade integra a execução do estelionato eletrônico qualificado, a tipificação que prevalece é a do artigo 171, § 2º-A, do Código Penal, com suas penas mais graves. Essa solução, embora tecnicamente satisfatória, não esgota as dificuldades práticas de enquadramento, especialmente nas situações em que o agente age de forma organizada, assume múltiplas identidades falsas e atinge inúmeras vítimas em diferentes locais e momentos (Ribeiro; Lima, 2024). A complexidade dessas hipóteses reforça a necessidade de investigação especializada e de normas processuais adequadas à realidade dos crimes cibernéticos de grande escala.

3.4 Lacunas normativas e a necessidade de regulamentação mais específica para fraudes digitais

Apesar dos avanços proporcionados pela Lei nº 14.155/2021, persistem no ordenamento jurídico brasileiro lacunas normativas que fragilizam a resposta estatal ao fenômeno do phishing e das fraudes digitais em geral. A crítica mais recorrente na doutrina diz respeito ao fato de a reforma ter se concentrado no agravamento das penas sem criar mecanismos processuais e investigativos específicos para a apuração dos crimes cibernéticos, perpetuando a dependência de institutos processuais concebidos para a criminalidade tradicional e frequentemente

inadequados às especificidades do ambiente digital (Marra, 2019). Essa inadequação se manifesta de forma particularmente aguda nos procedimentos de obtenção de provas digitais, nos prazos de preservação de dados pelos provedores e nos critérios de admissibilidade das evidências colhidas em ambiente virtual.

Outra lacuna relevante reside na ausência de uma tipificação específica para o phishing enquanto conduta autônoma. O ordenamento brasileiro trata o fenômeno de forma indireta, por meio da qualificadora do estelionato eletrônico e do crime de invasão de dispositivo informático, sem prever expressamente as múltiplas modalidades de phishing ,spear phishing, vishing, smishing. e sem estabelecer parâmetros claros para a distinção entre elas no plano jurídico-penal (Lai, 2021). Essa lacuna gera insegurança jurídica e dificulta a uniformização da jurisprudência, favorecendo interpretações díspares que comprometem a isonomia no tratamento dos casos concretos. No plano comparado, países como Espanha e Portugal adotam tipificações mais detalhadas para as fraudes informáticas, o que sugere a conveniência de um aprimoramento legislativo que confira maior precisão ao tratamento penal dessas condutas no Brasil (Pereira, 2021).

A Lei Geral de Proteção de Dados ,Lei nº 13.709/2018 ,avançou na disciplina do tratamento de dados pessoais e na responsabilização administrativa das organizações que os manuseiam inadequadamente, mas não supre as lacunas do direito penal, operando em esfera normativa distinta (Brasil, 2018). A superação dessas deficiências requer, portanto, uma abordagem legislativa integrada que una o aperfeiçoamento das tipificações penais, a modernização dos instrumentos processuais de investigação digital e o fortalecimento dos mecanismos de cooperação jurídica internacional (Calixto; Facuri; Teles, 2023).

4 DESAFIOS NA INVESTIGAÇÃO DO PHISHING E DA RESPONSABILIZAÇÃO PENAL

4.1 Dificuldades na atribuição de autoria em crimes de phishing: o anonimato digital e as barreiras investigativas

A atribuição de autoria constitui um dos obstáculos mais significativos na investigação dos crimes de phishing, em razão das inúmeras técnicas disponíveis para a ocultação da identidade dos agentes no ambiente digital. O anonimato proporcionado pela arquitetura da internet ,que permite a criação de contas falsas, o uso de redes privadas virtuais, a utilização de servidores localizados em países com regulação débil e o emprego de criptomoedas para a

movimentação dos valores obtidos ilicitamente ,cria barreiras investigativas que os instrumentos tradicionais da persecução penal têm grande dificuldade de transpor (Lima, 2024). Nesses contextos, a identificação do responsável pela prática delitiva frequentemente depende de uma cadeia de pedidos de informação junto a diferentes provedores e operadoras, processo que consome tempo considerável e que pode resultar na prescrição do crime antes de sua elucidação.

