

NATHALIA KARINE CAVALCANTE SILVA
SABRINA ENDLICH DOS SANTOS

RESPONSABILIDADE PENAL NO CRIME DE ESTELIONATO ONLINE

Artigo Científico apresentado ao Centro Universitário São Lucas Ji-Paraná – São Lucas JPR, para obtenção de nota na disciplina Trabalho de Conclusão – Projeto de Pesquisa, no curso Direito, sob orientação do Prof. Esp. Teófilo Lourenço de Lima.

Ji-Paraná
2026

Dados Internacionais de Catalogação na Publicação - CIP

S586r	Silva, Nathalia Karine Cavalcante. Responsabilidade penal no crime de estelionato online. / Nathalia Karine Cavalcante Silva; Sabrina Endlich dos Santos. – Ji-Paraná, 2026. 32 p. Artigo Científico (Curso de Direito) – Afya Centro Universitário de Ji-Paraná, 2026. Orientador: Prof. Esp. Teófilo Lourenço de Lima. 1. Estelionato. 2. Cibercrime. 3. Responsabilidade. 4. Penal. I. Santos, Sabrina Endlich dos. II. Lima, Teófilo Lourenço de. III. Título. CDU 343.722:004
-------	--

RESPONSABILIDADE PENAL NO CRIME DE ESTELIONATO ONLINE

Nathalia Karine Cavalcante Silva¹

Sabrina Endlich dos Santos²

Teófilo Lourenço de Lima³

RESUMO: O presente estudo analisa a responsabilidade penal no crime de estelionato online diante das transformações tecnológicas e dos desafios enfrentados pelo Direito Penal contemporâneo. O avanço da internet e das ferramentas digitais ampliou significativamente a ocorrência de fraudes virtuais, exigindo adaptações normativas e interpretativas do ordenamento jurídico brasileiro. Nesse contexto, destaca-se a Lei nº 14.155/2021, que promoveu alterações no Código Penal, agravando as penas para o estelionato praticado por meio eletrônico. Contudo, verifica-se que a simples ampliação punitiva não é suficiente para garantir a efetividade da persecução penal, especialmente diante das dificuldades relacionadas à identificação da autoria, à volatilidade das provas digitais e à atuação transnacional dos agentes criminosos. A pesquisa, de natureza qualitativa e caráter exploratório, utiliza método dedutivo e análise bibliográfica e documental para compreender os limites e as possibilidades do sistema jurídico no enfrentamento desse tipo de criminalidade. Além disso, examina a interação entre o Direito Penal, o Direito Civil e o Direito do Consumidor, evidenciando a necessidade de uma atuação integrada. Conclui-se que o combate ao estelionato online exige não apenas avanços legislativos, mas também investimentos em tecnologia, capacitação institucional e políticas públicas preventivas.

Palavras-chave: Estelionato; Cibercrime; Responsabilidade; Penal.

CRIMINAL LIABILITY IN THE CRIME OF ONLINE FRAUD

ABSTRACT: This study analyzes criminal liability regarding the crime of online fraud in light of technological transformations and the challenges facing contemporary Criminal Law. The advancement of the internet and digital tools has significantly increased the occurrence of virtual fraud, necessitating normative and interpretive adaptations within the Brazilian legal system. In this context, Law No. 14,155/2021 stands out; it amended the Penal Code, increasing the penalties for fraud committed

¹ Acadêmica do 8º período do curso de Direito na Afya Centro Universitário de Ji-paraná. E-mail: nathaliakcavalcante6711@gmail.com

² Bacharel em Serviço Social pelo CEULJI/ULBRA, 2014; Tecnólogo em Estética pelo Instituto Monalisa, 2016 e acadêmica do 7º período do curso de Direito na Afya Centro Universitário de Ji-paraná. E-mail: s.endlich.s@gmail.com

³ Professor orientador, pós-graduado em Administração e Planejamento para Docentes pela ULBRA, 1996; pós-graduado em Inovação, Gestão e Práticas Docentes no Ensino Superior pela Faculdade Santo Agostino, 2021. Licenciado em Pedagogia pela Universidade Federal de Rondônia, 1996; Bacharel em Direito pelo Centro Universitário São Lucas Ji-Paraná. Ji-Paraná, Rondônia, Brasil. Email: teofilolourencodelima@gmail.com

through electronic means. However, it is observed that a mere punitive expansion is insufficient to ensure the effectiveness of criminal prosecution, particularly given the difficulties related to identifying perpetrators, the volatility of digital evidence, and the transnational operations of criminal agents. This research, qualitative in nature and exploratory in character, employs a deductive method as well as bibliographic and documentary analysis to understand the limits and possibilities of the legal system in combating this type of criminality. Furthermore, it examines the interplay among Criminal Law, Civil Law, and Consumer Law, highlighting the need for an integrated approach. The study concludes that combating online fraud requires not only legislative advancements but also investments in technology, institutional capacity-building, and preventive public policies. Keywords: Fraud; Cybercrime; Liability; Criminal.

1. INTRODUÇÃO

O avanço das tecnologias digitais e a expansão do acesso à internet transformaram profundamente as relações sociais, econômicas e jurídicas na contemporaneidade. A facilidade de comunicação, a rapidez das transações e a ampliação do comércio eletrônico trouxeram inúmeros benefícios à sociedade, mas também criaram um ambiente propício para o surgimento de novas modalidades de criminalidade. Nesse contexto, destaca-se o estelionato online, que se consolida como uma das infrações penais mais recorrentes no cenário atual, caracterizado pela utilização de meios tecnológicos para induzir vítimas em erro e obter vantagens ilícitas.

Embora o ordenamento jurídico brasileiro já prevísse o crime de estelionato no artigo 171 do Código Penal, a crescente incidência de fraudes praticadas no ambiente digital evidenciou a necessidade de atualização normativa, culminando na promulgação da Lei nº 14.155/2021. Essa legislação buscou adequar o tipo penal às novas formas de execução do delito, especialmente por meio eletrônico, além de agravar as penas aplicáveis. No entanto, apesar desse avanço legislativo, persistem questionamentos relevantes acerca da efetividade dessas medidas no enfrentamento da criminalidade digital.

A complexidade do estelionato online ultrapassa a simples tipificação penal, envolvendo desafios significativos relacionados à identificação da autoria, à produção e preservação de provas digitais e à atuação coordenada dos órgãos de persecução penal. Ademais, a natureza transnacional dessas condutas ilícitas e o uso de tecnologias cada vez mais sofisticadas, como inteligência artificial e mecanismos de

anonimização, impõem limites à atuação estatal e evidenciam a necessidade de uma abordagem mais ampla e integrada.

Diante desse cenário, o presente estudo tem como objetivo analisar a responsabilidade penal no crime de estelionato online, à luz das transformações tecnológicas e das inovações legislativas recentes, com destaque para a Lei nº 14.155/2021. Busca-se, ainda, examinar as dificuldades probatórias, os desafios enfrentados pelo Direito Penal contemporâneo e a interação com outros ramos do Direito, como o Direito Civil e o Direito do Consumidor.

A problemática central da pesquisa consiste em investigar em que medida o Direito Penal brasileiro é eficaz na repressão ao estelionato online, considerando as limitações técnicas, probatórias e jurisdicionais próprias do ambiente digital. Parte-se da hipótese de que, embora existam avanços normativos, a efetividade da resposta penal ainda é comprometida por deficiências estruturais e pela inadequação dos mecanismos tradicionais frente às novas dinâmicas tecnológicas.

Para tanto, a pesquisa adota abordagem qualitativa, de caráter exploratório e descritivo, utilizando-se do método dedutivo e de análise bibliográfica e documental, com base em doutrina, legislação e jurisprudência atualizadas. Ao final, pretende-se contribuir para o debate acadêmico e jurídico acerca da necessidade de reformulação das estratégias de enfrentamento da criminalidade digital, destacando a importância de uma atuação que vá além da resposta penal tradicional.

2. MATERIAL E MÉTODOS

A presente pesquisa caracteriza-se como básica, de natureza qualitativa, com enfoque exploratório e descritivo, tendo como objetivo compreender de forma aprofundada a responsabilidade penal decorrente da prática do crime de estelionato online, sob a ótica do Direito Penal contemporâneo e das inovações legislativas.

