



GUILHERME PORTELA CUNHA

IVES EDUARDA OLIVEIRA ARÊA LEÃO

VICENTE CARLOS SOARES FILHO

**O IMPACTO DA TECNOLOGIA DIGITAL NA PRÁTICA DO CRIME DE
ESTELIONATO**

TERESINA-PI

2025

GUILHERME PORTELA CUNHA
IVES EDUARDA OLIVEIRA ARÊA LEÃO
VICENTE CARLOS SOARES FILHO

**O IMPACTO DA TECNOLOGIA DIGITAL NA PRÁTICA DO CRIME DE
ESTELIONATO**

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Bacharel em Direito.

Orientador(a): Prof.(a) Dr(a). Jose Augusto
de Carvalho Mendes Filho

TERESINA – PI

2025

FICHA CATALOGRÁFICA

C972i Cunha, Guilherme Portela

O impacto da tecnologia digital na prática do crime de estelionato /
Guilherme Portela Cunha; Ives Eduarda Oliveira Arêa Leão; Vicente
Carlos Soares Filho – Teresina: UNINOVAFAPI, 2025.

Orientador (a): Profº. Dr. José Augusto de Carvalho Mendes Filho –
UNINOVAFAPI, 2025.

20.p.; 23cm.

Trabalho de conclusão (Graduação em Direito) – UNINOVAFAPI,
Teresina, 2025.

1. Estelionato. 2. Avanço digital. 3. Lei 14.155/2021. I. Título. II. Leão,
Ives Eduarda oliveira Arêa. III. Soares Filho, Vicente Carlos.

CDD 345.026

Catálogo na publicação
Francisco Renato Sampaio da Silva – CRB/1028

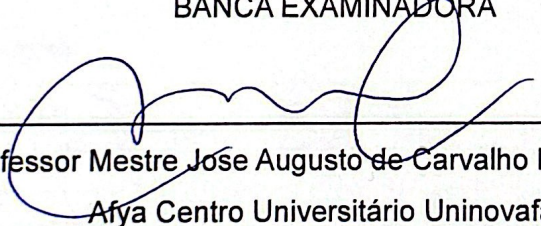
GUILHERME PORTELA CUNHA
IVES EDUARDA OLIVEIRA ARÊA LEAO
VICENTE CARLOS SOARES FILHO

**O IMPACTO DA TECNOLOGIA DIGITAL NA PRÁTICA
DO CRIME DE ESTELIONATO**

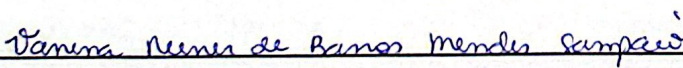
Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 13 / 11 / 2025

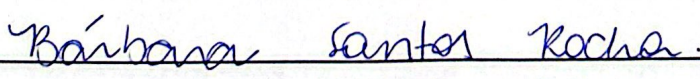
BANCA EXAMINADORA



Professor Mestre José Augusto de Carvalho Mendes Filho
Afya Centro Universitário Uninovafapi
(Orientador)



Profª Mestra Vanessa Nunes de Barros Mendes Sampaio
Afya Centro Universitário Uninovafapi
(1º Examinador)



Profª Mestra Barbara Santos Rocha
Afya Centro Universitário Uninovafapi
(2º Examinador)

RESUMO

A expressão “estelionato digital”, se refere à prática fraudulenta realizada por meios eletrônicos, geralmente com o uso de redes sociais, aplicativos de mensagens, plataformas financeiras e outros recursos tecnológicos que ampliam o alcance e a eficácia da ação criminosa. Dessa forma, o objetivo geral desse trabalho é investigar como o avanço da tecnologia digital tem influenciado a prática do crime de estelionato no Brasil. Quanto a metodologia, utilizou-se da revisão bibliográfica de cunho narrativo com caráter qualitativo. Obteve-se como resultado que os avanços tecnológicos trouxeram consigo benefícios na facilitação do acesso a informação e rapidez em diversas atividades do cotidiano, como aplicativos bancários que permitem transações instantâneas sem precisar se deslocar a agências bancárias, no entanto, essa evolução trazida pelo universo digital, passou a influenciar o desenvolvimento de um novo tipo de delito, o “estelionato digital”, que age principalmente no que se refere as mídias sociais, aplicativos fraudulentos e e-mails falsos. Observou-se que apenas a criação legislativa não se apresenta como uma forma de solucionar a nova vertente criminológica que o setor de segurança pública vem enfrentando. Logo, além do desenvolvimento de leis específicas que acompanham os delitos de cunho tecnológico, também é necessário avançar em ações que abrandem medidas de precaução, como: formação técnica do corpo investigativo da polícia, campanhas de formação de segurança digital que realmente cheguem ao público mais vulnerável, além da adoção de práticas de segurança por parte das plataformas digitais.

