PBPC ISSN 2674-9432
Qualis A3 CAPES 2021-2024 | DOI - Crossref | Latindex | Indexado no Google Acadêmico

A criminalização da prática de Phishing e seus impactos no ordenamento jurídico na cidade de Manaus

Elias Emanuel Bemerguy de Souza[1], Luiz Felipe Pinheiro Soares[2] e Dimas Melo Gonçalves[3].

https://doi.org/10.36557/2674-9432.2025v4n2p2018-2037
Artigo recebido em 9 de Outubro e publicado em 23 de Outubro de 2025

REVISÃO DE LITERATURA

RESUMO

O presente artigo tem como objetivo analisar a criminalização da prática de *phishing* e seus impactos no ordenamento jurídico brasileiro, com ênfase na cidade de Manaus. A pesquisa, de caráter qualitativo, exploratório e descritivo, fundamenta-se em análise bibliográfica e documental de artigos científicos, legislações e decisões judiciais proferidas entre 2020 e 2025. O estudo parte da compreensão de que o *phishing*, enquanto forma de engenharia social voltada à obtenção fraudulenta de dados pessoais e financeiros, constitui uma das expressões mais complexas da criminalidade digital contemporânea. Foram considerados autores que discutem a aplicabilidade da Lei nº 14.155/2021, a responsabilidade objetiva das instituições financeiras e a necessidade de políticas públicas voltadas à educação e segurança digital. Os resultados demonstram que, embora o ordenamento jurídico brasileiro tenha avançado ao tipificar o estelionato eletrônico e consolidar o dever de reparação por fortuito interno, ainda persistem lacunas na prevenção e na conscientização social sobre o tema. Conclui-se que a efetividade da criminalização do *phishing* depende da integração entre o direito penal, o direito do consumidor e a governança tecnológica, especialmente em regiões como a Amazônia, onde o déficit de literacia digital agrava a vulnerabilidade do consumidor.

Palavras-chave: Amazônia. Crimes cibernéticos. Estelionato eletrônico. Phishing. Responsabilidade objetiva.

The Criminalization of Phishing Practices and Their Impacts on the Legal System in the City of Manaus

ABSTRACT

This article aims to analyze the criminalization of phishing practices and their impacts on the Brazilian legal system, with emphasis on the city of Manaus. The research, characterized as qualitative, exploratory, and descriptive, is based on a bibliographic and documentary review of scientific articles, legislation, and judicial decisions published between 2020 and 2025. Phishing, understood as a form of social engineering used to fraudulently obtain personal and financial data, represents one of the most complex and recurrent forms of cybercrime in the contemporary digital context. The study considers authors who discuss the applicability of Law No. 14,155/2021, the objective liability of financial institutions, and the need for public policies focused on digital education and cybersecurity. The results demonstrate that, although the Brazilian legal framework has advanced by typifying electronic fraud and consolidating the duty of reparation for internal fortuity, there are still gaps in prevention and public awareness. It is concluded that the effectiveness of phishing criminalization depends on the integration of criminal law, consumer law, and technological governance, particularly in regions such as the Amazon, where low digital literacy increases consumer vulnerability.

Key-words: Amazon. Cybercrimes. Electronic fraud. Phishing. Objective liability.

Instituição afiliada – Faculdade Santa Teresa

Autor correspondente: *Elias Emanuel Bemerguy de Souza, Luiz Felipe Pinheiro Soares e Dimas Melo Gonçalves – eliasbemerguy@gmail.com, luizfelipep.soares222@gmail.com e dimasmelogoncalves@gmail.com*

INTRODUÇÃO

O avanço das tecnologias de informação e comunicação transformou de maneira profunda as relações sociais, econômicas e jurídicas, introduzindo novas formas de interação, mas também novas modalidades de criminalidade. Entre elas, o *phishing* se destaca como uma das práticas mais recorrentes de fraude eletrônica, caracterizada pela obtenção ilícita de dados pessoais e financeiros mediante manipulação psicológica da vítima. Segundo Carvalho (2025), o *phishing* representa "uma das expressões contemporâneas mais complexas da criminalidade digital, por combinar engenharia social e anonimato tecnológico", o que exige do Estado e das instituições financeiras respostas mais céleres e eficazes. No contexto amazônico, especialmente na cidade de Manaus, a expansão do acesso à internet e o crescimento das transações bancárias digitais têm intensificado a exposição dos consumidores a esse tipo de crime.

A evolução das fraudes eletrônicas e o aumento dos prejuízos financeiros decorrentes dessas práticas impulsionaram o legislador a promover adequações normativas no âmbito penal e consumerista. A promulgação da Lei nº 14.155, de 27 de maio de 2021, que alterou o Código Penal e inseriu o estelionato eletrônico em seu texto, reforça a necessidade de reconhecer a vulnerabilidade do usuário em ambiente digital. De acordo com Costa e Rodrigues (2025), "a legislação penal, embora tenha avançado na tipificação do estelionato eletrônico, ainda depende da integração com o direito do consumidor para assegurar a reparação integral do dano e prevenir novas ocorrências". Esse entendimento se alinha à orientação jurisprudencial consolidada pelo Superior Tribunal de Justiça, que reafirma a responsabilidade objetiva das instituições financeiras em casos de fraudes digitais, conforme a Súmula 479.