O método de abordagem utilizado será o dedutivo, partindo de princípios gerais do Direito Penal e da legislação vigente — em especial o artigo 171 do Código Penal e a Lei nº 14.155/2021 — para a análise dos casos concretos relacionados ao estelionato virtual. Essa escolha metodológica permite uma compreensão lógica e sistemática da matéria, possibilitando a identificação das limitações e potencialidades do sistema jurídico no enfrentamento desse tipo de crime.

Como procedimentos técnicos, a pesquisa adota a análise bibliográfica e documental, abrangendo doutrinas especializadas, legislações nacionais, artigos científicos, dissertações, teses e decisões judiciais recentes. De acordo com Lakatos e Marconi (2003, p. 183), a pesquisa bibliográfica “[...] é elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e atualmente de material disponibilizado na Internet”.

A coleta de dados será realizada por meio da consulta a bases de dados acadêmicas, como Google Scholar, Scielo e periódicos jurídicos nacionais e internacional, além de acervos da biblioteca online, jurisprudências disponíveis nos sites do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF). O material reunido servirá de base para identificar interpretações doutrinárias e tendências jurisprudências relacionadas à responsabilidade penal no estelionato online.

A análise dos dados ocorrerá de forma qualitativa, com o intuito de interpretar o conteúdo jurídico dos textos e julgados, buscando compreender os elementos objetivos e subjetivos da responsabilização penal e as dificuldades práticas de persecução criminal no ambiente digital. Essa abordagem possibilita não apenas descrever a realidade, mas também refletir criticamente sobre ela, identificando possíveis lacunas normativas e desafios aplicáveis ao contexto brasileiro.

Portanto, a metodologia adotada neste estudo busca integrar fundamentos teóricos e práticos, oferecendo uma visão abrangente sobre a temática e contribuindo para o debate acadêmico acerca da efetividade da legislação penal frente aos crimes virtuais.

3. O ESTELIONATO NO AMBIENTE DIGITAL: DIFICULDADES PROBATÓRIAS E EFETIVIDADE DA LEI PENAL

O avanço tecnológico e a expansão da internet transformaram significativamente as formas de interação humana, proporcionando inúmeros benefícios à sociedade contemporânea. Contudo, tais avanços também criaram novas possibilidades para a prática de crimes, especialmente no ambiente virtual, marcado pela instantaneidade, amplitude de alcance e, sobretudo, pelo anonimato. Nesse contexto, o estelionato online emerge como uma das principais condutas ilícitas,

apresentando características próprias que desafiam a aplicação do direito penal tradicional e a efetiva responsabilização dos agentes.

Embora o estelionato digital guarde semelhanças com o delito previsto no artigo 171 do Código Penal, suas particularidades demandam uma releitura dos mecanismos jurídicos existentes. Conforme leciona Capez (2021, p. 214), “[...] os crimes informáticos representam uma nova categoria de condutas delituosas que exigem do direito penal uma constante atualização interpretativa e normativa”. Tal entendimento evidencia a necessidade de adaptação do ordenamento jurídico frente às novas formas de fraude, especialmente aquelas praticadas por meio eletrônico.

Nesse cenário, observa-se que o avanço tecnológico tem possibilitado aos agentes criminosos a utilização de mecanismos sofisticados para ocultação de identidade e manipulação de sistemas, dificultando significativamente a identificação da autoria e a produção de provas. Segundo Nucci (2022, p. 89), “[...] o ambiente virtual cria obstáculos relevantes à persecução penal, pois as provas digitais são voláteis e demandam conhecimentos técnicos especializados”. Assim, evidencia-se um descompasso entre a evolução tecnológica e a capacidade do sistema jurídico de acompanhar tais mudanças.

Apesar dos esforços legislativos no enfrentamento dessa realidade, destaca-se a promulgação da Lei nº 14.155/2021, que alterou o artigo 171 do Código Penal, agravando as penas nos casos de estelionato praticado por meio eletrônico. Tal medida buscou conferir maior proteção às vítimas e maior rigor na punição dos infratores. No entanto, como observa Greco (2021, p. 305), “[...] a simples ampliação da pena não garante a efetividade da norma penal, sobretudo quando a aplicação da lei enfrenta entraves de natureza técnica e probatória”. Dessa forma, percebe-se que o enfrentamento do estelionato online exige não apenas mudanças legislativas, mas também o aprimoramento das instituições responsáveis pela investigação e julgamento.

Outro aspecto relevante diz respeito à dificuldade de cooperação entre órgãos nacionais e internacionais. Os crimes virtuais frequentemente ultrapassam fronteiras territoriais, o que torna a persecução penal ainda mais complexa. Nesse sentido, Silva (2020, p. 132) destaca que “[...] a globalização das redes digitais demanda uma nova postura estatal, capaz de integrar esforços investigativos e jurídicos em âmbito transnacional”. Tal realidade desafia os limites tradicionais da jurisdição penal e impõe a necessidade de mecanismos mais eficazes de cooperação internacional.

Ademais, deve-se considerar a vulnerabilidade das vítimas, frequentemente induzidas ao erro por meio de práticas como falsas ofertas, clonagem de perfis e esquemas de engenharia social. Conforme Bitencourt (2020, p. 417), o estelionato configura-se como “[...] um delito de astúcia, em que o agente se vale do engano para obter vantagem ilícita, causando prejuízo a outrem”. No ambiente virtual, esse engano é potencializado pela facilidade de criação de identidades falsas e pela dificuldade de rastreamento das transações, o que agrava os desafios probatórios e compromete a efetividade da persecução penal.

4. RESPONSABILIDADE PENAL NO ESTELIONATO ONLINE E OS DESAFIOS DO DIREITO PENAL CONTEMPORÂNEO

A transferência das relações interpessoais para o ambiente digital reconfigurou o *modus operandi* das fraudes e dos crimes, exigindo do Direito Penal uma constante adaptação às novas formas de condutas imateriais e sofisticadas. No caso do estelionato online, a responsabilização dos agentes torna-se ainda mais desafiadora, especialmente diante da necessidade de conciliar o tipo penal previsto no Artigo 171 do Código Penal com as novas modalidades delitivas que surgem ao longo do tempo.

Além disso, fatores como o anonimato dos agentes, a transnacionalidade das condutas e a rapidez com que os prejuízos são causados, muitas vezes em questão de segundos, intensificam as dificuldades da persecução penal. Nesse cenário, evidencia-se a necessidade de constante atualização do ordenamento jurídico, a fim de acompanhar as transformações tecnológicas e garantir a efetividade da tutela penal.

Dessa forma, o presente artigo tem como objetivo analisar como o ordenamento jurídico brasileiro vem enfrentando as novas modalidades de fraude no ambiente digital, bem como verificar se as atuais metodologias de imputação penal são suficientes para assegurar a eficácia da norma, sem violar princípios fundamentais do Direito Penal, como a legalidade e a intervenção mínima.

4.1 O BEM JURÍDICO TUTELADO DENTRO DO ESTELIONATO ONLINE

O bem jurídico tutelado desempenha um papel fundamental no entendimento da função do Direito Penal, pois através dele é possível identificar na sociedade

pontos centrais destinados à proteção jurídica. Dentro do crime de estelionato, tipificado no Código Penal em seu artigo 171, o bem jurídico tutelado é o Patrimônio com o seguinte texto “ 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” (BRASIL, 1940), Tal conteúdo da lei está voltado ao conjunto de bens e valores. Entretanto, o estelionato online com proteção penal ultrapassa os limites de proteção patrimonial e alcança também a confiança nas relações dentro do ambiente digital. Isso ocorre porque na contemporaneidade as fraudes virtuais, realizadas por meio das redes sociais, aplicativos de mensagens, plataformas de comércio eletrônico, sites falsos, entre tantas outras inovações que vem explorando a boa-fé das vítimas a fim de obterem vantagens ilícitas.

Assim, embora o bem jurídico tradicionalmente protegido seja o patrimônio, as transações digitais evidenciam a necessidade de tutela da confiança nas relações virtuais, elemento essencial para o funcionamento da economia contemporânea. Nesse sentido, a jurisprudência tem buscado adaptar a aplicação do Direito Penal às novas realidades tecnológicas. Em julgado do Superior Tribunal de Justiça, sob relatoria da Ministra Laurita Vaz, firmou-se o entendimento de que, nos crimes de estelionato praticados por meio eletrônico, a competência pode ser fixada no local em que ocorre o prejuízo da vítima (BRASIL, STJ, CC 168.522/PR, 2019).

