CENTRO UNIVERSITÁRIO DE IPORÁ (UNIPORÁ)
CURSO DE DIREITO

JOÃO NETO FERNANDES COSTA

MATHEUS ALVES DA COSTA SILVA

ESTELIONATO DIGITAL: DESAFIOS E ESTRATÉGIAS DE COMBATE NO SÉCULO XXI

IPORÁ, GO
2025

JOÃO NETO FERNANDES COSTA

MATHEUS ALVES DA COSTA SILVA

ESTELIONATO DIGITAL: DESAFIOS E ESTRATÉGIAS DE COMBATE NO SÉCULO XXI

Artigo Científico apresentado ao curso de Direito Centro Universitário de Iporá (UNIPORÁ) como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Ms. Helmer Marra

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
HELMER MARRA RODRIGUES
Data: 23/12/2025 19:41:13-0300
Verifique em https://validar.iti.gov.br

Ms. Helmer Marra
Presidente da Banca e Orientador

Documento assinado digitalmente
gov.br
ALEXANDRE FERREIRA DE MOURA
Data: 29/12/2025 15:29:48-0300
Verifique em https://validar.iti.gov.br

Esp. Alexandre Ferreira de Moura
Avaliador 1

Documento assinado digitalmente
gov.br
BEATRIZ SOUZA MARTINS
Data: 05/01/2026 19:01:25-0300
Verifique em https://validar.iti.gov.br

Esp. Beatriz Souza Martins
Avaliador 2

IPORÁ, GO
2025

ESTELIONATO DIGITAL: DESAFIOS E ESTRATÉGIAS DE COMBATE NO SÉCULO XXI

DIGITAL FRAUD: CHALLENGES AND COMBAT STRATEGIES IN THE 21ST CENTURY

João Neto Fernandes Costa[1]

Matheus Alves da Costa Silva[2]

Helmer Marra[3]

RESUMO

O estelionato digital representa um dos principais desafios da sociedade contemporânea, impulsionado pela transformação tecnológica e pela popularização da internet. Dado o crescimento acelerado dos crimes digitais, como *phishing*, clonagem de contas, fraudes bancárias e golpes em redes sociais, evidencia-se a necessidade de compreender e combater esse fenômeno, que afeta milhões de brasileiros e causa prejuízos significativos ao patrimônio e à privacidade. O artigo analisa criticamente os principais desafios enfrentados, como a sofisticação das técnicas criminosas, o anonimato no ambiente virtual e a dificuldade de identificação dos autores. Destaca-se o desenvolvimento legislativo, com a atualização do Código Penal e a criação de leis específicas, como a Lei 14.155/2021, a LGPD e o Marco Civil da Internet, embora persistam lacunas na responsabilização de plataformas digitais e instituições financeiras, especialmente quando operam fora do país. A investigação dos crimes digitais é dificultada pela dependência de representação da vítima, morosidade processual e baixa capacitação técnica das autoridades. O estudo propõe soluções inovadoras, como o fortalecimento da educação digital, aprimoramento dos mecanismos de investigação, adoção de tecnologias avançadas de prevenção e promoção de uma cultura de segurança entre usuários e empresas. Ressalta-se a importância da cooperação internacional e da atualização constante das normas jurídicas para enfrentar um fenômeno dinâmico e transnacional. O artigo delimita seu escopo ao contexto brasileiro, com ênfase em golpes praticados por meio de redes sociais, aplicativos de mensagens e fraudes bancárias, utilizando revisão de literatura, análise de dados estatísticos, legislação vigente e casos práticos.

Palavras-chave: Crimes virtuais; Estelionato digital; Fraudes bancárias; *Phishing*.

[1] Graduando em Direito pelo Centro Universitário de Iporá (UNIPORÁ), GO. E-mail: joaonetoferjoao@gmail.com.

[2] Graduando em Direito pelo Centro Universitário de Iporá (UNIPORÁ), GO. E-mail: matheusalvesdacs2002@gmail.com.

[3] Orientador, Docente (2025-Atual) e Coordenador-adjunto (2025-Atual) no curso de Direito do Centro Universitário de Iporá (UNIPORÁ). Mestre em Ciência Política e Relações Internacionais (Concentração: Política Internacional) pela Universidade Federal da Paraíba (UFPB). Pesquisador associado ao Grupo de Pesquisa em Mídia e Cultura Asiática Contemporânea (MidiÁsia) da Universidade Federal Fluminense (UFF). E-mail: helmer.marra@gmail.com.

ABSTRACT

Digital fraud represents one of the main challenges of contemporary society, driven by technological transformation and the popularization of the internet. The accelerated growth of digital crimes, such as phishing, account cloning, bank fraud, and social media scams, highlights the need to understand and combat this phenomenon, which affects millions of Brazilians and causes significant damage to property and privacy. This article critically analyses the main challenges faced, such as the sophistication of criminal techniques, anonymity in the virtual environment, and the difficulty in identifying perpetrators. It highlights legislative evolution, with the updating of the Penal Code and the creation of specific laws, such as Law 14.155/2021, the LGPD (Brazilian General Data Protection Law), and the Marco Civil da Internet (Brazilian Internet Bill of Rights). Although, gaps persist in the accountability of digital platforms and financial institutions, especially when operating outside the country. The investigation of digital crimes is hampered by the dependence on victim representation, procedural delays, and the low technical capacity of the authorities. This study proposes innovative solutions, such as strengthening digital education, improving investigation mechanisms, adopting advanced prevention technologies, and promoting a culture of security among users and companies. It emphasizes the importance of international cooperation and the constant updating of legal norms to address this dynamic and transnational phenomenon. The article limits its scope to the Brazilian context, focusing on scams perpetrated through social networks, messaging applications, and bank fraud, using literature review, statistical data analysis, current legislation, and practical cases.

Keywords: Bank fraud; Cybercrimes;. Digital fraud; Phishing.

1. INTRODUÇÃO

O estelionato digital tornou-se um dos principais desafios da sociedade contemporânea, refletindo a crescente relevância dos crimes virtuais no contexto da transformação tecnológica e da popularização da internet. O aumento expressivo das fraudes digitais evidencia a necessidade de compreender e combater esse fenômeno, que afeta milhões de pessoas e causa prejuízos significativos ao patrimônio e à privacidade dos cidadãos brasileiros.

Nas últimas décadas, observou-se um crescimento acelerado dos crimes digitais, impulsionado pela facilidade de acesso à tecnologia, pelo anonimato proporcionado pelo ambiente virtual e pela sofisticação das técnicas utilizadas pelos criminosos. Golpes como *phishing*, clonagem de contas, fraudes bancárias e ataques em redes sociais tornaram-se cada vez mais frequentes e complexos, exigindo respostas rápidas e eficazes por parte das autoridades, empresas e usuários.