Palavras-chave: Estelionato; Avanço digital; Lei 14.155/2021.

ABSTRACT

The term "digital fraud" refers to fraudulent practices carried out electronically, typically using social networks, messaging applications, financial platforms, and other technological resources that broaden the reach and effectiveness of criminal activity. Thus, the overall objective of this study is to investigate how advances in digital technology have influenced fraud in Brazil. The methodology used was a qualitative narrative literature review. The results suggest that technological advances have brought benefits by facilitating access to information and streamlining various daily activities, such as banking applications that allow instant transactions without the need to go to bank branches. However, this evolution brought about by the digital world has influenced the development of a new type of crime: "digital fraud," which mainly involves social networks, fraudulent applications, and fake emails. It was observed that legislation, by itself, is not a solution to the new criminological challenge faced by the public security sector. Therefore, in addition to developing specific laws that address technological crimes, it is also necessary to promote actions that make preventive measures more flexible, such as: technical training for investigating police officers, digital security training campaigns that effectively reach the most vulnerable populations, and the adoption of security practices by digital platforms.

Keywords: Fraud; Digital advancement; Law 14.155/2021.

SUMÁRIO

1 INTRODUÇÃO.....	5
2 ESTELIONATO DIGITAL.....	8
2.1 Conceituando o crime de estelionato tradicional.....	8
2.2 O estelionato no ambiente digital.....	9
2.3 Desafios na investigação e prevenção do crime de estelionato digital	10
2.4 Implicações sociais e criminológicas	11
3 ANÁLISE ACERCA DOS IMPACTOS DO AVANÇO TECNOLÓGICO NA PRÁTICA DO ESTELIONATO DIGITAL	11
3.1 Avanço digital no crime de estelionato	11
3.2 Principais práticas de fraude digital	12
3.3 Respostas legislativas e práticas de combate à fraude perante o avanço do estelionato em ambiente digital.....	14
4 CONSIDERAÇÕES FINAIS.....	15
REFERÊNCIAS	17

1 INTRODUÇÃO

A tecnologia tem evoluído de forma constante nas últimas décadas, com novas implementações no universo digital que acabaram influenciando setores como economia, comunicação política e aspectos sociais. Além dessas áreas, houve um grande impacto no setor jurídico, principalmente no que diz respeito ao Direito Penal (Soares, 2018).

Nesse contexto, os avanços tecnológicos tem se tornado uma ferramenta vinculada ao aumento da criminalidade, principalmente nos meios digitais, marcados por crimes patrimoniais como o estelionato, caracterizado de acordo com o Art. 171 do Código Penal (CP) como o ato ilícito onde o indivíduo utiliza de técnicas fraudulentas para gerar prejuízo material a vítima, geralmente ligado a bens financeiros (Sayeg, 2021).

Diante disso, surge o “estelionato digital”, expressão que se refere à prática fraudulenta realizada por meios eletrônicos, geralmente com o uso de redes sociais, aplicativos de mensagens, plataformas financeiras e outros recursos tecnológicos que ampliam o alcance e a eficácia da ação criminosa (Henriques; Gonçalves, 2024).

Como afirma Capez (2021), o Direito Penal deve acompanhar a evolução da sociedade e adaptar-se às novas formas de manifestação da criminalidade, sob pena de se tornar ineficaz. Nessa perspectiva, a análise do crime de estelionato em sua configuração clássica e sua transposição para o meio digital revela-se imprescindível para compreender como o ordenamento jurídico brasileiro tem enfrentado tais mutações.

Assim, a recente promulgação da Lei nº 14.155/21, que alterou o Código Penal para incluir a fraude eletrônica como causa de aumento de pena nos § 2º-A e §2º-B do art. 171, reflete esse esforço de atualização normativa frente à realidade contemporânea (BRASIL, 2021).