A promulgação da Lei nº 14.155/2021 foi apresentada como resposta estatal ao aumento dos crimes cibernéticos. A norma promoveu alterações no Artigo 171 do Código Penal, ampliando a punição para o estelionato cometido por meio eletrônico e estabelecendo causas de aumento de pena, especialmente quando a vítima é idosa ou vulnerável, bem como quando o crime é praticado mediante utilização de servidor mantido fora do território nacional.

Contudo, surge um relevante questionamento no âmbito da dogmática penal: tais alterações representam uma resposta efetivamente capaz de combater o estelionato online ou configuram apenas uma manifestação simbólica do Direito Penal?

Embora a majoração das penas e a atualização da tipificação demonstrem a preocupação do legislador com a criminalidade digital, a efetividade da norma depende, sobretudo, da capacidade investigativa do Estado, da produção de provas digitais e da cooperação entre os órgãos de persecução penal.

Nesse sentido, a discussão não se limita à adequação normativa, mas envolve também a estrutura institucional necessária para garantir a aplicação prática da lei e a efetiva responsabilização dos autores dessas fraudes no ambiente virtual.

Ademais, políticas públicas voltadas à conscientização da população, com a divulgação de orientações sobre segurança digital, podem contribuir significativamente para a redução do número de vítimas, funcionando como importante mecanismo de prevenção.

4.2 DESAFIOS E PERSPECTIVAS À LUZ DA LEI 14.155/2021

Os golpes praticados no ambiente digital utilizam, em grande parte, técnicas de engenharia social, método pelo qual a vítima é induzida a fornecer informações pessoais, realizar transferências financeiras ou acessar links enganosos e potencialmente ilícitos. Esse tipo de prática evidencia a sofisticação das fraudes contemporâneas, que exploram a vulnerabilidade do usuário. Nesse sentido, destaca-se que os crimes informáticos representam uma nova forma de atuação delituosa, exigindo constante adaptação do Direito Penal, uma vez que “[...] os crimes informáticos desafiam o direito penal tradicional” (Capez, 2021, p. 214). Entre os crimes mais recorrentes, destacam-se o falso suporte bancário, empréstimos fraudulentos, falsas propostas de investimento, clonagem de aplicativos de mensagens e golpes que utilizam inteligência artificial para falsificar rostos e vozes, aumentando significativamente o grau de convencimento das vítimas.

O cibercrime refere-se a qualquer atividade criminosa que envolva computadores ou dispositivos conectados à rede, podendo ser classificado em duas categorias principais: aquelas em que o computador é o alvo, como nos ataques de hackers, e aquelas em que o computador é utilizado como ferramenta, como nas fraudes financeiras. No primeiro caso, o objetivo é comprometer a integridade, a disponibilidade e a confidencialidade dos dados; no segundo, o ambiente digital é utilizado para ampliar o alcance e a eficácia das práticas ilícitas. Conforme observa Nucci (2022, pag.89), os delitos praticados no ambiente digital apresentam maior complexidade investigativa, sobretudo em razão da volatilidade das provas eletrônicas.

Dessa forma, os crimes cibernéticos podem ser categorizados em diversas modalidades, dentre as quais se destacam: o hacking, caracterizado pelo acesso não

autorizado a sistemas; o phishing, que consiste no envio de mensagens fraudulentas que se passam por instituições confiáveis; o ransomware, definido como um software malicioso que criptografa os dados da vítima mediante exigência de pagamento; além da fraude e do roubo de identidade, que envolvem o uso indevido de informações pessoais. Também se incluem o cyberbullying e o assédio online, práticas que utilizam o ambiente virtual para intimidar, humilhar ou ameaçar indivíduos.

Diante do aumento expressivo desses crimes, a legislação brasileira passou por importantes alterações, especialmente com a promulgação da Lei nº 14.155/2021, que modificou o Código Penal Brasileiro, tornando mais rigorosa a punição para crimes cometidos por meios eletrônicos, como a invasão de dispositivos informáticos, o furto mediante fraude e o estelionato digital. Nesse contexto, destaca-se que o estelionato, previsto no Artigo 171 do Código Penal, é tradicionalmente compreendido como a obtenção de vantagem ilícita mediante fraude, sendo considerado, nas palavras de Bitencourt (2020, p. 417), “[...] o crime de fraude por excelência”. Ademais, o art. 154-A do Código Penal, conhecido como Lei Carolina Dieckmann, tipifica a invasão de dispositivos informáticos e estabelece sanções penais para essa conduta.

Mais recentemente, observa-se a ampliação da proteção jurídica no ambiente digital com a promulgação da Lei nº 15.211/2025, conhecida como Lei Felca, que estabelece regras e sanções aplicáveis às plataformas digitais, com foco na proteção de crianças e adolescentes no ambiente virtual.

O crime de estelionato apresenta diversas modalidades contemporâneas, sendo frequentes a criação de páginas falsas de comércio eletrônico, a clonagem de perfis em redes sociais, a fraude em aplicativos de mensagens e a utilização indevida de dados pessoais. Essas práticas demonstram a constante evolução da criminalidade digital. Conforme ressalta Greco (2021, pág 305), o Direito Penal deve acompanhar as transformações sociais e tecnológicas para manter sua eficácia.

Além disso, observa-se uma nova vertente relacionada à exploração econômica da imagem de menores por influenciadores digitais, envolvendo práticas de adultização, erotização infantil e exposição excessiva para geração de engajamento e lucro. Soma-se a isso o risco decorrente da ausência de controle parental adequado, o que permite que crianças e adolescentes tenham acesso a conteúdos impróprios ou se tornem alvos de abusadores.

4.3 RESPONSABILIDADE PENAL DE TERCEIROS

Tratando-se da responsabilização penal de terceiros, o legislador tem demonstrado preocupação com a matéria. A Lei nº 15.211/2025 Lei Felca adota mecanismos de responsabilização para aqueles que descumprirem suas disposições, evidenciando o esforço normativo de adaptação aos novos comportamentos da sociedade contemporânea.

A expansão das relações digitais e a intensificação das transações eletrônicas trouxeram novos desafios à definição da responsabilidade jurídica de terceiros envolvidos em ambientes virtuais, especialmente bancos, instituições financeiras, plataformas digitais e provedores de internet.

Nesse contexto, torna-se essencial distinguir os limites entre responsabilidade civil e responsabilidade penal, uma vez que os critérios de imputação jurídica diferem substancialmente em cada esfera. No âmbito civil, admite-se, em determinadas hipóteses, a responsabilização objetiva de instituições financeiras, fundamentada na teoria do risco da atividade e na proteção do consumidor.

Nos termos da jurisprudência consolidada do Superior Tribunal de Justiça, as instituições financeiras respondem objetivamente pelos danos causados por fraudes praticadas por terceiros no âmbito de operações bancárias, quando caracterizado o chamado fortuito interno, conforme entendimento firmado no Tema 466/STJ (Brasil, STJ, 2023) .

Nesse mesmo sentido, a Corte Superior tem decidido que a responsabilidade da instituição financeira está condicionada à verificação de falha na prestação do serviço. Em recente julgado, a Terceira Turma do Superior Tribunal de Justiça entendeu que não há responsabilidade do banco quando demonstrado o cumprimento dos deveres de verificação e segurança na abertura e manutenção de contas digitais (Brasil, STJ, REsp 2.124.423, 2025) .

Entretanto, a lógica da responsabilidade penal é distinta. No Direito Penal brasileiro, vigora o princípio da responsabilidade subjetiva, segundo o qual não há crime sem dolo ou culpa, conforme disposto no art. 18 do Código Penal Brasileiro. Desse modo, as instituições financeiras não podem ser responsabilizadas penalmente apenas pela ocorrência de fraude praticada por terceiros em seus sistemas, salvo quando demonstrada participação consciente, omissão penalmente relevante ou violação deliberada de dever jurídico específico.

Situação semelhante ocorre em relação às plataformas digitais. A responsabilização penal dessas entidades exige demonstração inequívoca de participação direta na prática criminosa ou colaboração dolosa, não sendo possível imputação automática.

No âmbito processual, a jurisprudência também tem enfrentado questões relevantes relacionadas ao estelionato digital. O Superior Tribunal de Justiça firmou entendimento de que, nos crimes de estelionato praticados por meio eletrônico, a competência territorial deve ser fixada no local onde ocorre a obtenção da vantagem ilícita, ou seja, onde o valor é creditado (Brasil, STJ, CC 168.522/PR, 2019) .