O objetivo deste artigo é analisar criticamente o fenômeno do estelionato digital, discutindo seus principais desafios, lacunas legislativas e institucionais, bem

como propor soluções inovadoras para a prevenção e o combate a esse tipo de crime. Busca-se ainda, compreender o impacto das novas tecnologias e a importância da educação digital na construção de um ambiente virtual mais seguro.

O escopo do estudo está delimitado ao contexto brasileiro, com ênfase em golpes praticados por meio de redes sociais, aplicativos de mensagens e fraudes bancárias, considerando tanto o panorama nacional quanto exemplos emblemáticos que ilustram a complexidade do tema.

A metodologia utilizada envolve a revisão de literatura especializada, análise de dados estatísticos recentes, legislação vigente e casos práticos, permitindo uma abordagem abrangente e atualizada sobre o estelionato digital e suas implicações para a sociedade.

2. REVISÃO DA LITERATURA

2.1. Conceito de estelionato

Tipificado pelo artigo 171 do Código Penal, Estelionato é caracterizado como o ato de obter vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro por meio de fraude. Em outras palavras, trata-se de enganar alguém para obter benefício próprio, causando danos à vítima. É um crime contra o patrimônio e prevê pena de reclusão de 1 a 5 anos. Pela nova redação dada pela Lei n.º 13.964, de 24 de dezembro de 2019, foi acrescido o parágrafo 5º, para que as ações penais que decorrem do crime de Estelionato decorram mediante representação da parte ofendida, conforme segue:

> § 5º Somente se procede mediante representação, salvo se a vítima for:
> I - a Administração Pública, direta ou indireta;
> II - criança ou adolescente;
> III - pessoa com deficiência mental; ou
> IV - maior de 70 (setenta) anos de idade ou incapaz (Brasil, 2019).

Este artigo, no entanto, estará focado no crime de Estelionato Virtual ou Estelionato Digital, que também encontra amparo no artigo 171 do código Penal Brasileiro. Segundo Maia (2017, p. 92) “é um tipo de crime no qual o agente se utiliza de um meio de comunicação eletrônico, como a Internet, para atingir o seu objetivo de obter para si ou outrem vantagem patrimonial ilícita, induzindo ou mantendo a vítima em erro”.

Tal crime é cometido por uma pessoa com grande conhecimento de informática ou por um leigo que tenha um mínimo de conhecimento sobre

dispositivos computacionais. Entretanto, de acordo com Coltro e Waldman (2021, p. 115) “a ausência de tipicidade impede o combate efetivo a essas práticas, sendo muito comum a polícia somente instaurar investigação em casos em que seja possível aferir prejuízo financeiro de alguma das vítimas, enquadrando a conduta como delito de estelionato”.

Exemplos típicos deste crime consistem em e-mails falsos, conhecidos como “*phishing*, que induzem a vítima a clicar em *links* maliciosos ou a fornecer dados pessoais e bancários, ou sites fraudulentos, criados para imitar páginas legítimas de instituições bancárias, lojas, ou serviços, cuja finalidade é o de capturar senhas, número de cartão ou realizar cobranças indevidas. Golpes realizados por meio das redes sociais, mediante perfis falsos, simulando pessoas conhecidas que solicitam transferências.

2.1.1. Ambiente digital

A evolução do estelionato para o ambiente digital ocorreu como reflexo direto da transformação tecnológica e da popularização da internet. Anteriormente, o tradicional estelionato dependia unicamente do contato físico ou comunicação direta, como a falsificação de documentos ou promessas enganosas. Através da digitalização, os estelionatários passaram a explorar meios eletrônicos para aplicar golpes, aproveitando-se da facilidade de acesso, anonimato e alcance global.

> Os crimes e seus perpetradores estão em constante mutação por conta da evolução tecnológica, como por exemplo, em termos de tipologias e modo operandi, usando a tecnologia como meio ou objetivo de cometimento de ilícitos, e atuando de forma onde fica cada vez mais difícil identificar as barreiras entre o crime cometido no mundo real e no mundo digital (Duarte, 2023, p. 29).

O desenvolvimento ocorre por meio da ampliação do alcance, em que um golpe que antes atingia poucas pessoas localmente, atualmente alcança milhares de pessoas em somente um segundo, por meio de e-mails, redes sociais e aplicativos. As ferramentas usadas para criar páginas falsas, enviar mensagens em massa e capturar dados ficaram mais sofisticadas.

Além disso, surgiram novas modalidades como *phishing*, clonagem de contas, golpes do PIX, falsas promoções e engenharia social digital. Some-se a isso, a dificuldade de rastreamento, pois o ambiente digital permite a ocultação de identidade e localização, tornando a investigação ainda mais complexa. Para

combater esses crimes, o Código Penal Brasileiro foi atualizado com a Lei 14.155/2021 para incluir o estelionato digital, reconhecendo a gravidade e especificidade dessas práticas que, de acordo com Marques (2024, p. 7), “a evolução manifestada pela Lei 14.155 é para além uma atualização das penas, que praticamente dobram em comparação com o estelionato comum (prisão de 1 a 5 anos), para a estelionato eletrônico (prisão de 4 a 8 anos)”.

2.1.2. Espécies e tecnologias envolvidas

Entende-se que estelionato digital é uma categoria, da qual se subdivide espécies. Maia (2017) descreve que o *Phishing* “consiste em uma técnica na qual o cibercriminoso envia um e-mail pelo qual convence a vítima a lhe fornecer informações confidenciais como senhas, dados bancários, ou outras informações pessoais” (p. 39). Trata-se de uma fraude digital que consiste em enganar a vítima para fornecer informações pessoais, financeiras ou credenciais de acesso. Os meios utilizados são mensagens falsas, que imitam comunicações empresariais, bancárias ou de serviços on-line legítimas.

Já o *Vishing* trata-se de uma modalidade semelhante ao *phishing*, mas realizada por voz, geralmente, por telefone, o termo tem origem no “*voice phishing*”. De acordo com Galindo (2022, p. 18), o contato “é feito pelos telefones celulares, seja por meio de ligações ou envio de áudios em aplicativos de comunicação, onde o criminoso tenta, mediante argumentação, convencer a vítima a divulgar suas informações pessoais”.

Brochado (2025, p. 158) também aponta acerca dos Falsos boletos, que trata-se da emissão de boletos falsificados para desvio de pagamentos destinados a empresas, tributos ou compras *online*. É uma forma comum de estelionato digital. Tal golpe consiste em que os criminosos criam boletos com aparência legítima, alterando os dados do beneficiário de forma que o pagamento vá para contas fraudulentas.