Segundo Bitencourt (2022), a expansão dos crimes cibernéticos evidencia a vulnerabilidade do espaço virtual e a urgência de um sistema penal responsivo, que

garanta proteção jurídica efetiva aos bens jurídicos tutelados, sobretudo diante da crescente sofisticação dos meios eletrônicos utilizados para fraudar vítimas.

Greco (2023) complementa ao destacar que o Estado deve não apenas reprimir, mas também prevenir essas condutas estelionatárias, por meio de políticas públicas integradas e atualizadas com as novas tecnologias.

Perante esse cenário, o impacto da tecnologia digital na prática do crime de estelionato, com ênfase no estelionato digital, revela uma crescente sofisticação dos meios utilizados pelos criminosos, que se aproveitam da vulnerabilidade dos usuários na internet para aplicar golpes por meio de redes sociais, aplicativos de mensagens e sites falsos (Ferreira, 2024).

Essa modalidade criminosa causa não só prejuízos financeiros às vítimas, mas também abalos psicológicos e perda de confiança nas interações virtuais. Além disso, representa um grande desafio para as autoridades na investigação, prevenção e proteção contra esses crimes (Ferreira, 2024).

Dessa forma, a questão norteadora que rege esse estudo está pautada na análise de como a evolução da tecnologia digital tem fomentado a transformação e a expansão do crime de estelionato, e quais as adaptações que o ordenamento jurídico brasileiro tem implementado para gerenciar esses novos desafios.

Assim, o objetivo geral desse estudo é investigar como o avanço da tecnologia digital tem influenciado a prática do crime de estelionato no Brasil. Ademais, também possui como objetivos específicos: Estudar as mudanças nas leis que regem o crime de estelionato e que passaram a abranger o alcance digital, principalmente a Lei nº 14.155/2021, descrever as dificuldades que o sistema jurídico e a segurança pública possuem para reprimir e prevenir o estelionato digital, além de discutir a efetividade das medidas legislativas e institucionais adotadas para enfrentamento dessa modalidade delituosa

Este estudo justifica-se pelos novos desafios encontrados no sistema jurídico com os avanços dos crimes impactados pelo teor digital, pois com a Lei nº 14.155/2021 houve a alteração do Código Penal (incluindo os § 2º-A e § 2º-B ao artigo

171), onde o Brasil reconheceu a fraude eletrônica como algo específico, buscando uma punição mais dura.

Ainda assim, aplicar essa lei na prática é um desafio, pois muitas vezes ainda é difícil identificar quem cometeu o crime, definir qual tribunal tem competência e até diferenciar o estelionato tradicional do digital. Além disso, o combate a crimes digitais ainda é uma área de caráter recente no mundo jurídicos, o que traz consigo grandes desafios.

Logo, este estudo possui grande relevância para a área acadêmica, oferecendo um olhar crítico sobre como a tecnologia impacta o crime de estelionato, enquanto que para o mundo jurídico, traz reflexões essenciais sobre a real eficácia das leis e instituições que acompanham os avanços tecnológicos, aumentando a conscientização sobre os perigos das fraudes digitais e destacando a importância da adaptação do Direito frente às novas tecnologias.

Quanto a metodologia, utilizou-se da revisão bibliográfica de cunho narrativo com caráter qualitativo, onde ocorreram a seleção de estudos entre 2012 e 2025 no idioma português, com escopo jurídico-penal e criminológico, tratando direta ou indiretamente do estelionato digital, da Lei nº 14.155/2021, e da aplicação das normas penais em ambiente virtual. Dessa forma, as bases de dados consultadas incluíram a Biblioteca Digital Jurídica (BDJur), o Domínio Público, repositórios institucionais de universidades brasileiras, o Google Acadêmico, além de documentos oficiais da Polícia Federal, do Ministério da Justiça, do Comitê Gestor da Internet no Brasil (CGI.br) e do Superior Tribunal de Justiça (STJ). As palavras chaves principais aplicadas na busca dos estudos, foram: “fraude eletrônica”, “estelionato digital”, “cibercrime”, “Lei 14.155/2021”, “Direito Penal e tecnologia”, “responsabilidade penal em crimes virtuais” e “investigação criminal digital”.

2 ESTELIONATO NO AMBIENTE DIGITAL

O desenvolvimento das tecnologias tem sido o fator mais importante para o aumento rápido e a complexidade dos golpes digitais. Esse fator se dá em grande parte pelo fácil acesso à internet e a difusão dos smartphones, que mudaram o espaço

digital em um campo propício para infratores, que passaram a realizar atividades ilegais no ambiente virtual em razão do anonimato e da possibilidade de ganhos financeiros.