Tal entendimento reforça a necessidade de adaptação do Direito Penal às especificidades dos crimes digitais, especialmente diante da desterritorialização das condutas ilícitas.

5. DIMENSÃO INTERNACIONAL

A análise do estelionato online também exige a consideração de sua dimensão internacional, uma vez que os crimes praticados no ambiente digital frequentemente ultrapassam as fronteiras territoriais dos Estados. A internet possibilita que agentes localizados em diferentes países realizem fraudes contra vítimas situadas em outros territórios, o que dificulta a identificação dos autores, a coleta de provas e a aplicação da lei penal. Nesse sentido, observa-se que “[...] os delitos praticados no ciberespaço desafiam os mecanismos tradicionais de persecução penal, especialmente em razão de sua natureza transnacional” (Nucci, 2022, p. 89).

Nesse cenário, a cooperação jurídica internacional torna-se fundamental para a investigação e repressão desses delitos. Instrumentos internacionais, como a Convenção de Budapeste sobre o Cibercrime, estabelecem mecanismos de colaboração entre Estados para o combate aos crimes cibernéticos, incluindo o compartilhamento de informações e a harmonização das legislações penais. Conforme destaca Greco (2021, p. 213), “[...] a efetividade do Direito Penal, diante das novas formas de criminalidade, depende da integração entre os Estados e da modernização dos instrumentos investigativos”.

No âmbito internacional, a Corte Europeia de Direitos Humanos tem reconhecido a necessidade de adaptação dos Estados às novas formas de criminalidade digital, especialmente no que se refere à obtenção e preservação de

provas eletrônicas, destacando a importância do equilíbrio entre investigação criminal e proteção de direitos fundamentais (ECHR, 2015). De forma semelhante, a Corte de Justiça da União Europeia tem afirmado que a cooperação entre Estados-membros é essencial para garantir a efetividade da persecução penal em crimes transnacionais, sobretudo aqueles praticados por meio digital (CJEU, 2018).

Embora o Brasil tenha avançado na atualização normativa com a Lei nº 14.155/2021, os desafios impostos pela criminalidade digital demonstram que a efetividade do enfrentamento ao estelionato online depende não apenas de reformas legislativas internas, mas também do fortalecimento de mecanismos de cooperação internacional capazes de lidar com a natureza transnacional dessas condutas ilícitas. Nesse contexto, Capez (2021, p. 214) ressalta que “os crimes informáticos exigem constante atualização normativa e interpretativa, sob pena de ineficácia do sistema penal”.

6. CADEIA DE CUSTÓDIA DA PROVA DIGITAL

A cadeia de custódia, prevista nos arts. 158-A a 158-F do Código de Processo Penal, constitui mecanismo fundamental para assegurar a autenticidade, a integridade e a rastreabilidade dos vestígios coletados durante a persecução penal, garantindo, consequentemente, a confiabilidade da prova produzida. Tal matéria foi significativamente aprimorada pela Lei nº 13.964/2019, denominada Pacote Anticrime, que introduziu procedimentos técnicos destinados à preservação dos elementos probatórios desde a coleta até sua apresentação em juízo.

A cadeia de custódia relaciona-se diretamente com os princípios constitucionais do contraditório e da ampla defesa, previstos no art. 5º, inciso LV, da Constituição Federal de 1988. Nesse sentido, o Ministro Rogério Schietti Cruz, no julgamento do Habeas Corpus nº 598.051/SP, destacou que “a ausência de preservação da cadeia de custódia pode comprometer a validade da prova digital” (Brasil, STJ, HC 598.051/SP, 2021). Tal entendimento evidencia que a ausência de controle adequado sobre a origem, o armazenamento e o manuseio da prova digital pode gerar dúvida razoável acerca de sua integridade e autenticidade, comprometendo sua validade jurídica e exigindo maior rigor na produção probatória.

A matéria tem sido amplamente debatida no âmbito do Superior Tribunal de Justiça, especialmente diante do crescimento exponencial das provas digitais no

processo penal contemporâneo. Parte da jurisprudência sustenta que não se pode presumir a veracidade do conteúdo probatório quando inexistirem garantias técnicas mínimas de preservação da cadeia de custódia. Nesse contexto, o Ministro Ribeiro Dantas, no julgamento do Recurso em Habeas Corpus nº 133.430/PE, afirmou que “[...] mensagens de WhatsApp podem ser utilizadas como prova, desde que preservada sua autenticidade” (Brasil, STJ, RHC 133.430/PE, 2022). O entendimento reforça que imagens, diálogos e arquivos digitais extraídos de aplicativos de mensagens podem ser reconhecidos como meios probatórios válidos, desde que demonstrada a integridade do material e observados os requisitos legais de obtenção da prova.

A especificidade das provas digitais decorre de sua natureza imaterial, volátil e altamente suscetível à manipulação. Diferentemente das provas físicas tradicionais, os dados eletrônicos podem ser alterados, apagados ou inseridos sem deixar vestígios perceptíveis a olho nu, o que eleva o grau de exigência técnica na sua preservação. No contexto de dispositivos móveis, a situação torna-se ainda mais sensível, pois aparelhos conectados à rede permanecem aptos a receber atualizações automáticas, sincronização em nuvem e acessos remotos, circunstâncias que podem modificar o conteúdo armazenado caso não sejam adotadas medidas imediatas de isolamento digital, como o uso de bloqueadores de sinal ou a ativação do modo avião.

Importante destacar que, nas apreensões envolvendo tecnologia digital, o objeto material recolhido como, celulares, computadores ou mídias eletrônicas, não constitui propriamente a prova, mas apenas o suporte físico que contém os dados. A prova penal reside nas informações armazenadas em memória, cuja preservação depende da adoção de procedimentos técnicos especializados e da observância rigorosa da cadeia de custódia.

6.1 PERICIA FORENSE

A perícia forense digital assume papel central na validação da prova, inserindo-se no campo da computação forense, área técnico-científica responsável pela identificação, preservação, coleta, análise e apresentação de evidências digitais de forma juridicamente admissível. A atividade pericial possui rigorosos padrões de boas práticas, especialmente no que se refere à preservação da cadeia de custódia, assegurando a integridade e a confiabilidade dos vestígios eletrônicos.

Entre os procedimentos adotados, destaca-se a realização de cópia forense integral (*bit-by-bit forensic image*), técnica que replica fielmente todos os dados do dispositivo analisado, incluindo arquivos ocultos, metadados e fragmentos apagados, sem alteração do conteúdo original. Segundo a equipe da Legale Educacional (2024), a perícia digital exige “a realização de uma cópia bit-a-bit (imagem forense) do dispositivo, preservando o original intacto”. Tal método permite que a análise seja realizada sobre uma cópia tecnicamente idêntica, preservando-se o meio original contra qualquer modificação indevida.

A autenticidade dos dados é verificada por meio da geração e conferência de códigos hash, sequências alfanuméricas únicas que funcionam como verdadeira “impressão digital” dos arquivos, possibilitando a detecção de qualquer alteração posterior e garantindo a reprodutibilidade científica do exame pericial.

No âmbito da computação forense, também se inserem as técnicas de rastreabilidade de IP, utilizadas para reconstruir a origem lógica das conexões realizadas em ambiente digital. A análise de registros de acesso (*logs*), endereços IP, portas de comunicação, carimbos temporais (*timestamps*) e dados fornecidos por provedores de conexão e de aplicação permite reconstituir a dinâmica das atividades online investigadas. Embora o endereço IP, isoladamente, não identifique automaticamente o autor do fato, sua correlação com outros elementos probatórios possibilita a individualização da conduta e auxilia na atribuição de autoria em crimes praticados por meios informáticos.

Caso o laudo pericial identifique divergência entre os códigos hash ou indícios de manipulação dos dados, resta comprometida a confiabilidade do vestígio digital, configurando prova ilícita, nos termos do art. 157 do Código de Processo Penal. A adulteração rompe a autenticidade da prova e compromete a veracidade necessária à formação do convencimento judicial, inviabilizando a utilização do material probatório para fundamentar eventual condenação penal.

Ademais, deve-se observar a repercussão da ilicitude sobre as provas subsequentes, conforme a teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*), incorporada ao ordenamento jurídico brasileiro pelo §1º do art. 157 do Código de Processo Penal. Nesse sentido, Aury Lopes Jr. (2023, p. 712) afirma que “a preservação da cadeia de custódia constitui requisito essencial à validade da prova penal”, especialmente diante da crescente utilização de evidências digitais no processo penal contemporâneo.