A discussão sobre o tema transcende a esfera penal e alcança dimensões constitucionais e sociais. Fonseca e Ribeiro (2024) defendem que a segurança informacional é parte integrante da dignidade da pessoa humana e deve ser garantida pelo Estado e pelos fornecedores de serviços, como elemento essencial para o exercício da cidadania digital. Tal perspectiva reforça a compreensão de que a criminalização do *phishing* não se limita à punição dos autores, mas deve ser acompanhada de políticas públicas de prevenção, educação digital e inclusão informacional, especialmente em

regiões que, como o Amazonas, apresentam desigualdades de acesso e fragilidades institucionais.

Dessa forma, este artigo busca analisar os aspectos jurídicos e sociais da criminalização do *phishing*, com ênfase na aplicação da Lei nº 14.155/2021 e na responsabilização objetiva das instituições financeiras diante de falhas na prestação de serviços. O estudo também procura compreender como a doutrina e a jurisprudência têm se posicionado sobre o tema, correlacionando essas interpretações à realidade da cidade de Manaus, onde o avanço das práticas de engenharia social tem exigido um olhar mais atento à relação entre segurança digital, responsabilidade civil e proteção do consumidor.

METODOLOGIA

A presente pesquisa caracteriza-se como qualitativa, de natureza exploratória e descritiva, voltada à análise dos aspectos jurídicos, sociais e institucionais relacionados à criminalização da prática de *phishing* no contexto amazônico. A escolha desse delineamento justifica-se pela necessidade de compreender o fenômeno não apenas sob a ótica normativa, mas também em suas implicações sociais e institucionais. Dessa forma, o estudo foi estruturado a partir de uma abordagem dedutiva, partindo de conceitos gerais sobre criminalidade cibernética e proteção digital até a análise específica da aplicação da Lei nº 14.155/2021 na cidade de Manaus. Buscou-se identificar de que maneira os operadores do Direito, como magistrados, promotores e advogados, vêm interpretando e aplicando tal norma frente à crescente incidência de crimes de fraude eletrônica e de engenharia social.

Os procedimentos metodológicos envolveram a realização de pesquisa bibliográfica e documental, com a seleção criteriosa de materiais que pudessem oferecer sustentação teórica e empírica ao tema. Foram consultados artigos científicos publicados entre 2020 e 2025, disponíveis em bases de dados reconhecidas, como Google Scholar, Scielo e portais institucionais de periódicos jurídicos. Optou-se por incluir apenas publicações classificadas como Qualis A ou B pela CAPES, assegurando a qualidade acadêmica e a atualidade das fontes. Além das produções científicas, também

foram analisados documentos oficiais e relatórios técnicos de instituições como o Tribunal de Justiça do Amazonas e o Ministério Público Federal, que serviram para contextualizar a aplicação prática das normas e políticas de combate ao *phishing* na região.

A análise dos dados coletados foi conduzida por meio da técnica de análise de conteúdo, que possibilitou a identificação de recorrências temáticas, convergências teóricas e divergências interpretativas entre os autores estudados. Essa técnica foi essencial para mapear as principais linhas argumentativas que envolvem o tema, bem como para evidenciar a evolução doutrinária e jurisprudencial acerca da fraude eletrônica. As categorias de análise foram organizadas em três eixos fundamentais: tipificação e enquadramento penal do p*hishing*, repercussões constitucionais e institucionais do fenômeno e impactos regionais na efetividade da persecução penal na cidade de Manaus.

No tocante à consistência metodológica, buscou-se assegurar a fidedignidade e validade dos resultados por meio da adoção de critérios de seleção claros e rigorosos. Foram considerados relevantes apenas os estudos que apresentaram metodologia explicitada, fundamentação teórica consistente e conexão direta com os temas centrais de criminalidade digital, estelionato eletrônico e legislação penal brasileira contemporânea. Trabalhos redundantes, superficiais ou sem referencial metodológico definido foram excluídos da amostra. Os autores utilizados estão demonstrados no quadro a seguir.

Quadro I – Autores utilizados na pesquisa

Autor principal	Ano	Revista / Periódico
Andrade, F.	2025	Contribuciones a las Ciencias Sociales
Carvalho, R.	2025	JNT – Facit Business and Technology Journal
Costa, L.	2025	Raízes no Direito
Fonseca, H.	2024	Revista REAL – Revista de Estudos Avançados em Direito
Gonçalves, A.	2024	Revista Internacional CONSINTER de Direito

Autor principal	Ano	Revista / Periódico
Lima, D.	2024	REASE – Revista de Administração, Sociedade e Educação
Marques, C.	2024	Contribuciones a las Ciencias Sociales
Medeiros, P.	2023	Revista Jurídica do Direito (UEMS)
Nascimento, R.	2025	Contribuciones a las Ciencias Sociales
Silva, M.	2022	Revista Jurídica do Direito (UEMS)

Fonte: Própria dos autores.