2.1 Conceituando o crime de estelionato tradicional

O delito de estelionato, associado com ação de cunho fraudulento, está definido no artigo 171, caput, do Código Penal do Brasil, com a seguinte formulação:

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, de quinhentos mil réis a dez contos de réis (Brasil, 1940).

Dessa forma, é possível classificar essa tipologia de fraude como crime contra o patrimônio, visto que o mesmo consiste em obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro mediante fraude.

Segundo Capez (2021), trata-se de um delito que exige não apenas a conduta enganosa, mas também a relação de causalidade entre o ardil e o prejuízo da vítima, o que o diferencia de outras figuras típicas do Direito Penal. Já Greco (2023) observa que a relevância do estelionato para o estudo criminológico decorre de sua ampla incidência social e de sua capacidade de adaptação aos meios disponíveis em cada época.

A fraude está no núcleo deste delito, podendo ser rapidamente reconhecida pelos elementos abaixo: (i) ação do delinquente com o objetivo de obter vantagem ilegal, causando danos à vítima; (ii) a vantagem ilegal deve ser em benefício próprio ou de outra pessoa; (iii) a vítima precisa ser enganada ou mantida em confusão; (iv) o delinquente deve empregar algum método enganoso para realizar o crime e se usufruir do bem alheio (Greco, 2023).

O bem que se torna o objeto do delito é o patrimônio da pessoa afetada, que enfrenta perdas em função das ações enganosas do autor. Nota-se que, por não

demonstrar agressão ou ameaça significativa ao indivíduo afetado, a punição é, de maneira geral, moderada. Em linhas gerais, a prática de estelionato descrita na parte principal e nos incisos do artigo 171 envolve o autor do crime conseguir um ganho ilegal de qualquer tipo através de uma farsa que engane ou faça a vítima continuar equivocada (Diniz; Cardoso, 2022).

O agente que comete o crime é aquele que leva ou mantém a vítima em engano, valendo-se de truques enganosos. Logo, é evidente que para a realização desse crime, não é exigida nenhuma característica ou capacitação do autor, podendo ser executado por qualquer indivíduo. Esse pensamento se aplica igualmente ao sujeito que sofre as consequências, sendo ele o prejudicado, que padece, de forma obrigatória (Greco, 2023).

É fundamental destacar que o crime de estelionato é, em geral, de cunho material, ou seja, ocorre efetivamente quando o infrator obtém o resultado esperado, que é a conquista de um benefício ilegal, sendo possível a configuração de uma tentativa (Diniz; Cardoso, 2022).

2.2 O estelionato no ambiente digital

Historicamente, o estelionato esteve associado a documentos falsos, cheques sem fundos e manipulações presenciais. Contudo, sua natureza flexível permitiu que o delito se expandisse para o campo digital, onde a fraude se mostra ainda mais eficiente, dado o anonimato e a velocidade proporcionados pela internet (Henriques; Gonçalves, 2024).

Segundo Oliveira (2022), o desenvolvimento tecnológico modificou profundamente as interações sociais e econômicas, criando novas formas de vulnerabilidade. Com isso, houve o surgimento da expressão “estelionato digital”, que passou a se referir a fraudes praticadas mediante recursos tecnológicos, geralmente por meio de redes sociais, aplicativos de mensagens instantâneas, sites falsos e plataformas bancárias.

Bitencourt (2022) ressalta que a criminalidade virtual se aproveita da assimetria de informação entre criminoso e vítima, explorando falhas técnicas e a confiança do usuário. Nesse cenário, a prática do phishing, a clonagem de perfis em aplicativos de

mensagens e os falsos marketplaces tornaram-se algumas das modalidades mais recorrentes.

De acordo com Meireles e Pasitto (2024), o crescimento do comércio eletrônico e dos bancos digitais impulsionou significativamente os crimes de estelionato eletrônico, criando um ambiente fértil para golpes que antes exigiam maior exposição física do criminoso. Além disso, o uso de criptomoedas e carteiras digitais introduziu novas camadas de complexidade para a identificação de fluxos financeiros ilícitos.

Assim, o estelionato digital não é apenas uma transposição do delito clássico para o meio virtual, mas uma evolução qualitativa, marcada pela ampliação do alcance e pela sofisticação dos métodos.

