doi.org/10.51891/rease.v10i11.17063

# ESTELIONATO E SUAS IMPLICAÇÕES: O CONSTANTE CRESCIMENTO DOS GOLPES VIRTUAIS[I]

**Isys Gonzaga Meireles**[1]
**Fernando Teles Pasitto**[2]

RESUMO: Sabe-se que o crime de estelionato tipificado no artigo 171 do Código Penal Brasileiro é uma prática fraudulenta que visa a obtenção de vantagem ilícita, mediante dolo ou manipulação, em prejuízo de outra pessoa, e com o avanço da tecnologia e a popularização da internet, o estelionato passou a ser praticado em ambiente virtual, o que torna mais complexa sua detecção e investigação. O problema a ser enfrentado no presente trabalho é saber quais são as dificuldades em comater e prevenir eficazmente as modalidades de estelionato virtual? Como objetivo geral analisar o crime de estelionato, com ênfase em suas manifestações na era digital e nas modalidades virtuais dessa infração. Os objetivos específicos estão voltados em identificar as principais formas de estelionato digital no Brasil, como golpes relacionados ao sistema de pagamento instantâneo PIX, falsificação de boletos bancários e falsas promessas de empréstimo, avaliar as implicações sociais e econômicas desses crimes e examinar as políticas públicas e a legislação vigente que versam sobre essas práticas, bem como investigar as principais modalidades de estelionato virtual, com foco na análise dos golpes mais frequentes e suas consequências.. A pesquisa se justifica pela necessidade de compreender melhor as modalidades de estelionato digital e buscar soluções para minimizar o impacto desse tipo de crime, que afeta tanto os indivíduos quanto o setor econômico de maneira ampla. As implicações sociais e econômicas do estelionato digital são significativas, gerando prejuízos financeiros e emocionais às vítimas, além de impactar a confiança nas transações digitais e no comércio eletrônico. A desconfiança gerada por esses crimes pode retardar a adoção de novas tecnologias financeiras e inibir a inovação no setor. A metodologia utilizada é de natureza bibliográfica e documental, incluindo a análise de artigos acadêmicos, relatórios de órgãos especializados em segurança digital e documentos jurídicos. A pesquisa apresenta também um panorama das políticas públicas e das legislações em vigor no Brasil, destacando os desafios na implementação dessas medidas. O estudo conclui que o combate ao estelionato digital no Brasil requer um esforço conjunto entre sociedade, setor privado e poder público. Medidas como a educação digital da população, a implementação de tecnologias de segurança avançadas nas transações online e o fortalecimento das leis de crimes cibernéticos são essenciais para reduzir a incidência desses delitos. A cooperação internacional é igualmente importante, pois muitos crimes virtuais são transnacionais, dificultando a investigação e a responsabilização dos autores. Por fim, o trabalho enfatiza a necessidade de uma maior conscientização da população sobre os riscos das transações digitais e as melhores práticas de segurança para prevenir golpes virtuais.

**Palavras-chave:** Estelionato digital. Crimes virtuais. Segurança cibernética.



[1]Graduanda no curso de direito, Faculdade de Ciências Sociais Aplicadas – FACISA.
[2]Mestre em Educação, Gestão e Desenvolvimento Sustentável pela Faculdade Vale do Cricaré. Coordenador do Curso de Direito e Docente na Faculdade de Ciências Sociais Aplicadas - FACISA.

## 1. INTRODUÇÃO

O estelionato, previsto no artigo 171 do Código Penal Brasileiro, é caracterizado como um crime em que o agente obtém, para si ou para outrem, vantagem ilícita, em prejuízo alheio, mediante artifício, ardil ou outro meio fraudulento (BRASIL, 1940). Na era contemporânea esse crime adotou novas soluções com o uso crescente de tecnologias digitais, que permitem aos criminosos novas maneiras de enganar suas vítimas. Essa interação, amplamente conhecida como estelionato virtual, é facilitada pela ampla conectividade, permitindo que os infratores explorem vulnerabilidades em sistemas de comunicação e transação digital (Morais, 2020).