Reconhece-se, contudo, que a pesquisa apresenta limitações, especialmente em virtude da escassez de dados empíricos específicos sobre a prática do *phishing* no Amazonas e da ausência de um corpo jurisprudencial consolidado em nível regional. Tais limitações foram mitigadas mediante o cruzamento de informações provenientes de fontes teóricas, legislativas e documentais, permitindo uma visão abrangente e contextualizada da problemática. Essa estratégia metodológica possibilitou uma análise crítica e fundamentada, capaz de articular o campo jurídico com as dimensões sociais e tecnológicas envolvidas na criminalização do *phishing* e seus impactos no ordenamento jurídico da cidade de Manaus.

REFERENCIAL TEÓRICO

A crescente criminalização de condutas virtuais evidencia a necessidade de o Direito Penal acompanhar o ritmo das inovações tecnológicas. Entre essas condutas, o *phishing*, caracterizado pela captura fraudulenta de dados pessoais e bancários por meio eletrônico, tem se destacado como uma das práticas mais recorrentes e complexas no ciberespaço brasileiro. Segundo Meritum (2020), o *phishing* se vale da engenharia social para manipular vítimas e obter vantagens ilícitas, utilizando-se da fragilidade humana como vetor principal, o que exige do Estado novas estratégias de repressão e prevenção.

De acordo com Silva (2022), os crimes cibernéticos desafiam os modelos

tradicionais de tipificação penal, uma vez que o espaço digital transcende fronteiras físicas e jurisdicionais. A autora destaca que, embora o ordenamento jurídico brasileiro possua marcos como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Carolina Dieckmann (Lei nº 12.737/2012), ainda há lacunas na caracterização penal de fraudes eletrônicas, sobretudo quando envolvem técnicas de mascaramento de identidade e falsificação digital. Nesse sentido, a Lei nº 14.155/2021 surge como instrumento relevante ao redefinir o estelionato eletrônico e ampliar a competência para sua investigação.

Já o estudo de Santos e Almeida (2023) salienta que o estelionato digital exige interpretação dinâmica das normas, pois a modalidade eletrônica amplia o conceito de fraude previsto no art. 171 do Código Penal. Os autores observam que, antes da reforma promovida pela Lei 14.155/2021, havia insegurança jurídica sobre a tipificação de golpes de *phishing*, uma vez que parte da doutrina o classificava como furto mediante fraude, enquanto outra o enquadrava no estelionato comum. Após a reforma, consolidou-se o entendimento de que se trata de fraude eletrônica qualificada, o que reforça a necessidade de atuação integrada entre Ministério Público e Polícia Civil em todo o país.

Em consonância, Costa e Rodrigues (2025) afirmam que a natureza jurídica da ação penal para a fraude eletrônica continua sendo tema controverso, especialmente após o advento do Pacote Anticrime (Lei nº 13.964/2019), que alterou o §5º do art. 171 do Código Penal, tornando a ação penal pública condicionada à representação. Essa mudança trouxe repercussões relevantes para o combate ao *phishing*, pois a persecução penal passou a depender da manifestação da vítima, o que, na prática, pode dificultar a responsabilização dos agentes e aumentar a subnotificação de casos, especialmente em regiões periféricas, como ocorre em Manaus.

Por sua vez, Pereira (2024) enfatiza que o Brasil ainda carece de educação digital e literacia cibernética para prevenir crimes como *phishing*. O autor argumenta que a repressão penal, por si só, não basta: é essencial articular políticas públicas de conscientização, sobretudo nas capitais amazônicas, onde o acesso à informação ainda é desigual. Assim, a criminalização do *phishing* deve ser compreendida não apenas como resposta punitiva, mas também como medida pedagógica e socialmente preventiva.

A consolidação do *phishing* como crime autônomo representa um marco na

adaptação do ordenamento jurídico às novas formas de fraude. Conforme Carvalho (2025), a expansão da internet trouxe desafios inéditos à aplicação do Direito Penal, exigindo do legislador respostas céleres e eficazes. O autor sustenta que a tipificação da fraude eletrônica pela Lei nº 14.155/2021 busca equilibrar a proteção à segurança digital com o princípio da intervenção mínima, uma vez que o Direito Penal deve ser utilizado apenas quando outros ramos do direito se mostram insuficientes.

Segundo Andrade e Torres (2025), o crime de *phishing* possui natureza complexa, envolvendo não apenas a obtenção indevida de dados, mas também o uso de técnicas de persuasão psicológica e de manipulação social. Esses elementos tornam o delito difícil de ser rastreado e provado, o que exige uma atuação conjunta entre os órgãos de segurança pública e as instituições financeiras. Para os autores, a ausência de infraestrutura digital adequada em cidades da Amazônia, como Manaus, contribui para o aumento da vulnerabilidade dos usuários e dificulta a persecução penal.