2.3 Desafios na investigação e prevenção do crime de estelionato digital

Soares (2024), pontua que a investigação do estelionato digital enfrenta obstáculos singulares, pois o anonimato proporcionado por redes privadas e criptografia, aliado à transnacionalidade dos crimes cibernéticos, dificulta a coleta de provas e a responsabilização dos autores.

Cunha (2025) defende que, para tornar a persecução penal mais eficiente, é necessário integrar as normas do Marco Civil da Internet (Lei nº 12.965/2014) às práticas de investigação, equilibrando o direito à privacidade com a necessidade de rastrear atividades criminosas e investir na repressão dessa tipologia de crime fraudulento.

Entretanto, segundo Greco (2023), somente a repressão isolada não é suficiente, é preciso investir em medidas preventivas, como campanhas de conscientização digital, capacitação técnica das forças policiais e aprimoramento da cooperação entre órgãos nacionais e internacionais.

Araújo (2025) complementa ainda, que outro ponto crucial é a responsabilidade compartilhada, principalmente entre empresas de tecnologia, bancos digitais e operadoras de internet, pois desempenham papel central na prevenção das fraudes, devendo adotar mecanismos de segurança mais robustos e colaborar com as autoridades em tempo hábil.

2.4 Implicações sociais e criminológicas

Silva (2025) expõe que o estelionato digital não gera apenas perdas financeiras, mas também impactos sociais e psicológicos, visto que muitas vítimas enfrentam ansiedade, vergonha e perda de confiança em ambientes digitais, o que pode comprometer sua inclusão social e econômica.

Do ponto de vista criminológico, a facilidade de acesso a meios digitais e o baixo risco percebido pelos criminosos favorecem a expansão desse delito. Como aponta Bitencourt (2022), a sensação de impunidade no espaço virtual é um dos principais fatores que alimentam a criminalidade digital.

Além dos danos financeiros, existem efeitos psicológicos, como constrangimento, receio e incerteza em relação ao uso de tecnologias, o que impacta de maneira negativa a inclusão digital e a confiança nas instituições. Esse cenário exige um Direito Penal responsivo, capaz de proteger os bens jurídicos tradicionais e, ao mesmo tempo, adaptar-se às mutações sociais e tecnológicas (Silva, 2025).

3 ANÁLISE ACERCA DOS IMPACTOS DO AVANÇO TECNOLÓGICO NA PRÁTICA DO ESTELIONATO DIGITAL

O desenvolvimento tecnológico além de implantar ferramentas que impactaram a criação de novos tipos de golpes, também criou um grupo específico mais suscetível a essa tipologia de crime, como idosos e indivíduos com pouca formação digital, que muitas vezes tem dados pessoais desprotegidos e expostos, o que passou a gerar a necessidade de políticas que englobam muito mais que ações legislativas partindo do poder público.

3.1 Avanço digital no crime de estelionato

O progresso tecnológico, promovido pela disseminação da web, das plataformas de redes sociais e dos sistemas eletrônicos de pagamento, mudou radicalmente as maneiras de interação social e econômica. Simultaneamente, facilitou

a criação de novas chances para atividades ilegais, especialmente no âmbito dos delitos relacionados ao patrimônio (Meireles; Pasitto, 2024).

Nesse cenário, o golpe digital aparece como uma forma avançada do golpe tradicional, moldada pelas características do mundo online e evidenciada pelo emprego de tecnologias para ludibriar e obter benefício ilegal às custas de outra pessoa (Meireles; Pasitto, 2024).

Segundo Mesquita, Ferreira e Reis (2025), o ambiente digital tornou-se um dos principais obstáculos para o sistema de justiça criminal, uma vez que possibilita que o infrator atue remotamente, com menor probabilidade de ser identificado e com a chance de impactar várias vítimas simultaneamente.

Antigamente, o golpista necessitava se comunicar pessoalmente com a pessoa alvo, mas atualmente, é suficiente criar um perfil fictício, mandar mensagens automáticas ou criar sites enganosos. Essa mudança é resultado do aumento da quantidade de pessoas online e da crescente digitalização das interações sociais e econômicas (Marques, 2024).

De acordo com Oliveira, Brito e Ferreira Júnior (2022), a expansão das vendas pela internet e dos apps de pagamento durante a pandemia da COVID-19 acentuou essa situação. A pandemia de isolamento social levou um número maior de indivíduos a utilizar plataformas online para fazer transações, o que aumentou as oportunidades para os golpistas.