Golpes em redes sociais e aplicativos de mensagens: são a forma mais frequente de estelionato digital, onde os criminosos exploram a comunicação rápida entre usuários. Por essa modalidade, ocorrem a clonagem de contas, falsas ofertas e sorteios, engenharia social e links fraudulentos. Estes golpes, podem ser realizados por meio da

> Venda de produtos falsificados ou inexistentes em plataformas de comércio eletrônico, o oferecimento de oportunidades de investimento falsas em criptomoedas ou outros esquemas de pirâmide, e a aplicação de golpes em redes sociais, onde os criminosos se passam por pessoas conhecidas das vítimas para solicitar dinheiro ou informações pessoais (Sá, Costa, *et. al.,* 2025, p. 2812).

Fraudes bancárias e de cartão de crédito: estas são as modalidades mais comuns de estelionato digital. Nelas, os criminosos utilizam meios tecnológicos para obter acesso a contas, dados financeiros ou realizar transações fraudulentas. Elas crescem à medida que o uso dos serviços bancários on-line e pagamentos digitais aumentam. As fraudes bancárias são as mais comuns. Nelas, o falso funcionário ou falsa central de atendimento, o golpista se passa por um colaborador do banco e informa problemas no cadastro ou irregularidades na conta, levando a vítima a fornecer seus dados, possibilitando que o criminoso realize transações indevidas (SOARES, 2024, p. 18).

Por fim, temos a mais recente modalidade denominada de Golpe do Pix. Ele ocorre quando criminosos induzem a vítima a fazer uma transferência instantânea sob pretextos, tais como promoções falsas, clonagem de *WhatsApp*, ou ainda, fingindo ser uma pessoa conhecida com problemas. É um golpe rápido, a reversão é difícil e se tornou comum pela praticidade do sistema.

Conforme pontua Bicalho (2024, p. 54), o pix “facilita transferências bancárias, impulsionou o aumento de fraudes envolvendo roubos e furtos de celulares, onde vítimas são induzidas a fazer transferências ou têm suas contas acessadas após o roubo do dispositivo”. A rapidez e a praticidade do Pix contribuíram para o aumento de fraudes. Os criminosos aproveitam roubos de celulares para acessar contas bancárias ou induzir a vítima a realizar transferências imediatas, explorando a agilidade do sistema.

O estelionato digital se aproveita de tecnologias como redes sociais, malwares, engenharia social e inteligência artificial para enganar as vítimas e aplicar os golpes online. As principais tecnologias e recursos utilizados pelos golpistas virtuais são as redes sociais e os mensageiros instantâneos: por estes meios, os criminosos aplicam golpes de engenharia social como sequestro de contas, perfis falsos e solicitações de dinheiro em nome de terceiros. De acordo com Muniz (2023, online), “é frequentemente executada por indivíduos que demonstram notável conhecimento sobre a internet e tecnologias da informação. Eles adentram o espaço

virtual com a intenção de prejudicar e enganar outras pessoas, visando obter vantagens ilícitas".

Por outro lado, as *Phishing* e *Spoofing* também agregam essas práticas por serem técnicas que simulam páginas ou comunicações legítimas para enganar usuários a fim de obter dados sensíveis, como senhas e números de cartão. De acordo com Araújo (2025, p. 12), *phishing* "consiste no envio de mensagem falsa, principalmente por e-mail ou aplicativo de mensagens que imitam comunicações legítimas de instituições financeiras ou empresas governamentais, e levam as vítimas a fornecer informações confidenciais". Já o *Spoofing*, segundo a autora, ocorre quando uma pessoa falsifica identidades online para enganar as pessoas, como criar páginas falsas que parecem legítimas (ARAÚJO, 2025, p. 12).

Na mesma perspectiva os *Malwares* e *Spywares* são programas maliciosos que se instalam em dispositivos e que capturam informações bancárias, senhas ou redirecionam transações sem que a vítima tome conhecimento. Segundo Santos (2023, p. 9) malware "é uma categoria extensa que engloba *software* malicioso, como vírus, *trojans*, *spyware* e *ransomware*".

Contudo essas práticas se avançam constantemente nas abordagens de clonagem de dispositivos e cartões por meio de dispositivos como *skimmers*, popularmente denominados de "chupa-cabras" copiam dados de cartões físicos, enquanto aplicativos podem clonar interfaces bancárias para roubar credenciais, conforme afirma Tubino (2016, p. 60-61), "ataques como "Chupa-Cabras" e adulteração de máquinas de cartões utilizam dados roubados dos usuários para trazer prejuízos ao sistema em geral".

2.2. Cenário atual e Estatísticas

O Brasil está enfrentando um cenário crítico de fraudes digitais, com aumento expressivo de golpes, principalmente entre jovens e usuários das redes sociais, bancos e e-commerce. O país figura entre os mais vulneráveis do mundo. Conforme o site (Poder360 2025), os crimes digitais tiveram um aumento de 45% em 2024, totalizando 5 milhões de fraudes, citando a Associação de Defesa de Dados Pessoais e do Consumidor (ADDP).

Isso significa que uma em quatro pessoas já sofreu uma tentativa de golpe, sendo metade delas efetivamente. Ainda segundo o site, os tipos de fraudes que

mais cresceram foram invasão de contas, *phishing*, golpes bancários e fraudes em redes sociais. A inteligência artificial fez com que os golpes se tornassem cada vez mais sofisticados, simulando vozes e imagens de pessoas convincentemente (Poder360, 2025).

Citando dados da Global Fraud Index 2025, O jornalista Emanuel Negromonte afirma que o Brasil “entrou oficialmente no grupo dos 15 piores países do mundo em risco de fraude digital e hoje é o país com a pior classificação da América Latina” (Negromonte, 2025). A afirmação do autor do artigo evidencia a grave vulnerabilidade do Brasil diante dos crimes digitais. Isso mostra que o Brasil possui falhas estruturais na proteção de dados, na educação digital da população e na capacidade de resposta das autoridades.

Este cenário pede urgência na implantação de políticas públicas mais eficazes, investimentos em cibersegurança e campanhas de conscientização voltadas para o uso seguro da tecnologia, principalmente diante da crescente digitalização dos serviços financeiros e sociais. O site Poder 360 afirma que o prejuízo médio por vítima pode ultrapassar o valor de R$ 6.000,00, com perdas nacionais estimadas em R$ 10 bilhões (Poder360, 2025).

Conforme a TransUnion, as transações suspeitas tiveram um aumento de 11% em 2024 em relação ao ano anterior., destacando a invasão de contas que teve aumento de 20% (Transunion, 2025). Este crescimento de fraudes destaca a sofisticação dos golpes e a urgência de reforçar mecanismos de segurança e autenticação nos serviços online.