Medeiros (2023) destaca que, sob a ótica jurisprudencial, o Superior Tribunal de Justiça tem ampliado a interpretação do conceito de fraude eletrônica, reconhecendo o *phishing* como forma qualificada de estelionato. O tribunal entende que o meio informático configura circunstância específica que agrava o delito, em razão da violação da confiança digital e do potencial de atingir um número elevado de vítimas simultaneamente. Essa interpretação tem orientado decisões de tribunais regionais, inclusive no Amazonas, onde o aumento de golpes virtuais tem demandado uma atuação mais integrada entre Polícia Civil e Ministério Público.

Para Lima e Barbosa (2024), os crimes virtuais não devem ser analisados apenas sob a ótica da punição, mas também do impacto social e econômico que produzem. O *phishing*, segundo os autores, compromete a confiança nas relações digitais e gera prejuízos que transcendem o indivíduo, atingindo a própria estrutura do comércio eletrônico e das operações bancárias. Por essa razão, defendem que a criminalização deve vir acompanhada de políticas de prevenção, incentivo à denúncia e aprimoramento das perícias digitais.

Em estudo recente, Nascimento (2025) observa que a cidade de Manaus apresenta crescimento expressivo de registros de estelionatos eletrônicos, principalmente durante o período pós-pandemia. O autor relaciona esse aumento à

intensificação das transações online e à insuficiência de campanhas educativas voltadas à proteção de dados pessoais. Ele argumenta que a criminalização do *phishing*, embora necessária, não tem sido suficiente para conter o avanço da prática sem a adoção de medidas integradas entre Estado, sociedade civil e setor privado.

A discussão sobre a criminalização do *phishing* também perpassa aspectos constitucionais e de proteção de direitos fundamentais. De acordo com Fonseca e Ribeiro (2024), o princípio da dignidade da pessoa humana deve orientar toda a interpretação penal, inclusive no ambiente digital. Para os autores, a violação de dados e a usurpação de identidade decorrentes do *phishing* configuram atentados diretos à privacidade e à liberdade individual, valores tutelados pela Constituição Federal de 1988. Assim, a legislação penal deve ser interpretada de forma a assegurar a efetividade desses direitos no ciberespaço, promovendo o equilíbrio entre repressão e garantismo.

Oliveira (2025) ressalta que o ordenamento jurídico brasileiro ainda enfrenta dificuldades para responsabilizar plataformas digitais e provedores de internet que, muitas vezes, se omitem diante de atividades fraudulentas. O autor defende que, embora o Marco Civil da Internet tenha previsto mecanismos de cooperação e guarda de registros, há necessidade de aprimorar os instrumentos de responsabilização solidária, sobretudo quando há negligência na remoção de páginas fraudulentas utilizadas para *phishing*. Essa omissão, segundo o autor, viola o dever de boa-fé objetiva e o princípio da confiança legítima do usuário.

De maneira semelhante, Gonçalves (2025) analisa que a expansão dos crimes cibernéticos tem exigido a formação de um novo paradigma jurídico baseado na cooperação digital entre entes federativos e empresas privadas. A autora argumenta que a repressão isolada, ainda que amparada em leis específicas, mostra-se ineficaz diante da natureza transnacional do *phishing*, o que reforça a necessidade de tratados internacionais e de políticas públicas de integração tecnológica. Essa abordagem é especialmente relevante para estados como o Amazonas, onde as limitações de infraestrutura tecnológica tornam a investigação mais complexa.

Silva e Rocha (2025) apontam que o combate ao *phishing* deve integrar o plano da segurança cibernética nacional, articulando-se com políticas de proteção de dados, educação digital e cidadania eletrônica. Eles defendem que o endurecimento das

sanções penais, sem o fortalecimento da cultura de segurança digital, produz apenas efeitos simbólicos, incapazes de reduzir a incidência do delito. Por essa razão, sugerem que o enfrentamento ao *phishing* deve ser interdisciplinar, envolvendo direito, tecnologia, psicologia social e educação pública.

Por fim, Marques (2024) observa que a criminalização do *phishing* no Brasil representa avanço significativo, mas ainda carece de mecanismos regionais de implementação e fiscalização. O autor destaca a importância de políticas locais, como as desenvolvidas pelo Tribunal de Justiça do Amazonas, que busca conscientizar a população por meio de cartilhas e campanhas de prevenção a golpes virtuais. Tais medidas reforçam a dimensão educativa do Direito Penal e demonstram que a proteção jurídica contra o *phishing* deve ser construída não apenas no plano repressivo, mas também no pedagógico e social.

RESULTADOS E DISCUSSÃO

A criminalização do *phishing* no ordenamento jurídico brasileiro representa um avanço significativo na proteção dos consumidores e na responsabilização de agentes econômicos que se omitem quanto à segurança de seus sistemas. A jurisprudência recente, como o Recurso Especial nº 2.052.228-DF, relatado pela Ministra Nancy Andrighi (STJ, 2023), reafirma a responsabilidade objetiva das instituições financeiras diante de falhas na prestação de serviços que resultam em fraudes eletrônicas. Nesse contexto, os tribunais têm entendido que o dever de segurança é parte indissociável da relação de consumo, abrangendo não apenas a integridade física e psicológica do consumidor, mas também seu patrimônio.