Desse modo, o progresso na tecnologia, apesar de ter proporcionado conforto e rapidez, igualmente ampliou a quantidade de possíveis alvos e facilitou a entrada no mundo do crime. Logo, as maneiras de praticar crimes também se tornaram mais variadas (Marques, 2024).

3.2 Principais práticas de fraude digital

Ibrahin e Júnior (2025), conceituam que a fraude digital pode acontecer através de e-mails, imitação de perfis em plataformas sociais, utilização de aplicativos fraudulentos, alteração de links e QR Codes, entre várias táticas que tiram proveito da confiança e da distração das pessoas afetadas.

De acordo com Teixeira e Chaves (2019), os delinquentes empregam métodos de engenharia social para levar o usuário a cometer enganos, imitando mensagens autênticas de instituições financeiras, negócios ou entidades governamentais.

Esse tipo de golpe é particularmente arriscado, pois utiliza a confiança nas instituições e a fragilidade emocional da pessoa alvo, muitas vezes provocada por um sentimento de pressa, logo, a influência do progresso tecnológico nas fraudes é perceptível também no crescimento das estatísticas relatadas pelos órgãos competentes (Mesquita; Ferreira; Reis, 2025).

De acordo com os dados do Anuário Brasileiro de Segurança Pública (ABSP), no ano de 2024, houve o aumento de 17% em crimes de estelionato de cunho digital, assim, essa estatística mostra a extensão da questão e indica que o espaço virtual se transformou no principal cenário para a execução de delitos (Dias, 2025).

Oliveira, Brito e Ferreira Júnior (2022), também apontam que o ambiente online é visto como mais sedutor por indivíduos criminosos, pois proporciona um nível maior de sigilo e um risco pessoal reduzido, pois enquanto que no ambiente físico é essencial ter interação direta, papéis e testemunhas, o meio digital permite esconder a identidade e desaparecer rapidamente após a fraude.

De acordo com Mesquita, Ferreira e Reis (2025), a digitalização dos serviços ampliou a fragilidade de determinados grupos, como os idosos e indivíduos com pouca habilidade tecnológica, visto que esse grupo de pessoas geralmente não conhecerem práticas fundamentais de proteção online, e assim, acabam se tornando vítimas mais suscetíveis.

O Serviço Federal de Processamento de Dados (SERPRO) (2025), observou que aproximadamente 43% dos incidentes cibernéticos no Brasil provêm de e-mails enganosos, evidenciando que a aplicação de tecnologias como inteligência artificial e automação tem aprimorado as táticas de fraude.

Outro fator está ligado aos recursos de inteligência artificial, que são capazes de criar textos, imagens e sons autênticos, aumentando a possibilidade de induzir as vítimas a cair em golpes, essa situação destaca a urgência de ações de prevenção e de educação sobre o uso da tecnologia (Ibrahin; Júnior, 2025).

A globalização e a conexão digital permitem ainda que as mesmas fraudes sejam reproduzidas em diversos países com mínimas alterações, logo, isso enfatiza o valor da colaboração global e da unificação de estratégias de segurança cibernética. Para lidar com essa questão, é fundamental implementar uma abordagem abrangente que inclua formação digital, fortalecimento das instituições e normas tecnológicas (Ibrahin; Júnior, 2025).

3.3 Respostas legislativas e práticas de combate à fraude perante o avanço do estelionato em ambiente digital

A resposta legislativa mais relevante ao estelionato digital no Brasil foi a criação da Lei nº 14.155/2021, que alterou o Código Penal para prever aumento de pena quando o crime for cometido por meio eletrônico, essa mudança reflete o esforço do legislador em atualizar a norma penal frente à realidade tecnológica.

No entanto, conforme Wendt (2024), a tipificação e o aumento de pena não são suficientes para solucionar o problema, pois ainda existem desafios estruturais na persecução penal, como a dificuldade de cooperação internacional e a ausência de capacitação especializada em investigação digital.

A jurisprudência também desempenha papel crucial, o Superior Tribunal de Justiça (2025) tem decidido que instituições financeiras podem ser responsabilizadas por falhas de segurança em plataformas digitais, o que demonstra uma tendência de ampliar a proteção das vítimas e redistribuir o ônus da prevenção (Miler, 2025).

