

92. DO PAPEL À TELA: A TRANSFORMAÇÃO DO ESTELIONATO COM O AVANÇO DA TECNOLOGIA

Camila Virissimo Rodrigues da Silva Moreira

Mestra em Ciências Jurídicas, UniCesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0000-3911-9699>

<https://lattes.cnpq.br/8591500782530359>

camila.moreira@docentes.unicesumar.edu.br

Isadora Campos Cartapati

Acadêmica, UniCesumar

Maringá – Paraná - Brasil

<https://orcid.org/0000-0002-1333-1891>

ra-24191523-2@alunos.unicesumar.edu.br

Gabriela Christina Ramos

Acadêmica, UniCesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0003-4181-9530>

ra-23297900-2@alunos.unicesumar.edu.br

Murilo Rocha Ferrarezi

Acadêmico, UniCesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0003-4792-5385>

ra-24444254-2@unicesumar.edu.br

RESUMO

O estelionato é um crime previsto no artigo 171 do Código Penal Brasileiro e ele acontece quando alguém engana outra pessoa com o objetivo de obter vantagem indevida. Com o crescimento do uso da internet e das tecnologias digitais, esse tipo de golpe se adaptou ao ambiente virtual, passando a ser praticado com técnicas de manipulação psicológicas e sociais que confundem e convencem as vítimas com facilidade. É comum que os golpistas ofereçam produtos com preços abaixo do normal, criem boletos falsos, enviem mensagens de cobranças indevidas ou até usem mentiras, como bloqueio de cartões, para conseguir dados bancários. A pena prevista em lei pode chegar a oito anos, principalmente quando o crime acontece por meios eletrônicos. Além das sanções penais, também existe a possibilidade de indenização pelas perdas causadas. Este artigo analisa como o estelionato virtual tem se manifestado no Brasil, tendo como objeto os golpes mais comuns, e apresenta possíveis soluções para aumentar a segurança digital, com base em estudos, reportagens e dados recentes sobre o tema. A metodologia utilizada é documental, dedutiva e de revisão bibliográfica. Os resultados esperados incluem analisar os principais padrões de golpe, facilitar a identificação das vulnerabilidades mais comuns e buscar soluções ou aprimoramento de segurança para os usuários das tecnologias digitais.

PALAVRAS-CHAVE: Código penal. Golpes virtuais. Transgressão digital.

ABSTRACT

Fraud is a crime defined in Article 171 of the Brazilian Criminal Code and occurs when an individual deceives another person with the intent of obtaining an unlawful advantage. With the increasing use of the internet and digital technologies, this type of scam has adapted to the virtual environment, being carried out through psychological and social manipulation techniques that easily confuse and persuade victims. It is common for scammers to offer products at unusually low prices, create fake payment slips, send false billing messages, or use fabricated situations—such as blocked bank cards—to obtain banking information. The penalty established by law may reach up to eight years of imprisonment, especially when the crime is committed through electronic means. In addition to criminal sanctions, victims may also seek compensation for the losses incurred.

This article analyzes how online fraud has manifested in Brazil, focusing on the most common types of scams and presenting possible solutions to enhance digital security, based on studies, reports, and recent data on the subject. The methodology used is documentary, deductive, and based on bibliographic review. The

expected results include identifying the main scam patterns, facilitating the detection of common vulnerabilities, and seeking solutions or security improvements for users of digital technologies.

KEYWORDS: Criminal Code. Online fraud. Digital transgression.

1 INTRODUÇÃO

Nos últimos anos, é cada vez mais comum ouvir relatos de pessoas que caíram em golpes pela internet. Em 2023, por exemplo, foram registrados cerca de 1,9 milhão de casos no Brasil, resultando em uma média de um golpe a cada 16 segundos. Tal média é, de certa forma, bem alarmante tendo em vista que vivemos imersos nesse mundo digital. Não é à toa que vemos tantos casos de estelionato online nas notícias, além dos inúmeros casos que nunca chegam a ser denunciados. O crescimento é visível: o número representa um aumento de mais de 8% em relação ao ano anterior.

Já em meados de 2024, o Brasil apresentou uma taxa alarmante: 24% da população com mais de 16 anos foram vítimas de algum tipo de crime cibernético nos meses anteriores. Tal montante, totalizou cerca de 40,85 milhões de brasileiros que perderam dinheiro em razão de fraudes online, como clonagem de cartão, falsos boletos, empréstimos fraudulentos e invasões de contas bancárias (Agência Senado, 2024).