A popularização do uso da internet no Brasil, somada ao aumento das transações financeiras digitais, possibilitou um crescimento significativo dos crimes cibernéticos. Segundo Diniz (2022), os golpes virtuais tornaram-se uma das principais formas de estelionato no país, com destaque para fraudes envolvendo o sistema de pagamento instantâneo (PIX), boletos falsificados e falsas promessas de empréstimos  são realizados com uma sofisticação crescente, utilizando-se de métodos avançados, como o phishing, engenharia social e técnicas de invasão de sistemas, o que torna sua detecção e combate um grande desafio para as autoridades (Henriques, 2024).



A relevância do tema é evidente quando se observam os impactos sociais e econômicos causados pelos golpes virtuais, as vítimas enfrentam tanto os prejuízos financeiros quanto os traumas emocionais, perda de confiança nas instituições bancárias e o receio de utilizar serviços digitais. De acordo com Lacerda (2022), as fraudes digitais afetam profundamente a vida das vítimas, que muitas vezes não conseguem recuperar os valores perdidos e enfrentam um longo processo de reestruturação emocional e financeira. Esse cenário é agravado pela rapidez com que as fraudes são aplicadas e pela dificuldade de rastreamento dos autores, que muitas vezes se aproveitam do anonimato fornecido pela internet (De Oliveira, 2024).

Sob essa perspectiva, o presente trabalho concentra-se em responder ao seguinte questionamento: quais são as dificuldades em combater e prevenir eficazmente as modalidades de estelionato virtual?

O objetivo geral propõe-se em analisar o crime de estelionato, com ênfase em suas manifestações na era digital e nas modalidades virtuais dessa infração. Os objetivos específicos estão voltados em identificar as principais formas de estelionato digital no Brasil, como golpes relacionados ao sistema de pagamento instantâneo PIX, falsificação de boletos bancários e falsas promessas de empréstimo, avaliar as implicações sociais e econômicas desses crimes e

examinar as políticas públicas e a legislação vigente que versam sobre essas práticas, bem como investigar as principais modalidades de estelionato virtual, com foco na análise dos golpes mais frequentes e suas consequências.

A literatura indica que os crimes cibernéticos evoluem na mesma velocidade das tecnologias, o que exige das autoridades uma adaptação contínua nas estratégias de prevenção e combate. Conforme destaca Burrowes (2017), "o combate ao crime digital requer não apenas uma legislação atualizada, mas também uma conscientização massiva da população quanto aos riscos do ambiente virtual".

A cibernética no Brasil tem avançado lentamente, e ainda são grandes os esforços de segurança necessários para que as medidas de proteção sejam amplamente aplicadas. Em termos legais, o Brasil possui uma legislação que tipifica crimes cibernéticos, como o Marco Civil da Internet e a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que trata da invasão de dispositivos informáticos (BRASIL, 2012). Entretanto, a legislação atual não tem sido suficiente para conter o crescimento das fraudes digitais devido à sua complexidade e às limitações na aplicação prática (Henriques, 2024).

Diante dessa problemática, o presente artigo se justifica pela necessidade de se compreender a evolução das práticas de estelionato na era digital, contribuindo para o desenvolvimento de medidas preventivas mais eficazes. Uma análise crítica das fraudes virtuais e seus impactos permitirá uma compreensão mais profunda das vulnerabilidades do ambiente digital e dos mecanismos que podem ser implementados para mitigar esses riscos. Além disso, o estudo busca alertar para a importância de políticas públicas e campanhas educativas que orientem a população quanto aos cuidados necessários ao realizar transações online.



Portanto, o objetivo principal deste artigo é analisar as modalidades de estelionato virtual no Brasil, identificando os métodos mais utilizados pelos criminosos e propondo soluções para aumentar a segurança digital. O estudo se baseia em dados secundários, orientações de bibliografia especializada e relatórios sobre segurança cibernética, além de estudos acadêmicos que tratam do impacto econômico e social desses crimes. Espera-se que as instruções aqui apresentadas possam contribuir para o fortalecimento das medidas de combate ao estelionato digital e para a construção de uma cultura de segurança digital no Brasil.

Por fim, ao compreender a sofisticação crescente dos golpes virtuais e o impacto devastador nas vítimas, torna-se urgente que a sociedade, as empresas e as autoridades brasileiras unam esforços para promover um ambiente digital mais seguro. A análise dos dados

disponíveis, em conjunto com as legislações já existentes, pode fornecer um panorama mais claro sobre os desafios enfrentados e as soluções possíveis para mitigar o avanço desse tipo de crime.