Assim, reconhecida a ilicitude da prova originária, todas aquelas dela derivadas também poderão ser invalidadas, salvo quando demonstrada a existência de fonte independente ou a descoberta inevitável conforme artigo publicado.

A constatação de adulteração na prova digital atrai a aplicação do artigo 157 do Código de Processo Penal. Além da ilicitude da prova adulterada em si, deve-se analisar a contaminação das provas derivadas, conforme a teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*)." (Legale Educacional, 2025 p. <https://legale.com.br>).

Desse modo, se dados extraídos de dispositivo adulterado fundamentarem medidas judiciais, como decretação de prisão preventiva, expedição de mandado de busca e apreensão, rastreamento telemático baseado em registros de IP ou quebra de sigilo bancário, tais atos poderão ser declarados nulos em razão da contaminação probatória, em observância ao devido processo legal e às garantias constitucionais da ampla defesa e do contraditório.

6.2 INTELIGÊNCIA ARTIFICIAL E NOVAS FORMA DE FRAUDES

A utilização de *deepfakes*, técnica baseada em inteligência artificial capaz de criar ou manipular imagens, áudios e vídeos com elevado grau de realismo, tem se tornado relevante objeto de discussão no âmbito jurídico-penal. Essa tecnologia permite a simulação de falas, comportamentos e identidades inexistentes, sendo frequentemente empregada na prática de delitos como estelionato, extorsão, crimes contra a honra e fraudes financeiras, especialmente quando utilizada para induzir vítimas em erro mediante falsificação de identidade digital.

A responsabilização penal nessas hipóteses depende da demonstração do dolo do agente responsável pela produção, divulgação ou utilização do conteúdo manipulado, bem como da comprovação do nexo causal entre a fraude tecnológica e o prejuízo suportado pela vítima. A inteligência artificial, por si só, não pode ser considerada sujeito ativo do delito, permanecendo a imputação penal vinculada à conduta humana que a utiliza como instrumento para a prática criminosa. Nesse sentido, o Superior Tribunal de Justiça tem consolidado entendimento de que a responsabilização penal em crimes digitais exige demonstração concreta da autoria e da participação consciente do agente na prática delitiva (Brasil, STJ, RHC 133.430/PE, 2022).

Entretanto, o uso de inteligência artificial intensifica os desafios probatórios no processo penal contemporâneo. A elevada qualidade técnica das falsificações digitais dificulta a distinção entre conteúdos autênticos e manipulados, exigindo a atuação de perícia forense especializada, apta a examinar metadados, padrões algorítmicos e inconsistências técnicas muitas vezes imperceptíveis ao usuário comum. Além disso, a volatilidade das evidências digitais e a possibilidade de anonimização mediante utilização de redes privadas virtuais (VPNs), proxies e sistemas automatizados ampliam as dificuldades relacionadas à identificação da autoria delitiva.

A relevância da preservação da prova digital foi reconhecida pelo Superior Tribunal de Justiça no julgamento do Habeas Corpus nº 598.051/SP, de relatoria do Ministro Rogério Schietti Cruz, ao afirmar que “[...] a ausência de preservação da cadeia de custódia pode comprometer a validade da prova digital” (Brasil, STJ, HC 598.051/SP, 2021). Tal entendimento demonstra que a autenticidade e a integridade das evidências tecnológicas constituem requisitos essenciais à validade da persecução penal em crimes praticados no ambiente virtual.

Nesse contexto, ganha relevância a discussão acerca da autoria mediata por tecnologia. Tradicionalmente, a autoria mediata ocorre quando o agente utiliza outra pessoa como instrumento para a prática do crime. No ambiente digital, observa-se fenômeno semelhante, no qual sistemas automatizados, algoritmos e ferramentas de inteligência artificial são empregados como meios executórios da conduta criminosa. Embora a tecnologia não possua vontade própria juridicamente relevante, o indivíduo que programa, direciona ou conscientemente se beneficia da automação poderá ser responsabilizado penalmente, desde que demonstrado o domínio do fato e o controle funcional sobre o resultado produzido.

Outro aspecto relevante refere-se à automatização de golpes virtuais. Ferramentas automatizadas permitem a realização simultânea de milhares de tentativas fraudulentas, ampliando significativamente o alcance da atividade criminosa e reduzindo os custos operacionais para os agentes envolvidos. Nesse cenário, destacam-se os chamados *bots* de fraude, programas desenvolvidos para simular interações humanas, criar perfis falsos, enviar mensagens em massa e explorar vulnerabilidades em sistemas financeiros e plataformas digitais. A automação modifica a escala da criminalidade, mas não afasta a responsabilidade penal daquele que desenvolve, controla ou utiliza o sistema com finalidade ilícita.

De forma semelhante, o *phishing* automatizado utiliza algoritmos capazes de personalizar mensagens fraudulentas a partir de dados obtidos na internet, aumentando consideravelmente a eficácia das fraudes. Sistemas de inteligência artificial conseguem adaptar linguagem, contexto e aparência das comunicações, tornando-as mais convincentes e dificultando a identificação do golpe pelas vítimas. Sob a perspectiva jurídico-penal, tais práticas permanecem enquadradas nos tipos penais tradicionais, especialmente no Artigo 171 do Código Penal, ainda que executadas mediante tecnologias avançadas.

A jurisprudência brasileira também tem reconhecido a validade de elementos digitais como meio de prova, desde que preservada sua autenticidade. No julgamento do Recurso em Habeas Corpus nº 133.430/PE, o Ministro Ribeiro Dantas afirmou que “[...] mensagens de WhatsApp podem ser utilizadas como prova, desde que preservada sua autenticidade” (Brasil, STJ, RHC 133.430/PE, 2022). Tal entendimento reforça a necessidade de rigor técnico na obtenção e preservação das evidências digitais utilizadas em investigações envolvendo fraudes tecnológicas e manipulação por inteligência artificial.

Diante desse cenário, evidencia-se a necessidade de interpretação evolutiva do Direito Penal, capaz de aplicar institutos clássicos, como autoria, dolo e nexo causal, às novas dinâmicas tecnológicas, sem violação dos princípios fundamentais da legalidade e da culpabilidade. A inteligência artificial não inaugura uma categoria autônoma de responsabilidade penal, mas redefine os meios de execução do delito, exigindo maior rigor técnico na produção da prova e na análise da imputação subjetiva.

Assim, o emprego de inteligência artificial em práticas criminosas amplia os desafios investigativos e probatórios, especialmente em razão da utilização de *deepfakes*, da automatização de golpes e da atuação de *bots* fraudulentos. A responsabilização penal permanece centrada na conduta humana que controla e direciona a tecnologia, cabendo ao sistema jurídico desenvolver mecanismos técnicos e interpretativos capazes de assegurar a efetividade da persecução penal sem comprometer as garantias fundamentais do Estado Democrático de Direito.

7 INTERSEÇÃO COM OUTROS RAMOS DO DIREITO

A análise da responsabilidade penal no crime de estelionato online demonstra que a repressão às fraudes digitais não se limita exclusivamente ao âmbito do Direito

Penal, exigindo diálogo constante com outros ramos do ordenamento jurídico. A complexidade das relações estabelecidas no ambiente virtual evidencia a necessidade de atuação interdisciplinar, envolvendo normas de Direito Civil, Direito do Consumidor, Direito Digital, Direito Processual Penal e Direito Internacional, de modo a garantir maior efetividade na proteção das vítimas e na responsabilização dos agentes envolvidos.

7.1 DIREITO DO CONSUMIDOR

A temática relaciona-se diretamente com o Direito do Consumidor, sobretudo nas hipóteses em que fraudes ocorrem em plataformas digitais, instituições financeiras ou ambientes de comércio eletrônico. O Código de Defesa do Consumidor estabelece mecanismos de proteção ao consumidor diante da vulnerabilidade existente nas relações digitais, impondo deveres de segurança, informação e transparência aos fornecedores de serviços. A jurisprudência do Superior Tribunal de Justiça reconhece, inclusive, a responsabilidade objetiva das instituições financeiras por falhas na prestação de serviços relacionados a fraudes bancárias eletrônicas, especialmente quando demonstrada deficiência nos mecanismos de segurança.