O rastreamento do endereço IP ,identificador numérico que permite localizar a origem de uma conexão à internet ,é o ponto de partida habitual das investigações de crimes cibernéticos, mas apresenta limitações práticas significativas. O uso de redes de anonimização como o Tor, a utilização de servidores intermediários, os chamados *proxies*, e a contratação de serviços de VPN impedem ou dificultam a identificação do endereço IP real do agente, rompendo a cadeia investigativa no ponto em que ela mais importa (Wendt; Jorge, 2021). Além disso, mesmo quando o IP é identificado, sua titularidade é atribuída à operadora de internet ou ao estabelecimento que o forneceu ,como lan houses ou redes de wi-fi público, exigindo diligências adicionais para vincular o endereço a um usuário específico. O Marco Civil da Internet, ao estabelecer a obrigação de guarda dos registros de conexão pelos provedores, criou um instrumento relevante para a investigação, conforme se extrai de seu artigo 13: "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento" (Brasil, 2014, art. 13).

Apesar da relevância desse dispositivo, o prazo de um ano para a guarda dos registros de conexão nem sempre é suficiente em investigações que se iniciam tardiamente, seja em razão da demora das vítimas em registrar a ocorrência, seja em virtude da morosidade dos próprios órgãos investigativos. A essa limitação agrega-se a questão dos provedores sediados no exterior, que frequentemente não se submetem às determinações judiciais brasileiras de forma direta, obrigando as autoridades a recorrer aos morosos mecanismos de cooperação jurídica internacional (Dobler, 2023). Tais obstáculos evidenciam a necessidade de um aparato investigativo especializado e de protocolos operacionais específicos para a apuração dos crimes cibernéticos, cujos traços de execução diferem substancialmente dos delitos tradicionais (Ribeiro; Lima, 2024).

4.2 Limitações na análise de provas digitais: a volatilidade das evidências e as dificuldades periciais

A prova digital apresenta características que a distinguem profundamente das modalidades probatórias tradicionais e que impõem desafios específicos tanto à sua coleta quanto à sua valoração nos processos penais. A volatilidade é a característica mais crítica das evidências digitais, pois dados armazenados em dispositivos eletrônicos, registros de acesso e metadados de comunicações podem ser alterados, apagados ou sobrescritos em questão de segundos, deliberadamente ou por simples operação técnica de rotina dos sistemas envolvidos (Escola de Magistrados da Justiça Federal da 3ª Região, 2012). Essa transitoriedade impõe à investigação criminal a necessidade de atuação célere e tecnicamente qualificada para a preservação das evidências antes que se percam definitivamente, sob pena de inviabilizar a comprovação da materialidade e da autoria do crime.

A admissibilidade das provas digitais nos processos penais depende do cumprimento de critérios rigorosos de autenticidade, integridade e cadeia de custódia, cujo conceito foi expressamente incorporado ao ordenamento processual penal brasileiro pela Lei nº 13.964/2019, o Pacote Anticrime. A ausência de protocolos padronizados de coleta e preservação de evidências digitais nos órgãos policiais brasileiros representa uma vulnerabilidade sistêmica que frequentemente compromete a validade jurídica das provas produzidas, abrindo espaço para questionamentos defensivos que podem resultar na absolvição de agentes cujos crimes estão materialmente documentados (Lima, 2024).

A perícia forense digital, embora reconhecida como instrumento indispensável na investigação dos crimes cibernéticos, enfrenta o déficit crônico de profissionais especializados nas delegacias e nos institutos de criminalística, bem como a desatualização dos equipamentos e softwares utilizados nas análises periciais (Wendt; Jorge, 2021). O Marco Civil da Internet, reconhecendo a relevância probatória dos registros eletrônicos, estabelece em seu artigo 22: "Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet" (Brasil, 2014, art. 22).