## 2. METODOLOGIA

Este estudo utiliza uma abordagem qualitativa e quantitativa, descrita como uma pesquisa descritiva e exploratória. A pesquisa descritiva tem como objetivo principal fornecer uma visão detalhada sobre as especificações do estelionato virtual, analisando suas implicações jurídicas, sociais e econômicas. Por sua vez, a pesquisa exploratória busca identificar as tendências e os padrões nos crimes digitais, particularmente no contexto brasileiro, a fim de propor estratégias de prevenção e combate eficazes.

A metodologia empregada neste trabalho é de natureza bibliográfica e documental. Segundo Gil (2008), a pesquisa bibliográfica "é desenvolvida com base em material já elaborado, constituída principalmente de livros e artigos científicos" (Gil, 2008, p. 50). Assim, uma revisão da literatura constitui a base deste estudo, sendo utilizadas fontes secundárias que tratam do estelionato virtual, da legislação penal brasileira e das tecnologias relacionadas à segurança digital.



A pesquisa documental complementa a revisão bibliográfica por meio da análise de relatórios de órgãos governamentais e não governamentais, como o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), além de dados disponíveis em artigos científicos, publicações de institutos de segurança digital e relatórios de segurança cibernética. Esses documentos fornecem informações sobre o número de incidentes de fraudes digitais, as metodologias utilizadas pelos crimes e as principais estratégias de prevenção adotadas por diferentes países.

Para a coleta de dados, foram consultadas bases de dados como Scielo , Google Acadêmico e Portal de Periódicos da CAPES . A seleção das fontes se deu pelo especializado de relevância ao tema do estelionato digital, priorizando estudos realizados nos últimos dez anos, período no qual houve uma intensificação das fraudes virtuais devido ao aumento do uso de plataformas digitais de pagamento e serviços online no Brasil. Segundo Prodanov e Freitas (2013), uma pesquisa bibliográfica permite "identificar, coletar, selecionar e interpretar criticamente as fontes" que fundamentam o estudo e dão suporte ao teórico (Prodanov; Freitas, 2013, p. 29).

A análise dos dados foi feita de forma qualitativa, considerando as implicações sociais, econômicas e jurídicas do estelionato virtual. Para isso, as informações coletadas foram agrupadas em categorias temáticas, tais como: tipos de golpes virtuais, impacto financeiro nas vítimas, respostas legais ao crime cibernético e estratégias de prevenção. De acordo com Bardin (2011), a análise de conteúdo é uma técnica que permite interpretar dados a partir de uma organização prévia em categorias e permite compreender as dinâmicas subjacentes ao treinamento.

O estudo limita-se ao cenário brasileiro, mas faz comparações com outros países sempre que necessário para compreender as práticas internacionais no combate aos crimes cibernéticos. Essa perspectiva comparativa busca identificar quais políticas públicas e medidas de segurança cibernética poderiam ser adaptadas ao contexto brasileiro para aumentar a eficácia no combate ao estelionato virtual. Além disso, considera-se a legislação vigente no Brasil, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 12.737/2012, que tipifica crimes relacionados ao uso de dispositivos informáticos.

Portanto, a metodologia proposta visa fornecer uma compreensão abrangente e detalhada do estelionato digital no Brasil, contribuindo com informações relevantes para a elaboração de estratégias de combate a esse crime. O uso de fontes bibliográficas e documentais, bem como uma análise qualitativa dos dados, permite uma abordagem robusta e bem fundamentada, adequada ao objetivo deste estudo.



## 3. A FRAUDE DO SÉCULO E SEU HISTÓRICO MUNDIAL

O estelionato é uma das fraudes mais antigas da história, adaptando-se às transformações sociais e econômicas ao longo dos séculos. Sua prática remonta à Antiguidade, quando já se observavam registros de ações fraudulentas em sociedades como a romana, em que se utilizavam artifícios para enganar e obter vantagens ilícitas sobre terceiros (Diniz, 2022). O desenvolvimento do comércio e das transações financeiras na Idade Média também impulsionou novas formas de estelionato, com a falsificação de moedas e documentos sendo uma prática comum (Morais, 2020).