Comparativamente, em países como os Estados Unidos e os membros da União Europeia, a legislação cibernética já prevê há mais tempo medidas de rastreamento e cooperação internacional, o que serve de referência para o aperfeiçoamento do sistema jurídico brasileiro (Miler, 2025).

De acordo com Barros (2023), a classificação distinta do crime de estelionato eletrônico tem como objetivo penalizar com mais rigor o uso de tecnologia para enganar as vítimas, entendendo que essas ações podem causar danos a um grupo mais amplo. Contudo, somente a elaboração de tipos penais exclusivos não é bastante.

De acordo com Teixeira e Chaves (2019), a luta eficaz contra fraudes no mundo virtual exige não só atualizações nas leis, mas também a ação proativa das plataformas, pois estas devem implementar métodos de checagem, avisos de segurança e meios para denúncias.

Segundo Meireles e Pasitto (2024), a fraude online não pode ser vista apenas como uma questão de crime, mas sim como um desafio econômico e social, haja visto que as fraudes online causam danos imediatos às pessoas afetadas e despesas adicionais para as empresas, que devem aplicar recursos em proteção, suporte ao cliente e tecnologias de combate a fraudes. Além disso, impactam a confiança nas transações online e podem limitar o avanço do comércio virtual e da economia digital.

4 CONSIDERAÇÕES FINAIS

Através deste estudo foi possível analisar que os avanços tecnológicos trouxeram consigo benefícios na facilitação do acesso a informação e rapidez em diversas atividades do cotidiano, como aplicativos bancários que permitem transações instantâneas sem precisar se deslocar a agências bancárias, no entanto, essa evolução trazida pelo universo digital, passou a influenciar o desenvolvimento de um novo tipo de delito, o “estelionato digital”, que age principalmente no que se refere as mídias sociais, aplicativos fraudulentos e e-mails falsos.

Essa nova modalidade de crime influenciado pelo desenvolvimento digital passou a demandar uma reformulação nas leis, que até então abrangia apenas o “estelionato tradicional”, com isso, houve a promulgação da Lei 14.155/2021, que alterou o Código penal, passando a incluir as fraudes eletrônicas e aumentando a pena do infrator. No entanto, observou-se que apenas a criação legislativa não se apresenta como uma forma de solucionar a nova vertente criminológica que o setor de segurança pública vem enfrentando.

Pois, a criptografia de aplicativos e o anonimato presente no mundo digital dificulta a ação dos órgãos de repressão, além disso, o avanço tecnológico também trouxe consigo a criação de um público mais suscetível aos golpes de estelionato

digital, sendo os idosos e indivíduos com pouco conhecimento tecnológico, o público mais vulnerável.

Dessa forma, além do desenvolvimento de leis específicas que acompanham os delitos de cunho tecnológico, também é necessário avançar em ações que abrandem medidas de precaução, como: formação técnica do corpo investigativo da polícia, campanhas de formação de segurança digital que realmente cheguem ao público mais vulnerável, além da adoção de práticas de segurança por parte das plataformas digitais.

REFERÊNCIAS

ARAÚJO, Natalia Rocha. **Estelionato e vazamento de dados: a interseção entre crime digital e proteção da privacidade**. 2025. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/9037/1/NATALIA%20ROCHA%20ARA%c3%9aJO.pdf>. Acesso em: 12 out. 2025.

BARROS, Rubens Matheus Garcia. **O estelionato eletrônico e a Lei nº 14.155/2021**. São José dos Campos: Universidade de São José, 2023. Disponível em: <https://saojose.br/wp-content/uploads/2023/12/TCC-II-Rubens-Matheus-Garciabarros.pdf>. Acesso em: 22 out. 2025.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte geral e especial**. 27. Ed. Ver.E atual. São Paulo: Saraiva, 2022.

BRASIL. **Lei nº 14.155, de 26 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tratar da fraude eletrônica. Diário Oficial da União: seção 1, Brasília, DF, 27 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 04 jun. 2025.

CAPEZ, Fernando. **Curso de Direito Penal: parte especial**. 30. Ed. São Paulo: Saraiva, 2021.

CUNHA, Vinícius Segatto Jorge da. **Avanços tecnológicos na investigação criminal e o standard probatório para o acesso aos dados armazenados em nuvem**. 2025. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/5439/1/DISSERTACAO_VIN%c3%8dCIUS%20SEGATTO%20JORGE%20DA%20CUNHA_MESTR%20DIR_2025.pdf. Acesso em: 15 out. 2025.