A expansão do comércio eletrônico e a popularização dos pagamentos digitais transformaram significativamente as relações de consumo, ampliando o acesso a bens e serviços e modificando a dinâmica entre consumidores e fornecedores. Nesse contexto, o Código de Defesa do Consumidor estabelece, como um de seus princípios fundamentais, a vulnerabilidade do consumidor, reconhecendo-o como parte hipossuficiente na relação de consumo.

No ambiente digital, essa vulnerabilidade torna-se ainda mais evidente, uma vez que as transações são frequentemente intermediadas por plataformas tecnológicas que concentram grande volume de informações pessoais e financeiras. Tal cenário potencializa riscos relacionados a fraudes eletrônicas, vazamentos de dados e utilização indevida de informações sensíveis.

O Código de Defesa do Consumidor, promulgado em 1990, incorporou a noção de responsabilidade objetiva do fornecedor, fundamentada na teoria do risco do empreendimento e no dever de segurança. Dessa forma, independentemente da comprovação de culpa, o fornecedor responde pelos danos decorrentes de falhas na

prestação do serviço ou na segurança oferecida ao consumidor, conforme previsto no art. 14 do Código de Defesa do Consumidor.

A jurisprudência dos tribunais superiores brasileiros consolidou o entendimento de que fraudes digitais e falhas nos sistemas de proteção integram o risco inerente à atividade econômica desenvolvida pelo fornecedor. O Superior Tribunal de Justiça, ao editar a Súmula 479, firmou entendimento de que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias” (BRASIL, STJ, Súmula 479, 2012). Tal posicionamento reconhece que a segurança das operações eletrônicas integra o dever de qualidade e confiabilidade dos serviços prestados pelas instituições financeiras.

No mesmo sentido, o Superior Tribunal de Justiça entende que falhas nos mecanismos de autenticação, proteção de dados e monitoramento de operações suspeitas configuram defeito na prestação do serviço, ensejando o dever de indenizar. Em diversos julgados, a Corte reconheceu que fraudes eletrônicas praticadas mediante invasão de contas, clonagem de aplicativos ou transferências indevidas inserem-se no risco da atividade bancária, sobretudo quando demonstrada fragilidade dos sistemas de segurança disponibilizados aos consumidores.

Paralelamente, a doutrina e a jurisprudência vêm revisitando institutos clássicos, como nexo causal, fortuito interno e fortuito externo, buscando adequá-los às novas demandas impostas pela sociedade digital. Nessas hipóteses, discute-se se o evento fraudulento decorre de risco inerente à atividade econômica desenvolvida pelo fornecedor ou de fato totalmente estranho à prestação do serviço, circunstância capaz de afastar a responsabilidade civil.

Outro ponto sensível nas relações de consumo contemporâneas refere-se ao tratamento de dados pessoais. Em muitos casos, o consumidor é impedido de acessar determinados serviços ou adquirir produtos sem o fornecimento prévio de informações pessoais, o que amplia a exposição a práticas fraudulentas e reforça a necessidade de observância dos princípios de proteção de dados, segurança da informação e transparência informacional previstos na Lei Geral de Proteção de Dados Pessoais.

A proteção do consumidor no ambiente digital demonstra que o enfrentamento das fraudes eletrônicas exige atuação conjunta entre o Direito Penal, o Direito do Consumidor e o Direito Digital, especialmente diante da crescente sofisticação dos

golpes virtuais e da ampliação dos riscos decorrentes da circulação massiva de dados pessoais e financeiros em plataformas eletrônicas.

7.2 ANÁLISE DO DIREITO CIVIL E SUA RELAÇÃO COM O DIREITO PENAL NO CRIME DO ESTELIONATO ONLINE

O estelionato online, embora tradicionalmente analisado sob a perspectiva do Direito Penal, também produz relevantes repercussões no âmbito do Direito Civil, especialmente no que se refere à responsabilização civil e à reparação dos danos causados às vítimas. Dessa forma, evidencia-se necessária interação entre esses dois ramos do direito, que atuam de maneira complementar no enfrentamento das fraudes digitais.

No campo penal, o estelionato encontra previsão no Artigo 171 do Código Penal, sendo caracterizado pela obtenção de vantagem ilícita mediante fraude. Já na esfera civil, a prática do delito configura ato ilícito, nos termos dos arts. 186 e 927 do Código Civil, gerando ao agente o dever de reparar os prejuízos causados à vítima. Assim, enquanto o Direito Penal possui função repressiva e preventiva, buscando a punição do infrator, o Direito Civil volta-se à recomposição do dano, assegurando à vítima o direito à reparação integral.

No contexto do estelionato online, essa relação torna-se ainda mais relevante diante das dificuldades práticas enfrentadas pelas vítimas na recuperação dos valores subtraídos. Em muitos casos, além da responsabilização do autor direto da fraude, admite-se a responsabilização civil de terceiros, como instituições financeiras e plataformas digitais, especialmente quando verificada falha na prestação do serviço ou deficiência nos mecanismos de segurança disponibilizados aos usuários.

Nessas hipóteses, aplica-se o Código de Defesa do Consumidor, sobretudo em razão da responsabilidade objetiva dos fornecedores de serviços prevista no art. 14 da referida norma. A jurisprudência do Superior Tribunal de Justiça consolidou entendimento nesse sentido ao editar a Súmula 479, segundo a qual “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias” (BRASIL, STJ, Súmula 479, 2012).

Ademais, o Direito Civil contribui para a compreensão de institutos fundamentais presentes nas fraudes virtuais, como a violação da boa-fé objetiva e a

ocorrência de vícios de consentimento, especialmente o dolo, elemento essencial na configuração do estelionato. Tais institutos demonstram que, embora o crime seja tipificado na esfera penal, suas consequências jurídicas ultrapassam esse campo, alcançando a validade dos negócios jurídicos e as relações obrigacionais estabelecidas no ambiente digital.

Outro aspecto relevante refere-se à possibilidade de cumulação das esferas penal e civil. A responsabilização criminal do agente não exclui a obrigação de indenizar, sendo plenamente possível que a vítima busque, simultaneamente, a condenação penal do infrator e a reparação dos danos sofridos na esfera cível. Nesse sentido, o Código Civil admite a coexistência entre responsabilidade penal e civil, reforçando a proteção jurídica da vítima e ampliando os mecanismos de tutela diante das fraudes eletrônicas.

Além disso, a jurisprudência brasileira reconhece que a reparação civil decorrente de fraude eletrônica independe do resultado da persecução penal, especialmente quando demonstrado o prejuízo patrimonial e o nexo causal entre a conduta ilícita e o dano suportado pela vítima. Tal entendimento reforça a autonomia relativa entre as instâncias civil e penal, permitindo respostas jurídicas mais efetivas diante da crescente complexidade das fraudes digitais.

Diante disso, verifica-se que o enfrentamento do estelionato online demanda atuação integrada entre o Direito Penal e o Direito Civil. Enquanto o primeiro exerce função repressiva e preventiva, o segundo assegura a efetividade da tutela dos direitos da vítima por meio da reparação dos danos. Assim, a conjugação desses dois ramos do direito revela-se essencial para uma resposta mais eficaz às novas formas de criminalidade desenvolvidas no ambiente digital.

7.3 ANÁLISE DO ESTELIONATO ONLINE SOB O DIREITO BANCÁRIO

A ampliação do acesso à internet em diversos setores da sociedade, especialmente no âmbito das instituições financeiras, proporcionou maior facilidade na abertura de contas e na realização de operações bancárias por meios digitais. Embora esse avanço tecnológico traga benefícios relacionados à praticidade, agilidade e inclusão financeira, também amplia as oportunidades para a atuação de estelionatários, que se utilizam dessas ferramentas para a prática de fraudes eletrônicas. Conforme observa Damásio de Jesus (2015, p.97), “[...] a criminalidade

informática desafia os mecanismos tradicionais de investigação e exige constante atualização legislativa e tecnológica por parte do Estado”.

Nesse contexto, mecanismos de transferência instantânea, como o Pix, bem como boletos bancários e plataformas digitais de pagamento, passaram a ser frequentemente utilizados na execução de golpes virtuais, além de constituírem relevantes elementos probatórios na investigação e persecução penal desses delitos. Segundo Patrícia Peck Pinheiro (2021, p. 63), “[...] os delitos virtuais apresentam elevada complexidade probatória em razão da volatilidade dos dados digitais e da facilidade de ocultação da autoria”.