Com o passar dos séculos, o estelionato se moldou conforme as inovações tecnológicas e as mudanças nos padrões econômicos. Durante a Revolução Industrial, com a supervisão das empresas e a intensificação do comércio internacional, novas modalidades de fraude surgiram, muitas vezes explorando a falta de regulamentação econômica e o desconhecimento das leis

comerciais por parte da população (Carvalho, 2006). Esses fatores tornaram o estelionato uma prática ainda mais comum, impactando fortemente o desenvolvimento econômico de várias nações.

No século XX, com o advento dos sistemas bancários mais complexos e o surgimento das bolsas de valores, as fraudes financeiras sofisticaram-se ainda mais. Esquemas de pirâmide, falsificação de identidades e documentos, além de golpes que exploraram brechas no sistema financeiro, tornaram-se uma preocupação global. Nomes como Charles Ponzi e Bernie Madoff ficaram conhecidos por arquitetar esquemas de estelionato em larga escala, que prejudicaram milhares de pessoas e instituições financeiras ao redor do mundo (Burrowes, 2017).

O surgimento da era digital, no final do século XX e início do século XXI, trouxe uma nova dimensão para o estelionato, com a emergência de golpes virtuais. Com a massificação da internet e o aumento das transações online, os estelionatários passaram a utilizar técnicas mais sofisticadas, explorando a vulnerabilidade dos sistemas de segurança digital e a falta de preparo da população para lidar com a nova realidade tecnológica. O estelionato virtual, marcado por ataques de phishing, ransomware e outras práticas de engenharia social, tornou-se um problema de segurança cibernética em escala global (De Oliveira, 2024).



A característica mais preocupante do estelionato virtual é sua capacidade de transcender fronteiras. Diferentemente das fraudes tradicionais, que geralmente eram restritas a uma localidade ou região, o crime cibernético pode ser perpetrado em qualquer lugar do mundo, dificultando a identificação dos infratores e a aplicação da lei. A internet oferece um ambiente anônimo, no qual os criminosos podem operar com relativa impunidade, ou que desafiam autoridades em todo o mundo a desenvolver novas estratégias de combate (Carvalho, 2006).

No contexto global, organizações como a Interpol e a Europol desempenham papéis fundamentais na cooperação internacional para combater as fraudes digitais. No entanto, o crescimento exponencial das transações digitais e a conectividade global ampliaram o alcance dos golpes, exigindo uma cooperação cada vez mais eficaz entre governos e empresas de tecnologia (Lacerda, 2022). Medidas como a padronização de normas de segurança cibernética, o fortalecimento das leis de proteção de dados e a promoção de campanhas educativas voltadas à conscientização digital são essenciais para mitigar o avanço do estelionato na era digital.

O estelionato, portanto, percorreu uma longa trajetória histórica, adaptando-se às diferentes formas de interação social e econômica. De fraudes simples cometidas em feiras comerciais a esquemas complexos que envolvem tecnologia de ponta, o crime continua a

evoluir, representando um desafio persistente para as sociedades modernas. Compreender essa evolução é essencial para a criação de políticas de prevenção e combate eficazes, que possam responder de maneira adequada às novas modalidades de estelionato que surgem com o avanço tecnológico.

## 4. ESTELIONATO E SEU HISTÓRICO NACIONAL

No Brasil, o crime de estelionato tem raízes profundas, refletindo as particularidades da evolução social, econômica e jurídica do país. Desde o período colonial, quando o sistema jurídico brasileiro ainda se baseava nas Ordenações do Reino de Portugal, já havia relatos de fraudes envolvendo falsificação de documentos e práticas enganosas em transações comerciais (Carvalho, 2006). Nessa época, a baixa fiscalização e a fragilidade das estruturas administrativas facilitavam a atuação de indivíduos que se aproveitavam da ignorância alheia para obter benefícios ilícitos.

Com a independência do Brasil, em 1822, e a posterior promulgação do Código Penal do Império em 1830, as primeiras tipificações criminais relacionadas ao estelionato surgiram a surgir. No entanto, apenas com a modernização do sistema jurídico brasileiro, a partir da segunda metade do século XIX, as práticas fraudulentas passaram a receber maior atenção do Estado. O desenvolvimento do comércio e o aumento das transações financeiras geraram a necessidade de legislações mais rigorosas que visassem coibir o estelionato e outros crimes contra a propriedade (BRASIL, 1940).