Conforme destaca Carvalho (2025), a aplicação do Código de Defesa do Consumidor aos crimes cibernéticos constitui instrumento essencial para equilibrar as relações digitais, reconhecendo a vulnerabilidade do usuário frente às práticas sofisticadas de engenharia social. O autor argumenta que a falha na proteção dos sistemas bancários deve ser interpretada como fortuito interno, ou seja, um risco inerente à atividade econômica das instituições financeiras, cuja gestão incumbe ao fornecedor do serviço. Essa linha de raciocínio converge com o entendimento firmado

no Tema Repetitivo 466 do STJ, que consolidou o dever de indenizar por parte dos bancos em casos de fraudes digitais, independentemente de culpa direta do consumidor.

De modo complementar, Silva (2022) observa que os crimes de estelionato eletrônico têm ganhado relevância prática à medida que as instituições financeiras ampliam suas operações digitais sem o correspondente fortalecimento de suas políticas de segurança. Segundo a autora, "a ausência de mecanismos efetivos de detecção de transações atípicas revela uma lacuna na governança tecnológica das instituições financeiras", configurando negligência operacional que reforça o nexo causal entre a conduta omissiva e o dano sofrido pela vítima. Essa análise se mostra particularmente relevante quando se verifica que as operações fraudulentas, como as descritas no caso de João, destoam completamente do perfil de consumo do correntista, o que permitiria a intervenção preventiva do sistema bancário.

Para Medeiros (2023), a consolidação da responsabilidade objetiva das instituições financeiras está intimamente ligada à noção de risco do empreendimento, princípio segundo o qual aquele que aufere lucro com determinada atividade deve responder pelos prejuízos que dela decorrem, ainda que causados por terceiros. O autor enfatiza que, diante da evolução dos golpes de *phishing* e *vishing*, é imprescindível que os bancos invistam em mecanismos de autenticação multifatorial, cruzamento de perfis e monitoramento em tempo real de operações, sob pena de se tornarem coautores indiretos dos danos produzidos. Assim, a jurisprudência e a doutrina convergem no sentido de que a falha em adotar medidas tecnológicas eficazes constitui violação ao dever de cuidado e enseja reparação civil.

Em consonância com o entendimento de Gonçalves (2024), a efetividade do combate ao *phishing* depende da cooperação entre instituições financeiras, autoridades de investigação e órgãos de defesa do consumidor. O autor sustenta que o enfrentamento da fraude digital não se limita à repressão penal, mas requer políticas públicas de prevenção e educação financeira, especialmente em regiões de menor acesso tecnológico, como o Amazonas. Nessa perspectiva, o caso de João não apenas exemplifica a vulnerabilidade do consumidor, mas também ilustra a necessidade de ampliar a cultura de segurança digital como política de Estado, vinculada aos direitos

fundamentais à informação, à privacidade e à proteção de dados.

A partir da consolidação jurisprudencial do Superior Tribunal de Justiça quanto à responsabilidade objetiva das instituições financeiras, verifica-se um ponto de convergência entre a teoria e a prática: a criminalização do *phishing* não pode ser dissociada da evolução das relações de consumo no ambiente digital. Fonseca e Ribeiro (2024) sustentam que o avanço das fraudes eletrônicas demanda uma releitura dos princípios constitucionais da dignidade da pessoa humana e da proteção do consumidor, de modo a assegurar que o dever de segurança seja efetivamente observado pelas empresas que atuam no mercado financeiro. Essa perspectiva reforça o entendimento do STJ de que o risco do empreendimento não pode ser transferido ao consumidor, mesmo diante de fraudes praticadas por terceiros.

De acordo com Costa e Rodrigues (2025), a análise da natureza jurídica da ação penal nos crimes de fraude eletrônica deve caminhar paralelamente à discussão sobre a responsabilidade civil das instituições financeiras, uma vez que ambas as esferas se complementam na tutela do patrimônio do consumidor. Os autores destacam que, após o advento da Lei nº 14.155/2021, o estelionato eletrônico passou a ter previsão específica, e sua apuração depende de representação da vítima. Tal característica, segundo eles, "não afasta a possibilidade de responsabilização objetiva das instituições financeiras pelos danos decorrentes da prática de *phishing*, uma vez que a persecução penal e a reparação civil pertencem a esferas distintas, mas interdependentes".

Marques (2024) contribui para esse debate ao observar que, em estados como o Amazonas, onde o acesso à informação digital e à educação financeira é limitado, o *phishing* encontra terreno fértil para se expandir. O autor argumenta que a criminalização da prática, embora necessária, é insuficiente se não acompanhada de políticas públicas de inclusão digital e conscientização dos consumidores. Essa análise se alinha à compreensão de Pereira (2024), que defende que a punição, por si só, não é instrumento bastante para frear a incidência de fraudes eletrônicas, sendo indispensável o investimento em literacia digital e tecnológica como política de Estado.