Flávia Albuquerque, jornalista da Agência Brasil, utilizando dados da TransUnion, revela que “40% dos brasileiros já foram alvo de fraudes por e-mail, internet, telefone ou mensagens de texto e 10% dos pesquisados disseram ter caído nos golpes. As perdas atingiram uma média de R$ 6.311,00 (Albuquerque, 2025). Esses dados evidenciam não somente o grau de sofisticação dos criminosos, mas também a fragilidade dos mecanismos de proteção e a falta de conscientização digital entre os usuários.

2.2.1. Principais vítimas

Não existe um perfil único para as vítimas de fraudes digitais, uma vez que esses golpes atingem todas as faixas etárias e diversas classes sociais. Segundo o jornalista Galtiery Rodrigues, do jornal digital Metrópoles, “não existe um perfil

específico de quem costuma cair mais nos golpes digitais. Em geral, os dados evidenciam semelhança com as características socioeconômicas dos brasileiros" (Rodrigues, 2024).

Segundo Albuquerque 2025, "a Geração Z, os nascidos entre 1997 e 2010, foi a que mais relatou perdas (38%), enquanto os *Baby Boomers*, os nascidos entre 1946 e 1964, foram os que menos relataram (11%) perdas". Os dados apresentados pela jornalista demonstram que a geração Z é a mais suscetível às fraudes digitais. Isso pode estar associado à maior exposição a plataformas digitais e à confiança excessiva em ambientes virtuais. Por outro lado, os chamados *Baby Boomers*, menos presentes no ambiente digital, registram apenas 11% de perdas, o que indica que o comportamento digital influencia diretamente o risco de ser vítima de estelionato virtual. Os jovens são os mais vulneráveis pelo fato de estarem mais expostos a redes sociais, aplicativos e compras online, na maioria das vezes, sem práticas seguras. Rodrigues afirma ainda que o Estado de São Paulo lidera em decorrência de golpes, sendo seguido por Mato Grosso, Roraima e Distrito Federal (Rodrigues 2024).

2.2.2. Plataformas mais visadas

As plataformas mais visadas pelos criminosos são bancos digitais e tradicionais, lojas de e-commerce e redes sociais. Os golpes bancários, *phishing* e fraudes sociais são líderes em ocorrências. No ano de 2024, o golpe do *Whatsapp* foi o mais frequente, conforme informa o G1, "o golpe do WhatsApp acontece quando criminosos clonam a conta de WhatsApp da vítima" (Machado 2025).

No Brasil também é destaque em ataques impulsionados por Inteligência Artificial e *deepfakes*. Consoante o G1, "grande parte dos dados cadastrais dos cidadãos já se encontram expostos, além de outras informações que podem ser coletadas em redes sociais pelos criminosos, somado ao uso da Inteligência Artificial, a prática de engenharia social tornou-se significativamente mais fácil".

Na área de e-commerce, as fraudes envolvem desde o uso de cartões clonados até a criação de sites falsos, que imitam com fidelidade os das lojas legítimas, capazes de enganar os consumidores. De acordo com Jesus (2023, p. 201), citando dados da Safety Detectives de 2020, este segmento "foi o segmento propulsor desses ataques, com 41% dos casos" (Jesus, 2023). A facilidade de

realizar compras online, associada à ausência de verificação rigorosa em algumas plataformas, contribui para a disseminação desse tipo de golpe.

O estelionato digital se manifesta de forma mais sofisticada e frequente, apresentando casos emblemáticos que ilustram tanto a criatividade dos criminosos quanto as fragilidades dos sistemas digitais e do comportamento dos usuários. De acordo com Negromonte (2025), “o Uruguai aparece na 30ª posição global como o país mais protegido da região, o Brasil figura entre os lanternas, ao lado da Colômbia, no grupo de nações ‘menos protegidas contra fraude digital’”. O caso mais emblemático de fraude digital é o já mencionado ‘golpe do *Whatsapp*’, quando criminosos clonam contas de usuários e solicitam transferências de valores. Para que este golpe se efetive,

> O fraudador necessita ter acesso ao número de telefone utilizado pela vítima no aplicativo WhatsApp e sua senha de entrada, ou seja, o código de autenticação composto por seis dígitos obtido por meio do mecanismo de segurança conhecido como "Verificação em duas etapas", que consiste essencialmente em uma senha personalizada definida pelo usuário para acessar o aplicativo (Gonçalves e Henriques, 2024, p. 14).

Globalmente, tem se observado um crescente uso de tecnologias de inteligência artificial como *deepfakes* e voz sintética, que aplicam fraudes de valores elevados. Sousa, Maia, *et al.* (2025, p. 6) afirmam que “ofensores motivados pela inteligência artificial generativa com uso de *deepfakes* podem potencializar a motivação e a capacidade dos fraudadores.” Este caso de fraude revela uma fronteira nova do estelionato digital, no qual a manipulação de identidades e de confiança interpessoal é potencializada por recursos tecnológicos avançados. Tais episódios emblemáticos demonstram que o estelionato digital não está limitado a ações isoladas. Ele constitui um fenômeno complexo, dinâmico e transnacional, que transcende fronteiras geográficas e jurídicas, articulando redes criminosas com alto grau de sofisticação, que explicam vulnerabilidades tecnológicas e humanas.

2.3. Legislação e Responsabilidade

O Brasil tem um conjunto de leis que busca combater o estelionato digital, incluindo o código Penal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e a lei dos crimes cibernéticos. No entanto, a aplicação dessas leis ainda esbarra em obstáculos práticos, tais como o impedimento de responsabilizar

plataformas digitais que abrigam ou promovem golpes, principalmente quando operam fora do país.

Além disso, a investigação desses crimes é complexa, demandando recursos avançados, colaboração internacional e equipes especializadas, algo que nem sempre se encontra disponível nos organismos policiais e judiciais brasileiros. São fatores como esses que cooperam para a percepção de impunidade e para o crescimento continuado de fraudes digitais.

O ordenamento jurídico brasileiro evoluiu significativamente para enfrentar os crimes digitais, em especial o estelionato virtual, acompanhando o avanço das tecnologias da informação e o aumento das práticas ilícitas no ambiente digital. Nesse contexto, foram instituídas leis específicas que visam não apenas a proteção de dados pessoais e da privacidade dos usuários, mas também a responsabilização penal dos agentes envolvidos em fraudes eletrônicas, além da regulação do uso da internet.

O Código Penal Brasileiro contempla dispositivos que tratam diretamente do estelionato digital, especialmente após atualizações legislativas que visam acompanhar a evolução dos crimes cibernéticos. O artigo 171, originalmente concebido para tratar de crimes de estelionato como obtenção de vantagem ilícita em prejuízo alheio mediante fraude, foi significativamente reforçado pela Lei 14.155/2021. Essa lei expandiu a pena para casos nos quais o crime é praticado por meio eletrônico, aumentando a reclusão para 4 a 8 anos, além de multa, quando há uso de redes sociais, e-mails, aplicativos de mensagens ou outras ferramentas digitais para enganar as vítimas.