Ao longo do século XX, o estelionato no Brasil foi ganhando novas formas, refletindo as mudanças socioeconômicas vividas pelo país. O processo de urbanização e a expansão do sistema financeiro possibilitaram o surgimento de fraudes mais elaboradas, muitas delas envolvendo esquemas de pirâmide e falsificação de cheques. Com o fortalecimento do setor bancário e o aumento do crédito, as fraudes financeiras se tornaram mais sofisticadas e mais difíceis de serem detectadas (Morais, 2020).

O Código Penal de 1940, que vigora até os dias de hoje, consolidou o estelionato como crime em seu artigo 171. Esse dispositivo legal abrange uma variedade de condutas fraudulentas, definindo o estelionato como "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante planejamento, ardil ou qualquer outro meio fraudulento" (BRASIL, 1940). Essa definição é ampla e contempla diversas

modalidades de fraude, adaptando-se às mudanças tecnológicas e às novas práticas criminosas que surgiram nas décadas subsequentes.

Com o advento da era digital e a popularização da internet, o estelionato no Brasil passou a se manifestar principalmente em ambiente virtual, dando origem a novas modalidades de golpes. O país, que tem uma das maiores populações de usuários da internet no mundo, também enfrentou uma crescente incidência de fraudes digitais, como golpes envolvendo transferências bancárias, compras fraudulentas e uso indevido de dados pessoais (Diniz, 2022). Entre os golpes mais comuns estão os boletos bancários falsos, as promessas de empréstimos sem consulta ao nome do consumidor e o uso indevido do sistema de pagamentos instantâneos, como o PIX.

Essas novas formas de estelionato digital são reflexo do crescimento das transações financeiras online e da inclusão digital acelerada, especialmente nos últimos anos. O cenário nacional apresenta desafios importantes para as autoridades, uma vez que o anonimato fornecido pelo ambiente virtual dificulta a identificação e a segurança dos infratores. Apesar da criação de legislações específicas, como a Lei Carolina Dieckmann (Lei nº 12.737/2012), que tipifica crimes relacionados ao uso de dispositivos informáticos, o combate ao estelionato digital ainda é insuficiente frente à crescente sofisticação dos métodos utilizados pelos criminosos (BRASIL, 2012).



Além das dificuldades operacionais para a detecção e proteção dos crimes, o estelionato no Brasil está diretamente relacionado a questões socioeconômicas. As fraudes, em grande parte, exploram a vulnerabilidade das camadas mais pobres da população, que muitas vezes são atraídas por promessas de vantagens rápidas e simples, como os falsos empréstimos ou promoções que exigem pagamento antecipado. A falta de educação financeira e de conhecimento sobre segurança digital torna essas pessoas alvos simples para os estelionatários (Henriques, 2024).

A história do estelionato no Brasil acompanha as transformações sociais e econômicas do país, adaptando-se às novas realidades. O crescimento das fraudes digitais no cenário contemporâneo reforça a necessidade de aprimorar as medidas de prevenção e combate a esses crimes, tanto por meio do fortalecimento da legislação quanto pela promoção de uma maior conscientização sobre os riscos das transações online. O país continua a enfrentar grandes desafios no enfrentamento ao estelionato, principalmente no que se refere à eficácia dos crimes e à proteção das vítimas.

### 4.1. Conceituação de estelionato

O crime de estelionato está previsto no artigo 171 do Código Penal Brasileiro, sendo definido como a obtenção de vantagem ilícita, em prejuízo de outra pessoa, mediante fraude ou ardil, induzindo ou mantendo a vítima em erro (BRASIL, 1940). A fraude, nesse contexto, é o principal elemento do crime, pois envolve o uso de mentiras, mentiras ou omissões que visam enganar a vítima, de modo que ela realize um ato que lhe traga prejuízos financeiros ou patrimoniais. O estelionato distingue-se de outros crimes patrimoniais, como o roubo ou o furto, justamente por envolver a cooperação involuntária da vítima, que acredita ser patrocinado de forma legítima.

Tradicionalmente, o estelionato era associado a práticas fraudulentas presenciais, como a falsificação de documentos, a aplicação de golpes comerciais ou a simulação de contratos. No entanto, com o desenvolvimento das tecnologias da informação e a digitalização das relações comerciais e sociais, o estelionato passou a ser praticado também no ambiente virtual. O estelionato digital caracteriza-se por golpes que utilizam a internet ou outros meios eletrônicos para enganar as vítimas, geralmente em transações comerciais ou bancárias (Diniz, 2022).