A judicialização da obtenção de dados digitais junto a provedores, embora necessária para preservar as garantias constitucionais de sigilo das comunicações e de privacidade, introduz uma etapa adicional no processo investigativo que pode comprometer a tempestividade da coleta das

evidências. Em crimes de phishing praticados em larga escala, nos quais os agentes frequentemente encerram as contas e apagam os rastros digitais logo após os golpes, a demora na obtenção da autorização judicial pode resultar na perda irreversível das provas (Gomes; Medrado; Gama, 2024). Esse dilema entre celeridade investigativa e salvaguarda das garantias individuais exige soluções normativas equilibradas, que permitam a preservação emergencial de dados suspeitos sem prescindir do controle judicial, à semelhança de modelos adotados em outros ordenamentos e preconizados pela Convenção de Budapeste (Brasil, 2023).

4.3 Cooperação internacional na investigação de fraudes digitais: a importância da colaboração entre países

A natureza transnacional do phishing e das fraudes digitais em geral constitui um dos principais fatores que ampliam a complexidade de sua investigação e comprometem a efetividade da responsabilização penal dos agentes. Grupos criminosos especializados em crimes cibernéticos frequentemente operam a partir de países com legislação menos rigorosa ou com capacidade investigativa limitada, utilizando infraestruturas tecnológicas distribuídas por múltiplas jurisdições para dificultar o rastreamento e a identificação de suas atividades. Nesse cenário, a cooperação jurídica internacional em matéria penal transcende a condição de instrumento complementar e se converte em pressuposto indispensável à efetividade da persecução criminal (Dobler, 2023).

O Brasil avançou significativamente nesse campo com a promulgação da Convenção de Budapeste sobre o Crime Cibernético, por meio do Decreto nº 11.491/2023. Essa convenção estabelece mecanismos de cooperação que permitem às autoridades brasileiras solicitar diretamente a preservação emergencial de dados armazenados em servidores localizados em países signatários, sem a necessidade de percorrer os longos trâmites dos pedidos formais de assistência mútua em matéria penal, conhecidos como cartas rogatórias. Além disso, a convenção fixa obrigações de tipificação penal mínima para os países signatários, contribuindo para a harmonização das legislações nacionais e facilitando o reconhecimento mútuo das infrações e das providências investigativas adotadas (Martins; Ferreira, 2023).

Não obstante a relevância da adesão à Convenção de Budapeste, persistem obstáculos práticos à efetividade da cooperação internacional. A diferença de sistemas jurídicos entre os países envolvidos, a ausência de acordos bilaterais específicos com nações que concentram grande parte da infraestrutura utilizada pelos criminosos cibernéticos e a demora nos

procedimentos formais de assistência mútua continuam a comprometer a celeridade das investigações (Calixto; Facuri; Teles, 2023). A busca por soluções mais ágeis tem levado à discussão sobre a possibilidade de requisição direta de dados a provedores estrangeiros que operem no Brasil, tema sobre o qual o Supremo Tribunal Federal se pronunciou no julgamento da Ação Declaratória de Constitucionalidade nº 51, reconhecendo a possibilidade de tal requisição com fundamento no artigo 11 do Marco Civil da Internet e no artigo 18 da própria Convenção de Budapeste (Gomes; Medrado; Gama, 2024). O aprofundamento desses mecanismos e a celebração de novos acordos bilaterais são apontados pela doutrina como caminhos prioritários para a superação dos gargalos que ainda comprometem a efetividade da persecução penal dos crimes cibernéticos transnacionais (Araújo et al., 2025).