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa.
> [...]
> § 2o-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (Brasil, 2024, p. 77-78).

Esta mudança reflete o reconhecimento do Estado sobre o aumento da gravidade e da incidência dos golpes virtuais. Além do reforço no artigo 171, foi inserida pela Lei 12.737/2012 o artigo 154-A, conhecida como Lei Carolina Dieckmann, que trata da invasão de dispositivo informático sem autorização do usuário titular, objetivando obter, adulterar, ou destruir dados, ou informações.

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> [...]
> § 2o Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Brasil, 2024, p. 68).

Estes dois artigos constituem a base penal para o enfrentamento do estelionato digital no Brasil, conquanto sua efetividade esteja sujeita à capacidade de investigação, da produção de provas digitais e da atuação entre autoridades policiais, Ministério Público e o Poder Judiciário.

2.3.1. Marco Civil da Internet

O Marco Civil da Internet, promulgado em 2014, pela lei n.º 12.965, de 23 de abril de 2014, representa um marco regulatório fundamental para o uso da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres dos usuários, provedores de serviços e do poder público. O objetivo da Lei é, segundo Ruas, Pinas, *et al.* (2024, p. 15), “proteger a privacidade, a liberdade de expressão e a neutralidade da rede, além de regular responsabilidades de provedores de internet e garantir a segurança dos usuários”.

Na área do estelionato digital, o marco civil da Internet é relevante por definir a responsabilidade dos provedores de conexão e de aplicações de internet em casos de violação de direitos. Segundo a legislação:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (Brasil, 2014).

Isso mostra que os provedores só poderão ser responsabilizados em caso de descumprimento de ordens judiciais específicas, que determinem a remoção de conteúdo ilícito ou ofensivo. Além disso, o marco civil determina a guarda e proteção de registros de acesso, essencial para investigações de crimes digitais (Artigo 10, da Lei 12.965/2014). O marco civil, apesar de não tratar diretamente da tipificação de crimes digitais, oferece uma base normativa importante para responsabilizar

plataformas que se omitem diante de conteúdos fraudulentos ou que não adotem medidas adequadas de segurança e transparência.

2.3.2. Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados, que recebeu o número 13.709/2018, representa um marco regulatório essencial para a proteção da privacidade e da segurança informacional no Brasil. O objetivo dessa lei é o de “garantir o cumprimento da legislação e proteger os direitos dos titulares dos dados, variando desde advertências, multa simples, multa diária, bloqueio de dados pessoais, suspensão parcial do funcionamento de banco de dados e outras penalidades” (Ruas, Pinas, *et al.*, 2024, p. 16).

No contexto do estelionato digital, a LGPD exerce papel estratégico ao determinar transparência, consentimento explícito e medidas de segurança apropriadas para o uso de dados pessoais. A LGPD prevê penas administrativas para infrações que incluem advertências, multas que podem atingir 2% do faturamento das empresas, bloqueio ou eliminação dos dados pessoais envolvidos. Sua aplicação coopera diretamente para a prevenção de fraudes digitais, ao requerer uma cultura de responsabilidade no tratamento de dados e ao fortalecer os direitos dos titulares, como acesso, correção e exclusão de suas informações.

2.3.3. Lei dos Crimes Cibernéticos (Lei n.º 12.737/2012)

Também conhecida como Lei Carolina Dieckmann, foi um marco inicial da tipificação de crimes informáticos no Brasil. A lei foi criada após um caso emblemático envolvendo a atriz que dá nome à norma. Segundo Maia (2017, p. 43), “apesar de ser a primeira a tipificar um delito estritamente virtual, ainda não é suficiente para englobar o número de ilícitos que podem ser cometidos em ambiente cibernético”.

Muitos crimes praticados em ambientes virtuais abrangem múltiplas jurisdições, uso de redes criptografadas e técnicas de anonimização, impedindo a aplicação direta da norma. Mesmo assim, essa lei serve como base para responsabilização penal em casos de acesso indevido a sistemas, roubo de dados e sabotagem digital.

2.3.4. Responsabilidade das plataformas digitais e instituições financeiras

A crescente incidência de fraudes digitais amplia o debate sobre a responsabilidade das plataformas tecnológicas e das instituições financeiras. De acordo com Silva (2025, p. 52) “O Marco Civil da Internet estabelece princípios importantes sobre neutralidade da rede e proteção de dados, mas é insuficiente para lidar com a responsabilização penal ou administrativa de empresas que facilitam a ocorrência de ilícitos digitais”.

As plataformas digitais são frequentemente utilizadas como vetores para golpes de engenharia social, sequestro de contas e disseminação de conteúdo fraudulento. Muitas dessas empresas operam fora do território nacional, dificultando a aplicação da legislação brasileira e o cumprimento das ordens judiciais.

No caso das instituições financeiras, principalmente os bancos digitais, estas têm sido pressionadas a adotar mecanismos robustos de autenticação, monitoramento de transações suspeitas e canais de atendimentos ágeis. Silva afirma que “a cooperação entre instituições bancárias e órgãos públicos intensificou-se nos últimos anos, com a criação de protocolos de notificação obrigatória de incidentes e a adoção de padrões mínimos de segurança digital” (Silva, 2025, p. 38).

A responsabilização dessas entidades é um elemento central na construção de um ecossistema digital mais seguro, exigindo compromisso ético, transparência operacional e cooperação com autoridades públicas no enfrentamento eficaz do estelionato digital.

2.4. Dificuldades na investigação e punição

Por mais que haja avanço legislativo e da crescente conscientização sobre os riscos do estelionato digital, a investigação e punição desses crimes ainda enfrentam barreiras significativas no Brasil. Uma das principais dificuldades na investigação, de acordo com Maia (2017, p. 69), “diz respeito à demora em se obter informações dos provedores de serviços de internet, informações estas por vezes essenciais ao desenvolvimento da investigação criminal”.

A natureza transnacional e altamente técnica das fraudes digitais impõe desafios que vão além da estrutura tradicional do sistema penal. Segundo Soares (2024, p. 24), “a falta de integração entre as forças policiais e a ausência de um canal unificado para comunicação entre agências agravam as dificuldades na

investigação de estelionatários virtuais". As limitações técnicas e operacionais nas forças de segurança pública também colaboram com essas dificuldades.

> Embora existam esforços para compelir as plataformas digitais a colaborarem com investigações criminais, especialmente no que tange o fornecimento de dados pessoais, há, ainda, uma série de limitações técnicas e jurídicas que impedem a fluidez do procedimento investigatório (Prado, 2024).