Uma das principais características do estelionato digital é a facilidade com que as identidades dos infratores podem ocultar sua origem de suas atividades ilícitas, utilizando-se do anonimato e da vasta rede de contatos fornecidos pela internet. Isso dificulta a investigação e a identificação dos responsáveis, além de criar um ambiente propício para a prática recorrente desse tipo de crime (De Oliveira, 2024). O advento de novas ferramentas tecnológicas, como o uso de criptomoedas e plataformas digitais de pagamento, também trouxe desafios adicionais para o combate ao estelionato, uma vez que essas inovações são frequentemente exploradas pelos criminosos para dificultar o rastreamento das transações.



Assim, a conceituação de estelionato, embora ancorada em fundamentos legais clássicos, foi ampliada na era digital, exigindo novas formas de interpretação e aplicação da lei. A adaptação da legislação e das práticas investigativas ao ambiente digital tornou-se essencial para garantir a eficácia dos estelionatários, principalmente em face da crescente sofisticação dos métodos empregados nas fraudes digitais (Carvalho, 2006).

## 5. IMPLICAÇÕES SOCIAIS E ECONÔMICAS

As implicações sociais e econômicas do estelionato, especialmente em sua forma digital, são profundas e amplamente divulgadas. No plano econômico, as fraudes afetam tanto os

indivíduos quanto as empresas, gerando prejuízos que podem comprometer a estabilidade financeira das vítimas. No Brasil, estima-se que o estelionato digital tenha causado perdas de milhões de reais nos últimos anos, principalmente por meio de golpes envolvendo boletos falsos, transferências fraudulentas pelo sistema PIX e compras online não autorizadas (Morais, 2020).

Além do impacto financeiro imediato, o estelionato digital provoca uma desconfiança generalizada nas transações realizadas pela internet. As vítimas de golpes muitas vezes evitam realizar novas compras online ou utilizar serviços digitais, o que acaba impactando melhorias o comércio eletrônico e outros setores da economia digital. Essa desconfiança também pode afetar a inovação tecnológica, uma vez que o medo de ser vítima de fraude inibe a adoção de novas tecnologias financeiras e plataformas digitais (Larcerda, 2022).

No plano social, as fraudes digitais afetam a confiança entre os cidadãos e as instituições financeiras e governamentais. O impacto emocional sobre as vítimas é específico, gerando sentimentos de insegurança, impotência e vulnerabilidade. Em muitos casos, as vítimas enfrentam dificuldades para recuperar os valores perdidos, uma vez que os crimes digitais costumam atuar de forma transnacional, dificultando a atuação das autoridades locais (Costa, 2023).

Essas implicações sociais são especialmente graves em países como o Brasil, onde grande parte da população está apenas começando a ter acesso à internet e aos serviços bancários digitais. A inclusão digital, que poderia ser um fator positivo para a economia, acaba expondo novas vítimas a golpes, especialmente aqueles que têm pouco conhecimento sobre segurança digital e proteção de dados (Diniz, 2022). Portanto, as fraudes digitais não causam apenas prejuízos financeiros, mas também agravam as desigualdades sociais e tecnológicas no país.



## 6. PREVENÇÃO E COMBATE AO ESTELIONATO DIGITAL

A prevenção e o combate ao estelionato digital envolvem uma abordagem multidisciplinar, que envolve tanto a educação do público quanto o aprimoramento das ferramentas tecnológicas e jurídicas. Em termos de prevenção, é essencial que a população seja educada sobre os riscos das transações digitais e as melhores práticas de segurança online. Isso inclui a conscientização sobre o uso de senhas seguras, a verificação de ocorrências de sites e e-mails, e a adoção de mecanismos de proteção de dados, como a autenticação em dois fatores (Burrowes, 2017).

Além da educação digital, as empresas que oferecem serviços online, como plataformas

de e-commerce e bancos digitais, têm um papel fundamental na prevenção de fraudes. A implementação de tecnologias de segurança avançadas, como criptografia, monitoramento de atividades suspeitas e sistemas de inteligência artificial, pode ajudar a detectar e bloquear a tentativa de estelionato antes que causem danos aos usuários (Carvalho, 2006). As empresas também devem investir na formação contínua de seus colaboradores, especialmente aqueles envolvidos em áreas sensíveis, como atendimento ao cliente e segurança da informação.