Estes golpes não apenas causam prejuízos econômicos, mas também traumas psicológicos nas vítimas, afetam sua confiança nas instituições e dificultam a recuperação dos valores perdidos. Embora o ordenamento jurídico brasileiro contemple a criminalização do estelionato por meio do artigo 171 do Código Penal, além de leis específicas como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet, essas normas têm se mostrado, em muitos casos, insuficientes para conter o crescimento das fraudes digitais.

Diante desse cenário, o presente artigo busca compreender a evolução do estelionato virtual, analisando seu contexto histórico, os principais métodos empregados pelos criminosos, os impactos sociais e jurídicos do crime, bem como propor medidas preventivas que possam auxiliar na mitigação desses riscos. Apenas por meio de uma análise crítica e aprofundada será possível compreender a dimensão do problema e apontar caminhos viáveis para a construção de uma cultura de segurança digital mais eficaz no Brasil.

2 REFERENCIAL TEÓRICO

O estelionato é um crime que surgiu na antiguidade e se transformou ao longo dos séculos, acompanhando as mudanças sociais, econômicas e tecnológicas. Em suas

primeiras manifestações, ainda na Roma Antiga, os golpistas já utilizavam artifícios para enganar e obter vantagens ilícitas. Com o crescimento do comércio durante a Idade Média, novas formas de fraude surgiram, como a falsificação de moedas e documentos. Já no período da Revolução Industrial, o aumento das transações financeiras e a falta de fiscalização deram espaço para o avanço do estelionato, um crime que se aproveitava da ignorância das vítimas em relação aos seus direitos, prejudicando o desenvolvimento econômico de diversas nações (Pasitto, 2024).

A evolução do estelionato iniciou-se com o surgimento da era digital no final do século XX. O advento da internet e das transações online criou novas oportunidades para os golpistas, que passaram a explorar falhas nos sistemas de segurança digital e a fragilidade da educação tecnológica da população. Diferente do estelionato tradicional, que tinha limitações geográficas, o estelionato digital permitiu que criminosos atuassem de qualquer lugar do mundo, dificultando a identificação e punição dos infratores. A natureza anônima da internet, somada à crescente utilização de plataformas digitais, tornou o estelionato virtual uma ameaça global (Meireles; Pasitto, 2024).

No Brasil, o estelionato tem raízes profundas, remontando ao período colonial. Durante esta época, as práticas fraudulentas eram comuns, em grande parte devido à fragilidade do sistema jurídico e da fiscalização. O Código Penal do Império, promulgado em 1830, representou um dos primeiros esforços normativos para coibir fraudes no Brasil. No entanto, foi com o Código Penal de 1940 que o crime de estelionato passou a ter definição expressa, sendo tipificado no artigo 171 como a prática de enganar alguém, mediante artifício ou ardil, com o objetivo de obter vantagem ilícita em prejuízo de outrem (Brasil, 1940). Este dispositivo permanece em vigor, embora a legislação tenha evoluído com a promulgação de novas leis, como a Lei nº 12.737/2012, também conhecida como "Lei Carolina Dieckmann", que tipifica crimes informáticos e invasão de dispositivos eletrônicos.

O estelionato no Brasil tem evoluído, especialmente com a crescente utilização de tecnologias digitais. O aumento das transações financeiras pela internet, a popularização dos sistemas de pagamento instantâneo como o PIX e o grande número de usuários de plataformas digitais tornaram o país alvo de fraudes cibernéticas. Golpes — como boletos falsos, empréstimos fraudulentos em nome de vítimas e o uso indevido de dados pessoais — são alguns dos crimes mais comuns (Meireles; Pasitto, 2024).

Um caso que ganhou destaque foi o desmantelamento de uma "escola online para estelionatários", liderada por Paulo César Gomes da Silva Dutra, conhecido como Banucha Gomes. Ele ensinava a aplicação de golpes, vendia dados pessoais e oferecia contas bancárias por meio de um site ilegal, atingindo mais de 50 mil pessoas e causando a clonagem de mais de 10 mil cartões de crédito (G1, 2025).

Além da legislação já existente, o governo brasileiro tem tomado medidas para combater as fraudes digitais. Em 2025, o Ministério da Justiça e a Febraban lançaram a Aliança Nacional de Combate a Fraudes Digitais, visando unir forças entre bancos, empresas de tecnologia e órgãos públicos para fortalecer a segurança digital. Além disso, o Serpro tem colaborado com a criação de ferramentas de segurança para prevenir golpes (Brasil, 2025). Tais iniciativas são fundamentais, uma vez que o estelionato digital afeta, com maior intensidade, as populações mais vulneráveis, que têm menor acesso à educação financeira e à informação sobre segurança digital. O despreparo dessas pessoas as torna alvo fácil para promotores de golpes, como empréstimos falsos ou promoções enganosas (Meireles; Pasitto, 2024).