Com o objetivo de regulamentar esse cenário, o Banco Central do Brasil editou a Resolução nº 4.753/2019, que estabelece critérios a serem observados pelas instituições financeiras em todas as fases relacionadas às contas de depósito no ambiente digital. Diferentemente da Resolução nº 2.025/1993, que previa de forma mais detalhada os documentos, informações e procedimentos necessários para abertura de contas bancárias, a norma mais recente adotou modelo regulatório mais flexível, transferindo às instituições financeiras maior responsabilidade quanto à definição dos mecanismos de identificação, qualificação e validação da identidade dos titulares.

A flexibilização dos procedimentos de abertura de contas digitais, embora compatível com a modernização do sistema financeiro, intensificou discussões acerca da responsabilidade civil das instituições financeiras diante de fraudes praticadas por terceiros. Nesse sentido, o Superior Tribunal de Justiça consolidou entendimento por meio da Súmula 479, segundo a qual “[...] as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias” (Brasil, STJ, Súmula 479, 2012).

Assim, comprovada falha nos mecanismos de segurança ou deficiência na prestação do serviço, as instituições financeiras poderão responder pelos prejuízos causados aos correntistas em decorrência de fraudes eletrônicas, especialmente diante do dever de proteção e segurança inerente à atividade bancária (TJDFT, 2023).

Todavia, a responsabilização das instituições bancárias não ocorre de maneira automática. O Superior Tribunal de Justiça, em julgamento relatado pela Ministra

Nancy Andrichi no Recurso Especial nº 1.978.901/SP, firmou entendimento de que “[...] a responsabilidade da instituição financeira em fraudes digitais depende da comprovação de falha na prestação do serviço” (Brasil, STJ, REsp 1.978.901/SP, 2022). Dessa forma, quando demonstrado que a instituição adotou mecanismos adequados de segurança e observou as regulamentações expedidas pelo Banco Central, poderá ser afastada a configuração de defeito na prestação do serviço bancário.

No âmbito penal, a utilização de contas digitais fraudulentas e mecanismos eletrônicos de transferência financeira também levanta discussões relacionadas à produção da prova digital e à preservação da cadeia de custódia. O Superior Tribunal de Justiça, no julgamento do Habeas Corpus nº 598.051/SP, de relatoria do Ministro Rogério Schietti Cruz, reconheceu que “[...] a ausência de preservação da cadeia de custódia pode comprometer a validade da prova digital” (Brasil, STJ, HC 598.051/SP, 2021). Tal entendimento demonstra a necessidade de rigor técnico na coleta, armazenamento e análise de vestígios eletrônicos relacionados às fraudes bancárias digitais.

Além disso, a utilização de aplicativos de mensagens e plataformas digitais como instrumentos para aplicação de golpes virtuais tornou frequente a utilização de conversas eletrônicas como meio de prova no processo penal. Sobre o tema, o Superior Tribunal de Justiça, no julgamento do Recurso em Habeas Corpus nº 133.430/PE, de relatoria do Ministro Ribeiro Dantas, firmou entendimento de que “[...] mensagens de WhatsApp podem ser utilizadas como prova, desde que preservada sua autenticidade” (BRASIL, STJ, RHC 133.430/PE, 2022).

Ademais, observa-se significativo aumento das atividades bancárias realizadas em ambiente virtual, impulsionando consumidores a utilizarem, de maneira cada vez mais frequente, serviços financeiros digitais. Essa transformação aponta para uma experiência mais eficiente, personalizada e acessível aos usuários. Contudo, paralelamente aos avanços tecnológicos, torna-se indispensável o fortalecimento dos mecanismos de segurança, autenticação e monitoramento das operações financeiras, de modo a reduzir riscos, prevenir fraudes eletrônicas e assegurar a confiança dos usuários no sistema financeiro digital.

Nesse sentido, César Roberto Bitencourt (2022, p. 418) afirma que “[...] a internet potencializou a prática de delitos patrimoniais, permitindo que o agente alcance inúmeras vítimas simultaneamente e com reduzido risco de identificação”.

Assim, o enfrentamento do estelionato online exige constante atualização legislativa, aperfeiçoamento dos mecanismos de segurança digital e integração entre instituições financeiras, órgãos de investigação e Poder Judiciário, a fim de garantir maior efetividade na proteção dos usuários e na repressão às fraudes eletrônicas.

8. POLÍTICAS PÚBLICAS E PREVENÇÃO

O enfrentamento do estelionato online não pode limitar-se apenas à atuação repressiva do Direito Penal, sendo necessária a implementação de políticas públicas eficazes voltadas à prevenção, à educação digital e ao fortalecimento institucional. É imprescindível uma abordagem integrada que envolva educação digital, atuação estatal qualificada e cooperação entre os diversos setores da sociedade. Nesse sentido, o Superior Tribunal de Justiça tem reconhecido a necessidade de aprimoramento dos mecanismos de proteção no ambiente digital, especialmente diante do crescimento das fraudes eletrônicas. Conforme entendimento consolidado no Recurso Especial n. 1.978.901/SP, de relatoria da Ministra Nancy Andrighi, “a responsabilidade da instituição financeira em fraudes digitais depende da demonstração de falha na prestação do serviço”, evidenciando a importância da adoção de mecanismos preventivos e sistemas eficazes de segurança pelas instituições financeiras.

A educação digital configura-se como elemento fundamental na prevenção dos crimes cibernéticos, considerando que grande parte dessas infrações explora a vulnerabilidade informacional das vítimas. Assim, torna-se essencial promover campanhas educativas e incentivar a inclusão da educação digital nas instituições de ensino, a fim de orientar a população acerca dos riscos existentes no ambiente virtual, da identificação de golpes e das boas práticas de segurança digital, reduzindo-se, conseqüentemente, a incidência dessas fraudes.

A atuação estatal também desempenha papel central no combate à criminalidade digital. Faz-se necessário o investimento em infraestrutura tecnológica, capacitação de agentes públicos e modernização dos órgãos de investigação e persecução penal. A complexidade dos crimes cibernéticos exige conhecimentos técnicos especializados, demandando formação contínua de policiais, peritos e membros do Ministério Público, bem como a utilização de ferramentas compatíveis com a realidade tecnológica contemporânea.

A criação e o fortalecimento de delegacias especializadas em crimes cibernéticos mostram-se medidas indispensáveis. Tais unidades possuem expertise técnica para lidar com provas digitais, rastreamento de atividades ilícitas e análise de dados complexos, aumentando a eficiência investigativa e a taxa de resolução dos crimes. Além disso, contribuem para a padronização dos procedimentos investigativos e para a adequada preservação da cadeia de custódia da prova digital.

As parcerias público-privadas, especialmente entre o Estado, instituições financeiras e plataformas digitais, revelam-se fundamentais para o enfrentamento das fraudes eletrônicas. A cooperação entre esses atores possibilita maior agilidade na identificação de fraudes, no bloqueio de valores desviados e no compartilhamento de informações relevantes às investigações. Nesse contexto, a integração entre bancos, forças policiais e plataformas tecnológicas torna-se essencial, uma vez que tais entidades concentram dados estratégicos relativos a transações financeiras, registros de acesso e comportamentos suspeitos.

Ademais, iniciativas conjuntas podem viabilizar a criação de protocolos de resposta rápida a fraudes, sistemas de alerta aos usuários e mecanismos automatizados de detecção de atividades ilícitas, reduzindo o impacto dos golpes e ampliando a proteção das vítimas. Tal atuação integrada reforça a compreensão de que a segurança digital constitui responsabilidade compartilhada, transcendendo a atuação isolada do Estado.

Dessa forma, verifica-se que o combate ao estelionato online exige a conjugação de medidas preventivas, educativas e institucionais capazes de acompanhar a evolução tecnológica e reduzir a vulnerabilidade dos usuários. A efetividade dessas políticas públicas depende não apenas da atuação estatal, mas também da cooperação entre diferentes setores da sociedade, consolidando um modelo de governança digital mais seguro, eficiente e compatível com os desafios contemporâneos.

Diante desse cenário, o enfrentamento da criminalidade digital exige maior cautela por parte dos usuários da internet, bem como o desenvolvimento de estratégias permanentes de prevenção e conscientização. A adoção de comportamentos seguros no ambiente digital torna-se fundamental para reduzir riscos e evitar prejuízos financeiros e pessoais.