Do ponto de vista jurídico, o Brasil já possui legislações que tipificam e regulam os crimes digitais, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Carolina Dieckmann (Lei nº 12.737/2012) (BRASIL, 2012). Contudo, é necessário fortalecer a aplicação dessas leis, garantindo que as violações digitais sejam investigadas e punidas. A cooperação internacional também é uma peça-chave no combate ao estelionato digital, visto que muitos infratores atuam fora das fronteiras nacionais, aproveitando-se das diferenças entre as legislações dos países para dificultar a sua captura (De Oliveira, 2024).

Além disso, o desenvolvimento de políticas públicas voltadas para a proteção dos consumidores digitais e a regulação de serviços financeiros virtuais é imprescindível. O Estado deve investir na capacitação de forças policiais especializadas em crimes cibernéticos e na criação de parcerias com o setor privado, a fim de promover um ambiente digital mais seguro para todos os cidadãos. Essas medidas, combinadas com a educação digital da população, são essenciais para reduzir a vulnerabilidade dos usuários às fraudes virtuais e conter o avanço do estelionato digital (Morais, 2020).



A tecnologia, embora ofereça inúmeras vantagens no âmbito das transações digitais, também expõe seus usuários às vulnerabilidades, sendo necessário um aprimoramento constante das medidas de segurança. O desenvolvimento de soluções tecnológicas robustas para proteção de dados é uma parte fundamental do combate ao estelionato digital. Entre as soluções mais eficazes estão os sistemas de monitoramento e prevenção de fraudes, que utilizam inteligência artificial para detectar padrões suspeitos de comportamento em tempo real. Esses sistemas permitem que empresas e bancos identifiquem tentativas de fraude antes que elas causem danos significativos, protegendo tanto os consumidores quanto as instituições financeiras (Carvalho, 2016).

Além das ferramentas tecnológicas, a cooperação internacional entre agências de segurança e governos é essencial para o combate ao estelionato digital, especialmente devido ao caráter transnacional de muitos desses crimes. Criminosos que operam em diferentes

jurisdições aproveitam as diferenças legais entre os países para dificultar o rastreamento e a abundância de suas atividades ilícitas. Nesse contexto, a criação de tratados e acordos internacionais que facilitam a troca de informações e a colaboração entre nações torna-se necessária. Organizações como a Interpol e a Europol desempenham um papel importante na coordenação dessas operações, mas ainda é necessário um esforço global mais coeso para enfrentar o problema em larga escala (Menezes, 2019).

Outro aspecto relevante no combate ao estelionato digital é a necessidade de atualizar constantemente as leis e regulamentações para acompanhar as rápidas mudanças tecnológicas. O Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) são exemplos de avanços importantes na legislação brasileira, mas essas normas devem ser complementadas por regulamentações específicas à proteção contra fraudes digitais. Além disso, o aprimoramento dos mecanismos de investigação digital é crucial para garantir que as violações sejam identificadas rapidamente e responsabilizadas por seus atos. A criação de delegações especializadas em crimes cibernéticos, bem como a capacitação técnica de policiais e peritos, são iniciativas que podem fortalecer a resposta do Estado a essas novas ameaças (BRASIL, 2012).

Por fim, a conscientização da população é uma das ferramentas mais poderosas na prevenção do estelionato digital. Programas educacionais que ensinam boas práticas de segurança digital, como o reconhecimento de e-mails fraudulentos, a importância de não compartilhar informações pessoais em redes não seguras e a adoção de soluções de autenticação multifator, são fundamentais para diminuir a incidência de golpes. Além disso, campanhas de conscientização pública, promovidas por governos e empresas, devem enfatizar a responsabilidade do usuário em se proteger, criando uma cultura de cibersegurança no Brasil. Essa abordagem proativa pode diminuir significativamente o número de vítimas de estelionato digital e reduzir o impacto financeiro e emocional desses crimes (Oliveira, 2018).



## 7. CONSIDERAÇÕES FINAIS

O estelionato, especialmente em sua forma digital, continua sendo um dos principais desafios para o sistema de justiça penal e para a segurança cibernética na era contemporânea, apesar dos avanços nas legislações e das iniciativas de combate, o problema não foi completamente resolvido pois a evolução tecnológica, embora tenha trazido benefícios significativos à sociedade, também ampliou as possibilidades de práticas fraudulentas, exigindo

uma resposta cada vez mais eficiente e adaptável por parte das autoridades, das instituições bancarias e financeiras e da população em geral.