Na cultura midiática, a série Vinagre de Maçã exemplifica bem como a manipulação de informações e a construção de uma imagem pública podem ser usadas para aplicar estelionatos. A personagem principal, Belle Gibson, cria uma narrativa falsa sobre sua cura de um câncer terminal com terapias alternativas, enganando milhares de seguidores e obtendo lucros através de um aplicativo e de um livro. Seu caso reflete um tipo de estelionato digital em que a confiança é explorada, e a manipulação de imagens e informações no ambiente online facilita a fraude (G1, 2025).

Em termos de prevenção, é essencial que os indivíduos adotem práticas de segurança digital — como o uso de senhas fortes, a ativação da verificação em duas etapas e a manutenção de sistemas atualizados. Além disso, a conscientização sobre os riscos e as técnicas utilizadas pelos golpistas deve ser incentivada para reduzir as chances de cair em fraudes. O governo e as empresas também devem continuar seus esforços para proteger os cidadãos, especialmente por meio da educação digital e do desenvolvimento de novas ferramentas de segurança (Brasil, 2022).

Portanto, o estelionato digital é um fenômeno complexo, que reflete a interseção entre fraudes tradicionais e a inovação tecnológica. Ele não só aproveita a vulnerabilidade das pessoas em um novo ambiente, mas também intensifica as desigualdades sociais e econômicas existentes. Combater esse tipo de crime exige uma ação conjunta de cidadãos,

empresas e governo, com foco na educação e na criação de sistemas mais seguros e eficientes.

3 METODOLOGIA

Este trabalho foi desenvolvido por meio de uma pesquisa qualitativa de caráter exploratório, com foco na análise do estelionato em sua trajetória histórica e nas suas transformações no ambiente digital, especialmente no contexto brasileiro. Para isso, foi adotada a técnica de pesquisa bibliográfica e documental, com base em fontes oficiais, artigos científicos, leis e reportagens.

A revisão bibliográfica concentrou-se em estudos acadêmicos que abordam o tema das fraudes e golpes virtuais, como os trabalhos de Meireles e Pasitto (2024), que discutem o crescimento dos crimes digitais e seus impactos sociais. Esses autores foram fundamentais para compreender o contexto atual do estelionato digital e os desafios enfrentados pelas autoridades e pela população.

No campo jurídico, analisaram-se documentos legais que tratam do estelionato no Brasil, especialmente o artigo 171 do Código Penal (Brasil, 1940) e a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que trata da invasão de dispositivos eletrônicos. Essas normativas foram estudadas para compreender os mecanismos legais existentes e suas limitações diante da evolução tecnológica.

Além disso, utilizou-se análise de conteúdo a partir de fontes jornalísticas atualizadas, como reportagens do G1 (2025) e da CNN Brasil (Marzolla, 2024), que apresentaram casos reais e dados estatísticos sobre fraudes no país. A operação que desmantelou uma “escola online para estelionatários”, por exemplo, foi estudada como um caso emblemático que ilustra o avanço do crime digital.

Também foram consideradas informações institucionais, como os relatórios do Ministério da Justiça e da Febraban sobre a Aliança Nacional de Combate a Fraudes Digitais (Brasil, 2025), além da atuação do Serpro em ações de prevenção. Esses dados forneceram suporte para entender os esforços governamentais e privados na tentativa de conter os crimes cibernéticos.

Complementarmente, utilizou-se a análise midiática da série “Vinagre de Maçã”, baseada em fatos reais, como recurso para refletir sobre a manipulação da confiança no ambiente digital. A representação cultural do estelionato auxilia a compreender como a fraude se perpetua com o uso da imagem pública nas redes sociais.

Assim, a metodologia adotada possibilitou uma abordagem ampla e interdisciplinar, articulando dados históricos, legais, jornalísticos e culturais para entender o estelionato como um fenômeno complexo e em constante transformação.

4 RESULTADOS ESPERADOS

A partir da análise apresentada, espera-se como resultado principal a ampliação da compreensão sobre a evolução do crime de estelionato, especialmente no contexto digital contemporâneo. O estudo demonstra que o estelionato, embora antigo, se adaptou às transformações tecnológicas e sociais, assumindo novas formas e alcançando um número crescente de vítimas por meio da internet. A abordagem histórica permitiu identificar como o crime evoluiu desde práticas rudimentares de fraude na Antiguidade até chegar aos sofisticados golpes digitais da atualidade.