CONCLUSÃO

A presente pesquisa analisou a responsabilidade penal no crime de estelionato online diante da expansão da criminalidade digital e das transformações provocadas pelas novas tecnologias nas relações sociais e econômicas. A partir do estudo desenvolvido, verificou-se que o avanço da internet, das plataformas digitais e dos mecanismos de inteligência artificial modificou significativamente as formas de execução das fraudes, ampliando a complexidade investigativa e os desafios enfrentados pelo Direito Penal contemporâneo.

O problema central da pesquisa consistiu em verificar se a Lei nº 14.155/2021 representa uma resposta efetiva ou meramente simbólica ao crescimento do estelionato praticado em ambiente virtual. Ao final da análise, conclui-se que a legislação representou importante avanço normativo ao atualizar o Código Penal e reconhecer expressamente as fraudes praticadas por meios eletrônicos, ampliando a proteção jurídica diante das novas modalidades criminosas. Contudo, constatou-se que a simples alteração legislativa e a majoração das penas não são suficientes, por si sós, para assegurar a efetividade do combate ao estelionato online.

Nesse sentido, a hipótese inicialmente apresentada foi parcialmente confirmada. Embora a Lei nº 14.155/2021 tenha contribuído para o fortalecimento da tutela penal e para a adequação normativa do ordenamento jurídico brasileiro à realidade digital, observou-se que sua eficácia prática permanece limitada diante das dificuldades estruturais relacionadas à investigação, à identificação dos autores, à produção de provas digitais e à cooperação internacional. Assim, verificou-se que a resposta estatal ainda apresenta traços de simbolismo penal quando desacompanhada de investimentos em tecnologia, capacitação institucional e políticas públicas preventivas.

Os objetivos propostos foram alcançados na medida em que a pesquisa possibilitou compreender a evolução do estelionato online, suas principais modalidades e os impactos provocados pela tecnologia na dinâmica criminosa contemporânea. Também foi possível analisar os pressupostos da responsabilidade penal no ambiente digital, os desafios relacionados à cadeia de custódia e à prova digital, bem como a relevância da computação forense na validação das evidências eletrônicas. Além disso, o estudo demonstrou a necessidade de interpretação evolutiva dos institutos penais clássicos frente às novas tecnologias, especialmente diante do uso de inteligência artificial, deepfakes e automação de golpes.

A pesquisa evidenciou ainda que o enfrentamento do estelionato online exige atuação integrada entre diferentes ramos do Direito, especialmente o Direito Penal, o Direito Civil, o Direito do Consumidor e a proteção de dados pessoais. Observou-se que a responsabilização jurídica não pode restringir-se apenas à punição criminal, sendo igualmente necessária a reparação dos danos causados às vítimas e a implementação de mecanismos preventivos voltados à segurança digital.

Por fim, conclui-se que o combate à criminalidade cibernética demanda não apenas atualização legislativa, mas também fortalecimento das instituições públicas, cooperação internacional, desenvolvimento tecnológico e educação digital da população. O estelionato online constitui fenômeno complexo e dinâmico, cuja repressão eficaz depende da conjugação entre norma jurídica, estrutura investigativa adequada e conscientização social, de modo a garantir a efetividade da tutela penal sem violação aos princípios fundamentais do Estado Democrático de Direito.

REFERÊNCIAS

ALMG – ASSEMBLEIA LEGISLATIVA DE MINAS GERAIS. Tecnologias aumentam a vulnerabilidade de consumidores. Belo Horizonte, 2026. Disponível em: ALMG. Acesso em: 14 mar. 2026.

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte especial – dos crimes contra o patrimônio*. 22. ed. São Paulo: Saraiva Educação, 2021.

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte especial*. 28. ed. São Paulo: Saraiva Educação, 2022.

BRASIL. Banco Central do Brasil. Resolução nº 2.025, de 24 de novembro de 1993. Dispõe sobre abertura, manutenção e movimentação de contas de depósitos. Brasília, DF: Banco Central do Brasil, 1993.

BRASIL. Banco Central do Brasil. Resolução nº 4.753, de 26 de setembro de 2019. Dispõe sobre a abertura, manutenção e o encerramento de contas de depósitos. Brasília, DF: Banco Central do Brasil, 2019. Disponível em: Banco Central do Brasil. Acesso em: 14 abr. 2026.

BRASIL. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, 11 jan. 2002.

BRASIL. Código de Defesa do Consumidor. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: seção 1, Brasília, DF, 12 set. 1990.

BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. *Diário Oficial da União*: seção 1, Rio de Janeiro, RJ, 31 dez. 1940.

BRASIL. Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência n. 168.522/PR. Relatora: Ministra Laurita Vaz. Brasília, DF: STJ, 2019.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus n. 598.051/SP. Relator: Ministro Rogério Schietti Cruz. Brasília, DF: STJ, 2021.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus n. 133.430/PE. Relator: Ministro Ribeiro Dantas. Brasília, DF: STJ, 2022.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.978.901/SP. Relatora: Ministra Nancy Andrighi. Brasília, DF: STJ, 2022.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 2.124.423. Relatora: Ministra Nancy Andrighi. Brasília, DF: STJ, 2025.

BRASIL. Superior Tribunal de Justiça. Súmula n. 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: STJ, 2012.

BRASIL. Superior Tribunal de Justiça. Tema Repetitivo 466. Responsabilidade civil de instituições financeiras por fraudes. Brasília, DF: STJ, 2023.

BRASIL. Superior Tribunal de Justiça. Responsabilidade de banco por golpe com uso de conta digital exige demonstração de falta de diligência. Brasília, DF, 2025. Disponível em: Superior Tribunal de Justiça. Acesso em: 18 mar. 2026.

BOLSA, Quero. O que é a Lei Felca? 2026. Disponível em: Quero Bolsa. Acesso em: 20 mar. 2026.

CAPEZ, Fernando. *Curso de direito penal: parte especial*. 23. ed. São Paulo: Saraiva Educação, 2021.

COURT OF JUSTICE OF THE EUROPEAN UNION. Case C-210/16. Luxembourg: CJEU, 2018.

EUROPEAN COURT OF HUMAN RIGHTS. Case of Barbulescu v. Romania. Strasbourg: ECHR, 2015.

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 4. ed. São Paulo: Atlas, 1994.

GOMES, Luiz Flávio; CERVINI, Raúl. *Crimes de informática: o direito penal e a internet*. São Paulo: Revista dos Tribunais, 2019.

GOMES, Victor. Cadeia de custódia: garantia da prova digital no processo penal. Blog Legale, 2026. Disponível em: Legale Educacional. Acesso em: 1 abr. 2026.

GRECO, Rogério. *Código Penal comentado*. 14. ed. Rio de Janeiro: Impetus, 2021.

JESUS, Damásio de. *Crimes de informática*. São Paulo: Saraiva, 2015.

LEGALE EDUCACIONAL. Artigos sobre cadeia de custódia digital. 2024-2025. Disponível em: Legale Educacional. Acesso em: 4 abr. 2026.

LEGALE. Plataformas digitais e fraude: responsabilidade pelo CDC. Blog Legale, 2026. Disponível em: Legale Educacional. Acesso em: 4 abr. 2026.

LOPES JR., Aury. *Direito processual penal*. 20. ed. São Paulo: Saraiva Educação, 2023.

MIGALHAS. Cadeia de custódia e prova digital: o garantismo no processo penal. 2026. Disponível em: Migalhas. Acesso em: 4 abr. 2026.

MIGALHAS. Responsabilidade civil em fraudes digitais. 2026. Disponível em: Migalhas. Acesso em: 4 abr. 2026.

NUCCI, Guilherme de Souza. *Código de Processo Penal comentado*. 21. ed. Rio de Janeiro: Forense, 2022.

NUCCI, Guilherme de Souza. *Crimes informáticos: doutrina, jurisprudência e prática*. 2. ed. São Paulo: Forense, 2022.

PINHEIRO, Patrícia Peck. *Direito digital*. 7. ed. São Paulo: Saraiva Educação, 2021.

PRADO, Luiz Regis. *Curso de direito penal brasileiro: parte geral*. 18. ed. São Paulo: Revista dos Tribunais, 2022.

SILVA, José Afonso da. *Direito e tecnologia: desafios contemporâneos do Estado e da sociedade digital*. São Paulo: Revista dos Tribunais, 2020.

TJDFT – TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Responsabilidade civil das instituições financeiras nas fraudes eletrônicas. Brasília, DF, 2023. Disponível em: TJDFT. Acesso em: 18 mar. 2026.