O presente estudo demonstrou que o estelionato digital envolve não apenas aspectos jurídicos e econômicos, mas também sociais e psicológicos, para mitigar essa prática criminosa, são necessárias soluções integradas que incluam o fortalecimento da legislação existente e a atualização constante das normas cibernéticas.

Para diminuir a incidência dos crimes virtuais, é fundamental a promoção de educação digital da população por meio de campanhas educativas e programas de conscientização, orientando os usuários sobre os riscos das transações online e as melhores práticas de segurança.

O aprimoramento das tecnologias de segurança com investimentos em sistemas de monitoramento mais eficazes que utilizem inteligência artificial para detectar e prevenir fraudes em tempo real é fundamental, a cooperação internacional deve ser fortalecida pois a colaboração entre países para o rastreamento e a punição de criminosos que atuam de forma transnacional.

Portanto, o fortalecimento das instituições e das leis, incluindo a capacitação de profissionais para investigar crimes digitais e a aplicação rigorosa das normas existentes, é imprescindível para conter o avanço dessas práticas.



Conclui-se que embora avanços tenham sido feitos, o combate ao estelionato digital requer um esforço coordenado entre o setor público, o setor privado e a sociedade civil. Somente por meio de ações conjuntas será possível criar um ambiente digital mais seguro e resiliente, capaz de proteger as vítimas em potencial e reduzir a incidência de fraudes virtuai

## REFERÊNCIAS

BARDIN, Laurence. Análise de conteúdo. Lisboa: Edições 70, 2011.

BRASIL. Código Penal Brasileiro. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http ://www .planalto .gov .br /ccivil_03 /decreto -lei /del2848compilado .htm . Acesso em: 13 out. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: http ://www .planalto .gov .br /ccivil_03 /_ato2011 -2014 /2012 /lei /l12737 .htm . Acesso em: 13 out. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http ://www .planalto .gov .br /ccivil_03 /_ato2011 -2014 /2014 /lei /l12965 .htm . Acesso em: 13 out. 2024.

BURROWES, Frederick B. A proteção constitucional das comunicações de dados: internet, celulares e outras tecnologias. Revista Jurídica da Presidência, v. 9, n. 87, p. 09-24, 2007.

CARVALHO, M. S. R. M. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. Unpublished Estudos de Ciência e Tecnologia no Brasil, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

C. E. R. T. Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil. Cartilha de Segurança para Internet. Disponível em:< https://cartilha. cert. br/livro/> Acesso em, v. 18, 2019.

COSTA, Vanessa Barbosa; ABRANTES, Joselito Santos. A influência da Pandemia da COVID-19 nos crimes de estelionato digital ocorridos no Município de Santana-Amapá. Revista Científica Multidisciplinar do CEAP, v. 5, n. 1, 2023.

DE OLIVEIRA, Emerson Prado; DE BRITO, Pedro Lincoln Prates; JÚNIOR, Adive Cardoso Ferreira. O aumento do estelionato digital em tempos pandêmicos. Graduação em Movimento-Ciências Jurídicas, v. 3, n. 1, p. 61-61, 2024.

DINIZ, Felipe Ferreira; CARDOSO, Jacqueline Ribeiro; PUGLIA, Eduardo Henrique Pompeu. O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet. Libertas Direito, v. 3, n. 1, 2022.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 6. ed. Ediitora Atlas SA, 2008.

HENRIQUES, Thiago Alves; GONÇALVES, Samuel Martins. CRIMES DIGITAIS: análise sobre o Estelionato virtual. Revista Eletrônica de Ciências Jurídicas, v. 14, n. 1, 2024.



LACERDA, Emanoel D. Nunes. A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E A INSUFICIÊNCIA DAS LEIS NO BRASIL. Repositório Institucional do Unifip, 2022.

MENEZES, Estera Muszkat. Metodologia da pesquisa e elaboração de dissertação. São Paulo: Pioneira, 2019.

MORAES, Alexandre Rocha Almeida; SILVA, Isabella Tucci; SANTIAGO, Bruno. Os cibercrimes e a investigação digital: novos paradigmas para a persecução penal. MOMENTUM, v. 18, n. 18, 2020.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição. Editora Feevale, 2013.