4.4 O papel das plataformas digitais e das instituições financeiras na prevenção e combate ao phishing

A responsabilidade pelo enfrentamento ao phishing não recai exclusivamente sobre o Estado e seus órgãos de persecução penal. As plataformas digitais e as instituições financeiras ocupam posição estratégica na cadeia de eventos que compõe os ataques de phishing, tanto como possíveis vetores de propagação das fraudes quanto como atores fundamentais na sua prevenção e detecção. A Lei Geral de Proteção de Dados ,Lei nº 13.709/2018 ,estabeleceu obrigações relevantes para as organizações que tratam dados pessoais, incluindo o dever de adotar medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas que possam resultar em sua destruição, perda, alteração, comunicação ou difusão indevida (Brasil, 2018). O descumprimento dessas obrigações sujeita as organizações às sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados, que podem alcançar multas de até 2% do faturamento da pessoa jurídica no Brasil.

No âmbito específico das instituições financeiras, o Banco Central do Brasil e os órgãos reguladores do sistema financeiro têm expedido normas e recomendações voltadas ao fortalecimento dos mecanismos de autenticação, à implementação de sistemas de detecção de transações suspeitas e ao estabelecimento de canais de comunicação ágeis para o bloqueio de transferências fraudulentas. A efetividade dessas medidas, contudo, depende em larga medida da adesão das próprias vítimas às práticas de segurança digital recomendadas, o que reforça a importância das campanhas de educação e conscientização dos usuários (Ribeiro; Lima, 2024).

As plataformas de redes sociais, por sua vez, desempenham papel paradoxal na dinâmica do phishing: são ao mesmo tempo o principal canal de disseminação dos ataques e potenciais instrumentos de sua contenção. A cooperação dessas plataformas com as autoridades investigativas ,mediante o fornecimento de dados de identificação de perfis falsos, logs de acesso e registros de comunicação ,é frequentemente determinante para a identificação dos agentes criminosos. Contudo, essa cooperação ainda se ressente de assimetrias, pois as grandes plataformas digitais, em sua maioria sediadas no exterior, submetem o fornecimento de dados a procedimentos e critérios próprios que nem sempre se alinham plenamente às exigências do direito brasileiro (Wendt; Jorge, 2021). O aprimoramento dos mecanismos de interação entre o poder público, as instituições financeiras e as plataformas digitais é, portanto, condição essencial para a construção de uma resposta mais integrada e efetiva ao fenômeno do phishing no Brasil (Santos, 2024).

5 CONSIDERAÇÕES FINAIS

A análise empreendida ao longo deste artigo evidenciou que o phishing e o estelionato eletrônico constituem fenômenos criminais de alta complexidade, cujo enfrentamento eficaz exige muito mais do que a simples edição de normas penais mais severas. A Lei nº 14.155/2021 representou, sem dúvida, um avanço no reconhecimento da especificidade das fraudes eletrônicas e na tentativa de adequar o Código Penal às demandas da sociedade digital, ao criar a qualificadora da fraude eletrônica, agravar as penas dos crimes praticados por meios informáticos e fixar a competência jurisdicional no domicílio da vítima. Esses progressos, porém, não foram acompanhados de reformas processuais e investigativas proporcionais, o que limita o potencial transformador da legislação no plano da realidade concreta.

Os desafios identificados ao longo do estudo revelam que o problema da impunidade nos crimes de phishing é multifatorial. O anonimato digital, a volatilidade das provas eletrônicas, a transnacionalidade das operações criminosas, a insuficiência técnica dos órgãos de persecução penal e as lacunas na cooperação com plataformas digitais sediadas no exterior compõem um quadro que nenhuma norma penal isolada é capaz de resolver. A resposta adequada a esse quadro exige uma abordagem sistêmica, que articule o aprimoramento legislativo com o investimento em estrutura investigativa especializada, a modernização dos protocolos de coleta e preservação de provas digitais, o aprofundamento dos mecanismos de cooperação jurídica internacional e o fortalecimento da parceria com o setor privado.

A adesão do Brasil à Convenção de Budapeste, concretizada pelo Decreto nº 11.491/2023, representa um passo importante nessa direção, ao inserir o país em uma rede global de cooperação contra o cibercrime e ao comprometê-lo com padrões internacionais de investigação e punição das condutas digitalmente ilícitas. O aproveitamento pleno desse instrumento, contudo, depende da implementação interna de medidas normativas e operacionais compatíveis com os compromissos assumidos, o que ainda está em curso.