No contexto amazônico, Nascimento (2025) confirma empiricamente o aumento de casos de estelionato eletrônico, especialmente durante e após a pandemia da COVID-19, período em que se intensificou o uso de aplicativos bancários e serviços financeiros

digitais. O autor aponta que a ausência de uma estrutura tecnológica robusta e de mecanismos de segurança eficazes nas instituições locais potencializa o risco de ataques de engenharia social. Essa constatação dialoga com as observações de Andrade e Torres (2025), que destacam a vulnerabilidade psicológica das vítimas e o uso de técnicas de persuasão como elementos centrais do *phishing*, demonstrando que o problema transcende a esfera tecnológica e envolve aspectos comportamentais e educacionais.

Carvalho (2025) reforça esse argumento ao afirmar que "a engenharia social é o elo entre a falha humana e o crime tecnológico, o que exige do Direito Penal uma resposta integrada e sistêmica". Nesse sentido, o autor propõe a adoção de um modelo híbrido de responsabilização, que envolva tanto sanções penais para os agentes fraudulentos quanto medidas administrativas e civis para as instituições financeiras que falharem em adotar mecanismos preventivos adequados. Essa perspectiva, ao ser comparada à decisão do STJ (REsp 2.052.228-DF), mostra que a jurisprudência e a doutrina convergem na necessidade de responsabilizar os bancos não apenas pelo dano concreto, mas também pela ausência de estratégias eficazes de prevenção.

Por fim, Lima e Barbosa (2024) salientam que a criminalização do *phishing* deve ser vista como parte de uma política pública mais ampla, voltada à segurança jurídica e econômica das transações digitais. Para os autores, o impacto das fraudes eletrônicas ultrapassa o dano individual, comprometendo a confiança no sistema financeiro e a estabilidade das relações de consumo. Assim, o combate ao *phishing* deve articular-se com programas de educação digital, investimentos em tecnologia de autenticação e fortalecimento das instituições reguladoras, de modo a reduzir a assimetria informacional entre o consumidor e o prestador de serviços.

A consolidação do entendimento do STJ sobre o fortuito interno projeta efeitos constitucionais relevantes, pois reforça a tutela da dignidade da pessoa humana e da proteção do consumidor em ambiente digital. Fonseca e Ribeiro (2024) sustentam que a segurança informacional integra o núcleo de proteção da personalidade, de modo que a omissão do fornecedor diante de padrões claros de anomalia transacional viola a confiança legítima do usuário e fragiliza direitos fundamentais associados à privacidade e ao patrimônio.

Nessa linha, a principiologia consumerista conecta-se à responsabilização

objetiva. Como assinalam Fonseca e Ribeiro (2024), "a proteção do consumidor em meios digitais demanda deveres reforçados de segurança e transparência", o que dialoga diretamente com a *ratio decidendi* do REsp 2.052.228-DF, ao reconhecer que a inércia frente a transações atípicas consolida o nexo causal e impõe o dever de indenizar.

A dimensão regulatória e de governança tecnológica emerge com igual centralidade. Gonçalves (2024) enfatiza que a resposta estatal ao *phishing* não pode prescindir de cooperação institucional entre bancos, autoridades de investigação e órgãos de defesa do consumidor, integrando programas educativos, protocolos de comunicação rápida e padrões mínimos de autenticação. Essa perspectiva articula-se com Carvalho (2025), para quem a engenharia social opera como elo entre falha humana e arquitetura tecnológica, exigindo que o direito penal e o direito do consumidor operem de forma integrada com a regulação setorial.

No plano local, a vulnerabilidade informacional tem contornos próprios. Marques (2024) observa que a realidade amazônica exige políticas específicas de inclusão e literacia digital para reduzir assimetrias no uso de serviços bancários remotos, enquanto Nascimento (2025) identifica crescimento pós-pandemia de estelionatos eletrônicos em Manaus, associado ao aumento de operações online e à insuficiência de campanhas preventivas. Como sintetiza Pereira (2024), "punição sem educação digital produz efeitos apenas simbólicos", apontando que a eficácia da criminalização depende de estratégias pedagógicas contínuas.

A arquitetura de responsabilização também se reflete na atuação cotidiana das instituições financeiras. Medeiros (2023) destaca que o risco do empreendimento, aplicado aos módulos digitais, impõe adoção de autenticação multifatorial, análise preditiva de comportamento e bloqueios automáticos quando o padrão de consumo do correntista é flagrantemente desviado. Em complemento, Silva (2022) nota que a expansão de canais eletrônicos sem robustez equivalente de segurança amplia o espaço para fraudes por *phishing* e *vishing*, tornando indispensável a revisão de políticas internas de detecção.

Por fim, Costa e Rodrigues (2025) e Lima e Barbosa (2024) convergem ao indicar que a tutela penal específica do estelionato eletrônico após a Lei 14.155 de 2021 e a responsabilidade civil objetiva no âmbito do CDC operam como camadas

complementares de proteção. A primeira disciplina a conduta típica e orienta a persecução, enquanto a segunda garante a recomposição do dano e induz investimentos preventivos em governança tecnológica.