Um dos resultados alcançados com esta investigação é o reconhecimento da vulnerabilidade da população diante dos crimes cibernéticos, especialmente as camadas sociais com menor acesso à informação e à educação digital. Como apontado por Meireles e Pasitto (2024), os golpes mais comuns são direcionados a essas populações, que muitas vezes não possuem conhecimento técnico para identificar tentativas de fraudes, como boletos falsos, links maliciosos e propostas financeiras enganosas. Essa constatação evidencia a urgência de ações educativas e preventivas que incluam toda a sociedade.

Outro resultado importante é a identificação da ineficiência parcial das medidas legislativas diante da rapidez com que os crimes digitais evoluem. Apesar da existência de normas como o artigo 171 do Código Penal (Brasil, 1940) e da Lei nº 12.737/2012 (Lei Carolina Dieckmann), os criminosos se aperfeiçoam continuamente, dificultando o acompanhamento por parte do poder público. A análise dos marcos legais mostra que, embora essenciais, as leis precisam ser constantemente atualizadas e complementadas por ações integradas entre governo, empresas e sociedade civil.

Também se destaca como resultado alcançado a valorização das medidas preventivas e da colaboração institucional como ferramentas indispensáveis para o enfrentamento do estelionato digital. A criação da Aliança Nacional de Combate a Fraudes Digitais, mencionada pela Agência Brasil (2025), representa um avanço significativo, pois mostra o esforço conjunto de órgãos públicos e privados na tentativa de mitigar os prejuízos causados por fraudes. A atuação do Serpro, com o desenvolvimento de ferramentas de

segurança e orientação para vítimas, reforça a importância da tecnologia no combate ao crime.

Por fim, espera-se que este estudo contribua para a conscientização sobre os riscos do ambiente digital e para a formação de uma cultura de segurança cibernética. A partir da compreensão das estratégias usadas pelos golpistas, como exemplificado no caso da série Vinagre de Maçã e na operação que desmantelou a escola virtual de estelionatários (G1, 2025), é possível fomentar um comportamento mais cauteloso e crítico por parte dos usuários da internet. A meta é que, com mais informação e preparo, o número de vítimas seja reduzido, fortalecendo a confiança no uso de tecnologias e promovendo uma sociedade mais segura digitalmente.

REFERÊNCIAS

AGÊNCIA SENADO. Golpes digitais atingem 24% da população brasileira, revela DataSenado. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado>. Acesso em: 19 abr. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 15 abr. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União: seção 1, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 abr. 2025.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. MJSP e Febraban lançam Aliança Nacional de Combate a Fraudes Digitais. Agência Brasil, 21 fev. 2025. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2025-02/ministerio-da-justica-e-febraban-lancam-alianca-contra-fraude-digital>. Acesso em: 19 abr. 2025.

BRASIL. GOVERNO FEDERAL. Plano Tático de Combate a Crimes Cibernéticos é lançado pelo Governo Federal. Brasília: Ministério da Justiça e Segurança Pública, 9 mar. 2022. Disponível em: <https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos>. Acesso em: 19 abr. 2025.

CNN BRASIL. MARZOLLA, Isabella. Tentativas de fraude já somam R\$ 1,2 bi em 2024; veja data, hora e alvos preferidos de golpistas. 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/ten-tativas-de-fraude-ja-somam-r-12-bi-em-2024-veja-data-hora-e-alvos-preferidos-de-golpistas/>. Acesso em: 19 abr. 2025.

G1. Escola do crime: a operação que desmontou um curso online para aplicar golpes. G1, 2025. Disponível em: <https://g1.globo.com/fantastico/noticia/2025/01/05/escola-do-crime-a-operacao-que-desmontou-um-curso-online-para-aplicar-golpes.ghtml>. Acesso em: 19 abr. 2025.

MEIRELES, Isys Gonzaga; PASITTO, Fernando Teles. Estelionato e suas implicações: o constante crescimento dos golpes virtuais. Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, São Paulo, v. 10, n. 3, p. 1-15, 2024. Disponível em: [https://periodicorease.pro.br/rease/](https://periodicorease.pro.br/rease/article/view/17063/9525) article/view/17063/9525. Acesso em: 19 abr. 2025.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (Serpro). Serpro integra Aliança Nacional de Combate a Fraudes Digitais. Brasília, 22 fev. 2025. Disponível em: [https://www.serpro.gov.br/](https://www.serpro.gov.br/menu/noticias/noticias-2025/serpro-integra-alianca-nacional-combate-fraudes-digitais) menu/noticias/noticias-2025/serpro-integra-alianca-nacional-combate-fraudes-digitais. Acesso em: 19 abr. 2025.

NETFLIX. Vinagre de Maçã. Direção: Jeffrey Walker. Produção: Netflix, 6 fev. 2025. Série baseada em fatos reais. Disponível em: <https://www.netflix.com>. Acesso em: 19 abr. 2025.