Outro fator que dificulta a investigação dos crimes digitais é a dependência de representação da vítima. Muito embora, a realização das investigações fique a cargo da polícia judiciária e do Ministério Público, de acordo com Diniz, (2022, p. 10) "referida provocação do juízo criminal só ocorrerá se a vítima demonstrar formalmente o desejo de representação contra o autor".

Finalmente, a taxa de condenações relativamente baixa e a morosidade dos processos judiciais tem contribuído para a sensação de impunidade, estimulando a continuidade das práticas criminosas, conforme pontua Araújo (2025, p. 8) "persistem entraves internos como a morosidade processual, a escassez de recursos técnicos e a baixa capacitação especializada nas instituições responsáveis pela investigação e repressão dessas condutas".

A lentidão na tramitação de processos, a dificuldade de produção de provas técnicas e a complexidade das investigações transnacionais tornam o sistema de justiça menos eficaz diante da agilidade e sofisticação dos criminosos. Este cenário afeta a reparação das vítimas e beneficia a reincidência e o crescimento das práticas fraudulentas.

2.5. Prevenção e Combate

Ante os crescentes casos de estelionatos digitais, torna-se indispensável adotar estratégias integradas de prevenção e combate, envolvendo usuários, empresas, instituições financeiras e o poder público. A proteção contra fraudes virtuais requer não somente o fortalecimento de sistemas tecnológicos, mas também a promoção de uma cultura de segurança digital. O Brasil, de acordo com Silva (2025, p. 112), "embora tenha centros especializados em alguns estados e iniciativas isoladas, carece de um programa nacional integrado que articule prevenção, repressão, educação digital e cooperação internacional".

Apesar de o Brasil possuir centros especializados em cibersegurança em alguns estados e iniciativas pontuais de prevenção e repressão, o país ainda não

dispõe de um programa nacional articulado que integre ações educativas, políticas públicas, mecanismos de investigação e cooperação internacional.

> Partindo de uma análise mais profunda sobre as formas de controle e de combate, pode-se ver que é um cenário muito complexo para o poder público tratá-lo de forma satisfatória no que diz respeito à prevenção e combate, gerando dificuldades quanto aos resultados de proteção no mundo concreto (Vanderei, 2024, p. 3).

Essa ausência compromete a eficácia das respostas institucionais, dificulta a padronização de procedimentos e limita a capacidade de atuação coordenada, frente a um fenômeno que transcende fronteiras e exige soluções interdisciplinares e colaborativas.

2.5.1. Boas práticas de segurança digital para usuários

Os usuários desempenham papel fundamental na prevenção de golpes virtuais. A adoção de boas práticas de segurança, como uso de senhas fortes e únicas, a ativação de autenticação em dois fatores, a verificação da origem de mensagens e links suspeitos, e o cuidado ao compartilhar dados pessoais, pode reduzir significativamente o risco de fraudes. De acordo com Santos (2023, p. 17), a internet “tornou-se um ambiente inseguro, tornando-se indispensável que os usuários adotem boas práticas de segurança digital, atentando-se para os perigos e ameaças potenciais”. Além disso, é recomendável manter os dispositivos atualizados, utilizar antivírus confiáveis e evitar conexões públicas para transações sensíveis.

Para Prado (2024, p. 56) “a falta de conhecimento quanto às inúmeras ameaças digitais, juntamente com a carência de boas práticas de segurança, expõe indivíduos e organizações às quais pertencem a riscos significativos”. A autora enfatiza um dos principais fatores que cooperam para a vulnerabilidade no ambiente digital: a deficiência de conhecimento técnico e de hábitos seguros por parte dos usuários. Essa brecha não somente afeta a proteção individual, mas também coloca em risco as organizações às quais esses indivíduos estão ligados, uma vez que práticas inseguras podem facilitar o acesso indevido a sistemas corporativos, dados sensíveis e recursos financeiros.

2.5.2. Medidas adotadas por empresas e bancos

Empresas e instituições financeiras investem em protocolos de segurança cibernética, como sistemas de detecção de comportamento anômalo, criptografia de

dados, monitoramento em tempo real e canais de atendimento especializado para vítimas de fraude. De acordo com Silva (2025, p. 36): “A adequada compreensão de protocolos de segurança, da rastreabilidade de IPs, da cadeia de custódia digital e da criptografia assimétrica, por exemplo, é essencial para garantir a paridade de armas e o contraditório nos processos judiciais”.

Os bancos têm aprimorado seus aplicativos com camadas adicionais de autenticação, alerta de transações suspeitas e bloqueio automático em caso de atividade incomum. A responsabilidade corporativa inclui também a educação dos clientes, por meio de campanhas informativas e treinamentos sobre segurança digital.

2.5.3. Papel da educação digital e da conscientização

A educação digital é uma ferramenta estratégica no combate ao estelionato virtual. A conscientização sobre os riscos, as formas de atuação dos criminosos e os mecanismos de proteção deve ser requerida desde a formação escolar até programas de capacitação para adultos e idosos. De acordo com Sá, Costa, ***et al.*** (2025, p. 9) “muitos usuários ainda não estão plenamente cientes de seus direitos ou das implicações do compartilhamento de seus dados pessoais na internet”.

> Medidas fundamentais à redução do estelionato virtual são as ações na área da educação, como a inserção e valorização de disciplinas voltadas ao ramo da informática em âmbito escolar, que venham a abranger não só o correto uso dos aparelhos eletrônicos no sentido do manuseio operacional, mas também a existência de discussões a respeito da proteção e cautela na divulgação de dados pessoais, no cuidado ao acessar determinados conteúdos, na verificação preliminar da confiabilidade de determinado acesso e na preparação do usuário para que o mesmo conheça as características de um possível golpe (Diniz, 2022, p. 20).

Campanhas públicas, iniciativas comunitárias e ações educativas nas redes sociais podem contribuir para a construção de uma sociedade mais preparada para lidar com ameaças digitais, reduzindo a vulnerabilidade dos usuários.

2.5.4. Tecnologias de prevenção

O avanço tecnológico tem proporcionado ferramentas eficazes para a prevenção de fraudes. A autenticação em dois fatores (2FA), que exige uma segunda verificação além da senha, é uma das medidas mais difundidas. A biometria, como reconhecimento facial ou digital, oferece uma camada adicional de segurança, dificultando o acesso indevido.

> Além de políticas e programas desenvolvidos pelos órgãos e entidades públicas, existem diversas ferramentas de prevenção que podem ser utilizadas pelos usuários da internet para não serem vítimas de cibercrimes, medidas acessíveis e de fácil entendimento, quais sejam: não abrir e-mails e anexos desconhecidos, utilizar programas de antivírus no intuito de detectar e bloquear ameaças, conectar-se em sinal de wiffi confiável, realizar compras através de sites de e-commerce conhecido, bem como averiguar se ele utiliza protocolo HTTPS (Jesus, 2023, p. 214).