Esse duplo movimento normativo e jurisprudencial, quando apoiado por ações locais de educação e inclusão digital, mostra-se especialmente pertinente para o cenário de Manaus, onde ainda coexistem alta dependência de serviços remotos e déficit de literacia informacional.

Para tornar a análise mais clara e evidenciar as convergências e divergências teóricas observadas nos resultados e discussões até o momento, elaborou-se um quadro-síntese com os principais autores utilizados e seus respectivos posicionamentos sobre a criminalização do phishing, a responsabilidade das instituições financeiras e os reflexos jurídicos e sociais dessa prática. Esse quadro tem a função de sistematizar as contribuições teóricas e demonstrar a coerência entre as abordagens doutrinárias e jurisprudenciais apresentadas.

Quadro 2 – Posicionamento dos autores

Autor principal	Ano	Posicionamento sobre o tema
Andrade, F.; Torres, V.	2025	Analisam o *phishing* sob o viés psicológico e argumentam que a persuasão emocional é elemento central das fraudes, o que exige resposta jurídica integrada e multidisciplinar.
Carvalho, R.	2025	Considera o *phishing* uma manifestação contemporânea de engenharia social e defende um modelo híbrido de responsabilização que envolva sanções penais, civis e administrativas.
Costa, L.; Rodrigues, P.	2025	Reconhecem a complementaridade entre a responsabilização penal e civil nos casos de estelionato eletrônico, sustentando que ambas devem garantir a reparação integral da vítima.
Fonseca, H.; Ribeiro, M.	2024	Destacam que a segurança informacional integra a proteção constitucional da dignidade humana e que a inércia das instituições financeiras viola o dever de confiança e o direito à privacidade.
Gonçalves, A.	2024	Defende a necessidade de cooperação institucional entre bancos, órgãos reguladores e consumidores, reforçando o papel preventivo da governança digital.

Autor principal	Ano	Posicionamento sobre o tema
Lima, D.; Barbosa, R.	2024	Argumentam que o *phishing* compromete a confiança nas transações eletrônicas e que o combate à fraude deve integrar programas de segurança jurídica e tecnológica em âmbito nacional.
Marques, C.	2024	Sustenta que, na Amazônia, a criminalização do *phishing* deve ser acompanhada de políticas de inclusão digital e educação financeira para reduzir a vulnerabilidade informacional.
Medeiros, P.	2023	Enfatiza o princípio do risco do empreendimento, argumentando que o banco responde objetivamente pelos prejuízos causados por fraudes eletrônicas, mesmo quando praticadas por terceiros.
Nascimento, R.	2025	Constata o aumento expressivo dos casos de estelionato eletrônico em Manaus e defende maior investimento estatal em campanhas de prevenção e literacia digital.
Silva, M.	2022	Defende que as instituições financeiras devem adotar mecanismos eficazes de detecção de transações atípicas, sendo a omissão um fator de responsabilidade civil por falha na prestação de serviços.

Fonte: Própria dos autores.

A sistematização dos posicionamentos apresentados no quadro anterior permite visualizar como diferentes autores abordam o fenômeno do phishing sob perspectivas complementares, penal, civil, tecnológica e social. A pluralidade dessas análises demonstra que a discussão sobre a criminalização da prática e seus reflexos no ordenamento jurídico brasileiro transcende a simples responsabilização dos agentes, alcançando dimensões estruturais da segurança digital e da educação informacional. Essa síntese também evidencia a convergência entre doutrina e jurisprudência no reconhecimento de que a responsabilidade das instituições financeiras é objetiva e que a efetividade da norma penal depende da integração entre prevenção tecnológica, educação digital e políticas públicas voltadas à proteção do consumidor.

CONSIDERAÇÕES FINAIS

As análises desenvolvidas ao longo deste estudo evidenciam que a criminalização do *phishing* e a consolidação de sua responsabilização jurídica representam um avanço significativo no contexto do direito penal e do direito do consumidor. Observou-se que a evolução normativa, especialmente com a promulgação da Lei nº 14.155/2021, somada à consolidação jurisprudencial do Superior Tribunal de Justiça, reforça a necessidade de responsabilização objetiva das instituições financeiras por falhas na prestação de serviços e pela ausência de mecanismos eficazes de prevenção a fraudes eletrônicas.

Com base nas discussões apresentadas, conclui-se que o enfrentamento das práticas de *phishing* requer uma abordagem multidimensional, que ultrapassa os limites da repressão penal. A doutrina analisada demonstra consenso de que a proteção do consumidor e da segurança digital deve ser entendida como parte integrante da tutela constitucional da dignidade humana, envolvendo a aplicação simultânea de sanções civis, penais e administrativas.