Conclui-se que a efetividade do combate ao phishing e ao estelionato eletrônico no Brasil demanda uma agenda de reformas que transcenda o campo estritamente penal. A educação digital da população, o fortalecimento da regulação das plataformas digitais, o investimento em perícia forense especializada e a construção de uma cultura institucional orientada para a prevenção, tanto quanto para a repressão, são dimensões indispensáveis a qualquer estratégia que aspire a resultados concretos na redução dos índices de vitimização e na responsabilização efetiva dos autores de crimes cibernéticos no país.

REFERÊNCIAS

ARAÚJO, Pena S. et al. Estratégias de políticas públicas no combate aos crimes cibernéticos: uma análise crítica. *Revista do Instituto Brasileiro de Segurança Pública (RIBSP)*, [S. l.], v. 8, n. 17, 2025. Disponível em: https://revista.ibsp.org.br/index.php/RIBSP/article/view/244. Acesso em: 12/04/2026.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética à luz do Marco Civil da Internet*. Rio de Janeiro: Brasport, 2016. Disponível em: https://www.editorabrasport.com.br/manual-de-investigacao-cibernetica-a-luz-do-marco-civil-da-internet. Acesso em: 12/04/2026.

BELINOTTE, Mariana et al. A Lei Carolina Dieckmann e o caso Snowden: respostas legislativas a incidentes de repercussão em segurança cibernética. *Relações Internacionais*, Lisboa, n. 82, p. 93-107, jun. 2024. Disponível em: https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri82/RI_82_NET_MarianaBelinotte_et_al.pdf. Acesso em: 12/04/2026.

BRASIL. *Decreto nº 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 12/04/2026.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12/04/2026.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012.* Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12/04/2026.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil; e dá outras providências (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12/04/2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12/04/2026.

BRASIL. *Lei nº 14.155, de 27 de maio de 2021.* Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 12/04/2026.

CALIXTO, Tharynne Marcela Barbosa; FACURI, Antônio Carlos Gomes; TELES, Fernando Hugo Miranda. As relações de cooperação jurídica internacional no combate às práticas de cibercrimes. *Revista do Ministério Público Militar*, Brasília, v. 50, n. 39, p. 235-244, 2023. Disponível em: https://revista.mpm.mp.br/rmpm/article/view/148. Acesso em: 12/04/2026.

DOBLER, Kellen. *Cooperação internacional em matéria penal e o crime cibernético no Brasil.* 2023. 159 f. Dissertação (Mestrado em Direito) ,Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023. Disponível em: https://www.bdtd.uerj.br:8443/handle/1/22382. Acesso em: 12/04/2026.

ESCOLA DE MAGISTRADOS DA JUSTIÇA FEDERAL DA 3ª REGIÃO (EMAG). *Investigação e prova nos crimes cibernéticos.* Cadernos de Estudos, n. 1. São Paulo: EMAG/TRF 3ª Região, 2012. Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 12/04/2026.

GOMES, Julio Cesar Lôbo da Costa; MEDRADO, Lucas Cavalcante; GAMA, Giliarde Benavinuto Albuquerque C. V. R. N. Crimes cibernéticos: desafios jurídicos no processo e julgamento de infrações penais virtuais cometidas por agentes estrangeiros contra vítimas brasileiras. *Revista JRG de Estudos Acadêmicos*, [S. l.], v. 7, n. 15, 2024. Disponível em: https://revistajrg.com/index.php/jrg/article/view/1563. Acesso em: 12/04/2026.

GOMES, Walyson Milhomem Souza de; MEDRADO, Lucas Cavalcante. Crimes cibernéticos: uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, São Paulo, v. 9, n. 9, p. 1870-1894, set. 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/11321. Acesso em: 12/04/2026.