Ademais, sistemas baseados em inteligência artificial são aproveitados para identificar padrões suspeitos, antever comportamentos fraudulentos e impedir transações em tempo real. Essas tecnologias, quando integradas a políticas de segurança e educação, formam um broquel potente contra o estelionato digital.

3. RESULTADOS E DISCUSSÃO

O combate ao estelionato digital enfrenta desafios multifacetados, que vão desde a rápida evolução das técnicas criminosas até a dificuldade de identificação dos autores. A sofisticação dos golpes, impulsionada pelo uso de inteligência artificial, *deepfakes* e engenharia social, torna cada vez mais difícil distinguir fraudes de interações legítimas (Duarte, 2023). Além disso, a amplitude do alcance digital permite que milhares de pessoas sejam afetadas em questão de segundos, dificultando a resposta das autoridades e das vítimas. O cenário brasileiro é agravado pela vulnerabilidade estrutural na proteção de dados, pela falta de educação digital e pela limitada capacidade de investigação das autoridades (Negromonte, 2025).

Apesar dos avanços legislativos, como a atualização do Código Penal e a criação de leis específicas (Lei 14.155/2021, LGPD, Marco Civil da Internet), persistem lacunas significativas. A legislação muitas vezes não acompanha a velocidade das inovações tecnológicas, dificultando a tipificação de novos delitos digitais (Brasil, 2014, 2019, 2024. A responsabilização de plataformas digitais e instituições financeiras ainda é limitada, especialmente quando operam fora do território nacional. Por essa falta, as investigações são prejudicadas pela dependência de representação da vítima, pela morosidade processual, pela escassez de recursos técnicos e pela baixa capacitação especializada das equipes policiais (Maia, 2017).

Para enfrentar o estelionato digital eficazmente, é fundamental investir em estratégias integradas que envolvam tecnologia, educação e cooperação

institucional. Entre as propostas de melhoria destaca-se o fortalecimento da educação digital, voltada para inserção de disciplinas sobre segurança digital desde o ensino básico, campanhas de conscientização e treinamento para todas as faixas etárias, especialmente jovens e idosos (Sá, costa, *et al.*, 2025; Diniz, 2022). Bem como o aprimoramento dos mecanismos de investigação para a criação de canais unificados de comunicação entre agências, investimentos em equipes especializadas e adoção de tecnologias avançadas de rastreamento e produção de provas digitais (Prado, 2024).

Na perspectiva de Silva (2025, a responsabilização efetiva de plataformas e bancos busca estabelecer protocolos obrigatórios de notificação de incidentes, exigência de padrões mínimos de segurança e cooperação internacional para cumprimento de ordens judiciais, de modo que, tal ação facilita a adoção de tecnologias de prevenção: implementação de autenticação em dois fatores, biometria, sistemas de inteligência artificial para detecção de padrões suspeitos e bloqueio automático de transações fraudulentas estabelecidas por (Jesus, 2023). Contudo, a promoção de uma cultura de segurança digital é o ponto forte e específico ao incentivo de boas práticas por usuários e empresas, como senhas fortes, verificação de links e atualização constante de sistemas (Santos, 2023; Prado, 2024).

4. Considerações finais

O presente estudo abordou os principais aspectos do estelionato digital, destacando sua evolução, modalidades, tecnologias envolvidas, cenário atual, legislação, desafios investigativos e estratégias de prevenção. Observou-se que o crescimento acelerado dos crimes virtuais no Brasil está diretamente relacionado à popularização da internet, à sofisticação das técnicas criminosas e à vulnerabilidade dos usuários e sistemas.

A análise crítica evidenciou que, apesar dos avanços legislativos e do investimento em tecnologias de segurança, ainda existem lacunas significativas na atuação das autoridades e na responsabilização de plataformas digitais e instituições financeiras. A morosidade processual, a dependência de representação da vítima e a baixa capacitação técnica dificultam a investigação e a punição dos crimes, contribuindo para a sensação de impunidade.

Diante desse cenário, reforça-se a importância do combate ao estelionato digital por meio de ações integradas, que envolvam educação digital, aprimoramento dos mecanismos de investigação, adoção de tecnologias avançadas de prevenção e promoção de uma cultura de segurança entre usuários e empresas. O fortalecimento da cooperação internacional e a atualização constante das normas jurídicas também são essenciais para enfrentar um fenômeno dinâmico e transnacional.

Como sugestões para futuras pesquisas ou ações, recomendam-se investigar o impacto de novas tecnologias, como inteligência artificial e biometria, na prevenção e detecção de fraudes digitais; avaliar a efetividade das campanhas de conscientização e educação digital em diferentes faixas etárias; propor modelos de cooperação internacional para agilizar investigações e responsabilização de agentes transnacionais; estudar mecanismos inovadores de proteção de dados e autenticação, visando reduzir vulnerabilidades em ambientes digitais.

A construção de um ecossistema digital mais seguro depende do engajamento de todos os atores envolvidos e da constante atualização das estratégias de enfrentamento, visando proteger o patrimônio e a privacidade dos cidadãos brasileiros.

Referências

ALBUQUERQUE, F. Quatro em cada 10 brasileiros já foram alvo de fraudes pela internet. **Agência Brasil**, 21/06/2025, online. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2025-06/brasileiros-perderam-em-media-mais-de-r-6-mil-em-fraudes. Acesso em: 13 nov. 2025.

BICALHO, Camila Fernandes. **Crimes patrimoniais na era digital:** contribuições da Teoria das Atividades Rotineiras. 2024. Monografia (Especialização em Estudos da Criminalidade e Segurança Pública) — Faculdade de Filosofia e Ciências Humanas, Universidade Federal de Minas Gerais, Belo Horizonte, 2024. Disponível em: https://hdl.handle.net/1843/80146. Acesso em; 01 nov. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2025]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 set. 2025.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código Penal. 7ª. ed. Brasília: Senado, 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 16 out. 2025.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 nov. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 16 nov. 2025.

BRASIL. **Lei n.º 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 10 nov. 2025.

BROCHADO, I. P. D. S. **Investigação de crimes cibernéticos nas Polícias Civis do Brasil:** contribuição da gestão do conhecimento. 2025. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento), Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis, 2025. Disponível em: https://repositorio.ufsc.br/handle/123456789/265749. Acesso em: 12 out. 2025.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Criminalidade Digital No Brasil: A Problemática E A Aplicabilidade Da Convenção De Budapeste. **Revista Em Tempo**, [S.l.], v. 21, n. 1, p. 104-123, ago. 2021. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3247. DOI: https://doi.org/10.26729/et.v21i1.3247. Acesso em: 21 nov. 2025.