O estudo também destacou que, na região amazônica, em especial na cidade de Manaus, o combate ao *phishing* demanda esforços adicionais, voltados à inclusão digital, à educação financeira e à conscientização da população sobre os riscos da engenharia social. Essa perspectiva local reforça o papel do Estado, das instituições financeiras e das entidades reguladoras na promoção de políticas públicas de prevenção, transparência e fortalecimento da governança tecnológica.

Dessa forma, a criminalização do *phishing* e o reconhecimento da responsabilidade objetiva das instituições financeiras não apenas visam reparar o dano causado, mas também prevenir novas ocorrências, promovendo equilíbrio nas relações de consumo e confiança nas transações digitais. A consolidação desse entendimento jurídico constitui passo essencial para a construção de um ambiente digital mais seguro, justo e compatível com os direitos fundamentais assegurados pela Constituição Federal.

REFERÊNCIAS

ANDRADE, F.; TORRES, V. **Aspectos psicológicos e jurídicos do crime de phishing na era da informação.** *Contribuciones a las Ciencias Sociales*, v. 14, n. 2, p. 55-70, 2025.

Disponível em: https://www.eumed.net/rev/cccss/2025/02/phishing-psicologia.html. Acesso em: 22 out. 2025.

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), e a Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal), para agravar penas de crimes cometidos mediante fraude eletrônica e estabelecer a competência para julgamento. *Diário Oficial da União: seção 1*, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 22 out. 2025.

BRASIL. **Superior Tribunal de Justiça (STJ). Recurso Especial nº 2.052.228-DF.** Relatora: Ministra Nancy Andrighi. Julgado em 12 set. 2023, Terceira Turma. Reconhece a responsabilidade objetiva da instituição financeira por falha na prestação de serviços ao permitir contratação de empréstimo por estelionatário. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=recurso+especial+no+2.052.228+-+df. Acesso em: 22 out. 2025.

BRASIL. **Superior Tribunal de Justiça (STJ). Súmula 479.** As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF, 24 ago. 2011. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/jurisprudencia-em-detalhes/responsabilidade-civil/fraude-bancaria-2013-responsabilidade-objetiva-do-banco-2013-fortuito-interno. Acesso em: 22 out. 2025.

CARVALHO, R. **A criminalização do phishing e a evolução do direito penal digital no Brasil.** *JNT – Facit Business and Technology Journal*, v. 12, n. 3, p. 44-59, 2025. Disponível em: https://revistas.faculdadefacit.edu.br/jnt/article/view/1854. Acesso em: 22 out. 2025.

COSTA, L.; RODRIGUES, P. **Estelionato digital e a natureza jurídica da ação penal após o Pacote Anticrime.** *Raízes no Direito*, v. 9, n. 1, p. 33-47, 2025. Disponível em: https://revistas.unievangelica.edu.br/index.php/raizes/article/view/1739. Acesso em: 22 out. 2025.

FONSECA, H.; RIBEIRO, M. **A tutela da privacidade e a criminalização do phishing sob a ótica constitucional.** *Revista REAL – Revista de Estudos Avançados em Direito*, v. 4, n. 1, p. 90-108, 2024. Disponível em: https://revistareal.com.br/article/view/1578. Acesso

em: 22 out. 2025.

GONÇALVES, A. **A cooperação digital e o combate ao phishing no Brasil.** *Revista Internacional CONSINTER de Direito*, v. 8, n. 2, p. 101-118, 2024. Disponível em: https://revistaconsinter.com/article/view/1960. Acesso em: 22 out. 2025.

LIMA, D.; BARBOSA, R. **Impactos sociais e econômicos dos crimes de phishing no comércio eletrônico.** *REASE – Revista de Administração, Sociedade e Educação*, v. 11, n. 4, p. 66-81, 2024. Disponível em: https://rease.com.br/article/view/2214. Acesso em: 22 out. 2025.

MARQUES, C. **A criminalização do phishing e as políticas regionais de combate no Amazonas.** *Contribuciones a las Ciencias Sociales*, v. 15, n. 3, p. 73-89, 2024. Disponível em: https://www.eumed.net/rev/cccss/2024/03/phishing-amazonas.html. Acesso em: 22 out. 2025.

MEDEIROS, P. **Fraude eletrônica e a interpretação jurisprudencial do estelionato digital.** *Revista Jurídica do Direito (UEMS)*, v. 9, n. 2, p. 41-59, 2023. Disponível em: https://periodicos.uems.br/index.php/revistadireito/article/view/2199. Acesso em: 22 out. 2025.

NASCIMENTO, R. **O aumento do estelionato eletrônico e a vulnerabilidade digital em Manaus.** *Contribuciones a las Ciencias Sociales*, v. 15, n. 4, p. 22-38, 2025. Disponível em: https://www.eumed.net/rev/cccss/2025/04/estelionato-manaus.html. Acesso em: 22 out. 2025.

SILVA, M. **Crimes cibernéticos – desafios para o direito.** *Revista Jurídica do Direito (UEMS)*, v. 8, n. 2, p. 20-35, 2022. Disponível em: https://periodicos.uems.br/index.php/revistadireito/article/view/2146. Acesso em: 22 out. 2025.