LAI, Sauvei. Lei 14.155/2021 dos crimes cibernéticos. *CONAMP – Associação Nacional dos Membros do Ministério Público*, Rio de Janeiro, 15 jun. 2021. Disponível em: https://www.conamp.org.br/publicacoes/artigos-juridicos/8468-lei-14-155-2021-dos-crimes-ciberneticos.html. Acesso em: 12/04/2026.

LIMA, Douglas Magno Fernandes do Nascimento. *Os desafios da investigação nos crimes cibernéticos*. 2024. 74 f. Trabalho de Conclusão de Curso (Graduação em Direito) ,Universidade Federal da Paraíba, Santa Rita, 2024. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/31393. Acesso em: 12/04/2026.

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. Crimes virtuais no ordenamento jurídico brasileiro. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, São Paulo, v. 9, n. 8, p. 462-472, ago. 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/10850. Acesso em: 12/04/2026.

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. *Journal of Law and Sustainable Development*, [S. l.], v. 7, n. 2, p. 145-167, 2019. Disponível em: https://ojs.journalsdg.org/jlss/article/view/51. Acesso em: 12/04/2026.

MARTINS, Larissa Pinheiro; FERREIRA, Rodrigo Augusto. A adesão do Brasil à Convenção de Budapeste e o enfrentamento do cibercrime: entre a cooperação internacional e a expansão do Direito Penal. *Revista Eletrônica Direito & TI*, Porto Alegre, v. 1, n. 15, 2023. Disponível em: https://direitoeti.com.br/direitoeti/article/view/155. Acesso em: 12/04/2026.

PEREIRA, Emanuela Araújo. A fraude eletrônica à luz da Lei nº 14.155. *Revista Jus Navigandi*, Teresina, ano 26, n. 6561, 18 jun. 2021. Disponível em: https://jus.com.br/artigos/91226/a-fraude-eletronica-a-luz-da-lei-n-14-155. Acesso em: 12/04/2026.

RIBEIRO, Thiago Lucas Santos; LIMA, Nayara Ferreira. Crimes cibernéticos: análise do processo investigatório e os desafios para combatê-los. *Revista Científica Multidisciplinar FT*, [S. l.], 2024. Disponível em: https://revistaft.com.br/crimes-ciberneticos-analise-do-processo-investigatorio-e-os-desafios-para-combate-los/. Acesso em: 12/04/2026.

SANTOS, Marcelo Humberto de Oliveira. O estelionato por meio de fraude eletrônica: apontamentos da Lei 14.155/2021 e sua efetividade. *Revista Científica Multidisciplinar FT*, [S. l.], 2024. Disponível em: https://revistaft.com.br/o-estelionato-por-meio-de-fraude-eletronica-apontamentos-da-lei-14-155-2021-e-sua-efetividade/. Acesso em: 12/04/2026.

SILVA, Dickson Carvalho Gonçalves da. *Crimes cibernéticos: limites e desafios da investigação*. 2022. 68 f. Trabalho de Conclusão de Curso (Graduação em Direito) ,Centro Universitário UNDB, São Luís, 2022. Disponível em: http://repositorio.undb.edu.br/handle/areas/834. Acesso em: 12/04/2026.

SOUZA, Vitor Hugo Maciel de; RODRIGUES, Rafaela Aparecida. Crimes cibernéticos: fraude eletrônica e a efetividade da legislação brasileira. *Revista Científica Multidisciplinar FT*, [S. l.], out. 2025. Disponível em: https://revistaft.com.br/crimes-ciberneticos-fraude-eletronica-e-a-efetividade-da-legislacao-brasileira/. Acesso em: 12/04/2026.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos: ameaças e procedimentos de investigação*. 3. ed. Rio de Janeiro: Brasport, 2021. Disponível em: https://www.editorabrasport.com.br/crimes-ciberneticos-3-edicao. Acesso em: 12/04/2026.