DUARTE, Emerson de Barros. **Cibercrimes e Humanidades Digitais** — Uma investigação transdisciplinar sobre o caso da segurança pública brasileira. 2023. 98 f. Dissertação (Mestrado em Humanidades Digitais). Instituto Multidisciplinar, Universidade Federal Rural do Rio de Janeiro, Nova Iguaçu, RJ. 2023. Disponível em: https://rima.ufrrj.br/jspui/handle/20.500.14407/14064. Acesso em: 12 out. 2025.

GALINDO, Guilherme Delgado. **A evolução do estelionato pelo meio digital**. 2022. Monografia (Bacharelado em Direito) - Faculdade de Direito, Campus Higienópolis, Universidade Presbriteriana Mackenzie, Higienópolis, 2022. Disponível em: https://dspace.mackenzie.br/handle/10899/32604. Acesso em: 30 out. 2025.

HENRIQUES, Thiago Alves; MARTINS GONÇALVES, Samuel. CRIMES DIGITAIS: : análise sobre o Estelionato virtual. **Revista Eletrônica de Ciências Jurídicas**, *[S. l.]*, v. 14, n. 1, 2024. Disponível em: https://revista.fadipa.br/index.php/cjuridicas/article/view/576. Acesso em: 11 dez. 2025.

JESUS, B. C. D. Crimes cibernéticos: desafios da segurança pública e seu enfrentamento. In: NOGUEIRA, F. L.; SILVA, D. B. D.; FÉLIX, Y. D. S. **Gestão em Segurança Pública:** relevância e desafios na perspectiva dos direitos humanos. Campo Grande: UFMS, 2023. p. 165-226. Disponível em: https://repositorio.ufms.br/handle/123456789/8244. Acesso em: 11 dez. 2025.

MACHADO, S. Os golpes virtuais que mais fazem os brasileiros perder dinheiro. **G1**, 02/05/2025, online. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/05/02/os-golpes-virtuais-que-mais-fazem-os-brasileiros-perder-dinheiro.ghtml. Acesso em: 16 nov. 2025.

MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. 2017. 114 f. Monografia (Bacharelado em Direito) — Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2017. Disponível em: http://www.repositorio.ufc.br/handle/riufc/31996. Acesso em: 19 out. 2025.

MARQUES, T. A. S. Crime de estelionato na contemporaneidade frente à tecnologia virtualL. **RECIMA21 - Revista Científica Multidisciplinar**, *[S. l.]*, v. 5, n. 5, p. e555244, 2024. DOI: 10.47820/recima21.v5i5.5244. Disponível em: https://recima21.com.br/recima21/article/view/5244. Acesso em: 11 dez. 2025.

MUNIZ, G. L. A. Estelionato e a facilitação do seu avanço por meio da tecnologia no cenário brasileiro. **Scientia et Ratio**, 2023, online. Disponivel em: https://scientiaetratio.com.br/estelionato-e-a-facilitacao-do-seu-avanco-por-meio-da-tecnologia-no-cenario-brasileiro/. Acesso em: 11 nov. 2025.

NEGROMONTE, E. Alerta vermelho: Brasil é classificado como um dos 15 países mais arriscados para fraudes digitais no mundo. **SempreUpdate**, 13 nov.2025, online. Disponivel em: https://sempreupdate.com.br/brasil-risco-de-fraude-global-fraude-digital/. Acesso em: 13 nov. 2025.

PODER360. Golpes digitais crescem 45% em 2024, diz associação. **Poder 360**, 02/01/2025. Disponivel em: https://www.poder360.com.br/poder-brasil/golpes-digitais-crescem-45-em-2024-diz-associacao/. Acesso em: 13 nov. 2025.

RODRIGUES, G. 24% dos brasileiros caíram em golpes virtuais em 1 ano, diz pesquisa. **Metrópoles**, 30/09/2024, online. Disponivel em: https://www.metropoles.com/brasil/24-dos-brasileiros-cairam-em-golpes-virtuais-em-1-ano-diz-pesquisa. Acesso em: 13 nov. 2025.

RUAS, L. S. et al. O tratamento jurídico dos crimes virtuais com base na legislação brasileira. **Revista Jurídica do Nordeste Mineiro**, Teófilo Otoni, v. 5, p. 1-20, 2024. ISSN 2675-4312.

SÁ, A. A. D. et al. cibercrimes no brasil: análise do estelionato virtual e suas implicações jurídicas. **Periódicos Brasil: Pesquisa Científica**, s/l, v. 4, n. 1, p. 2802-2818, Jun 2025. ISSN 2674-9432.

SANTOS, Glenda S. Felix. **Cibercriminalidade:** o dilema da sociedade atual na utilização dos espaços virtuais. 2023. Monografia (Bacharelado em Direito), Centro Universitário Doutor Leão Sampaio, Juazeiro do Norte, 2023. Disponível em: https://sis.unileao.edu.br/uploads/3/DIREITO/D1331.pdf. Acesso em: 12 nov. 2025.

SOARES, T. V. D. S. P. **Desafios e perspectivas da prevenção e investigação do estelionato on-line**. 2024. Monografia (Bacharelado em Direito), Centro Universitário do Rio Grande do Norte, 2024. Disponível em: https://repositorio.unirn.edu.br/jspui/handle/123456789/1008. Acesso em: 10 nov. 2025.

SOUSA, Gesson Eliésio Aguiar de; MAIA, Brena Gomes; LIMA JÚNIOR, Agnelo Batista de; MELLO, Cesar Mauricio de Abreu; SENA, Raylene Rodrigues de; AUFIERO, Mário Jumbo Miranda; AGUIAR, Kenny Rebouças de; SIMAS, Danielle Costa de Souza. O impacto da inteligência artificial generativa na sofisticação de fraudes e golpes online com uso de deepfakes no Brasil. **Revista DCS**, *[S. l.]*, v. 22, n. 84, p. e3604, 2025. DOI: 10.54899/dcs.v22i84.3604. Disponível em: https://ojs.revistadcs.com/index.php/revista/article/view/3604. Acesso em: 11dez. 2025.

TRANSUNION. Relatório de Tendências de Fraude Omnichannel 2025. **TransUnion**, 2025, online. Disponivel em: https://www.transunion.com.br/report/fraude-report-h1-2025. Acesso em: 13 nov. 2025.

TUBINO, E. R. R; KAZIENKO, J. F. **Um Estudo Acerca das Fraudes na Comunicação por Campo de Proximidade**. In: X Workshop de Trabalhos de Iniciação Científica e de Graduação (WTICG), 2016, Niterói, Brasil. XVI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg'16), 2016. p.586-596. Disponível em: http://sbseg2016.ic.uff.br/pt/files/anais/wticg/ST3-3.pdf. Acesso em: 05 nov. 2025.