DIAS, Lana. **Aumentam casos de estelionato digital**. Rádio Senado. 2025. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2025/08/12/aumentamcasos-de-estelionato-digital>. Acesso em: 14 out. 2025.

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. Disponível em: <https://www.periodicos.famig.edu.br/index.php/direito/article/view/215/142>. Acesso em: 14 out. 2025.

FERREIRA, Mariana Figueiredo Gonçalves. **Estelionato em ambiente virtual: desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais**. 2024. Tese de Doutorado. Universidade do Estado de Minas Gerais. Disponível em:

https://mestrados.uemg.br/images/ppgspcid/Disserta%C3%A7%C3%B5es/TURMA_4/FINAL__Mariana_Figueiredo.pdf. Acesso em: 05 out. 2025.

GRECO, Rogério. **Criminologia e política criminal**. 11. Ed. São Paulo: Revista dos Tribunais, 2023.

HENRIQUES, Thiago Alves; GONÇALVES, Samuel Martins. Crimes digitais: Análise sobre o Estelionato virtual. **Revista Eletrônica de Ciências Jurídicas**, v. 14, n. 1, 2024. Disponível em: <https://www.revista.fadipa.br/index.php/cjuridicas/article/view/576/525>. Acesso em: 10 out. 2025.

IBRAHIM, Francini Imene Dias; LEITÃO JÚNIOR, Joaquim. **Crimes Digitais**. Local: Editora Mizuno, 2025.

MARQUES, Thalya Aparecida Silva. Crime de estelionato na contemporaneidade frente a tecnologia virtual. **RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218**, v. 5, n. 5, p. e555244-e555244, 2024. Disponível em: <https://recima21.com.br/recima21/article/view/5244/3628>. Acesso em: 12 out. 2025.

MEIRELES, Isys; PASITTO, Fernando Teles. Estelionato e suas implicações: o constante crescimento dos golpes virtuais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 11, 2024. DOI: 10.51891/rease.v10i11.17063. Disponível em: <https://periodicorease.pro.br/rease/article/view/17063/9525>. Acesso em: 11 out. 2025.

MESQUITA, Milson Rodrigues; FERREIRA, Rony de Oliveira; REIS, Gabriel de Castro Borges. Estelionato digital: a natureza jurídica da ação penal para o crime de estelionato digital praticado em ambientes virtuais. **Revista Raízes no Direito**, v. 14, n. 1, p. 187–202, 2025. Disponível em: <https://revistas2.unievangelica.edu.br/index.php/raizesnodireito/article/view/8047/5736>. Acesso em: 14 out. 2025.

MILER, Pedro Luiz Chorro. STJ reforça responsabilidade bancária e proteção do consumidor digital. **Conjur**. 2025. Disponível em: <https://www.conjur.com.br/2025out-20/stj-reforca-responsabilidade-bancaria-e-protecao-do-consumidor-digital/>. Acesso em: 22 out. 2025.

OLIVEIRA, Carlos Henrique Bassani de. **Discussões jurídicas acerca do estelionato virtual: evolução, características e combate**. 2024. Trabalho de conclusão de curso. Disponível em: <http://repositorio.upf.br/bitstream/riupf/2723/1/SOL2024CarlosHenriqueBassanideOliveira.pdf>. Acesso em: 01 out. 2025.

OLIVEIRA, Emerson Prado de; BRITO, Pedro Lincoln Prates; FERREIRA JÚNIOR, Adivé Cardoso. O aumento do estelionato digital em tempos pandêmicos. Graduação em Movimento. **Ciências Jurídicas**, 2022. Disponível em: <https://periodicos.unifrc.edu.br/index.php/gdmdireito/article/view/755/276>. Acesso em: 14 out. 2025.

SAYEG, Márcio Roberto Hasson. **O Crime de Burla (Estelionato) Eletrônico: Uma Visão Luso-Brasileira à Luz do Avanço Tecnológico**. 2021. Dissertação de Mestrado. Universidade Portucalense (Portugal). Disponível em: <https://www.proquest.com/openview/edbb1e294e2cd6e357bab2cc058d5c8b/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 10 out. 2025.

SERPRO. **Fraude: uma das consequências de um ataque bem-sucedido**. Brasília, 2025. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias2025/fraude-uma-das-consequencias-de-um-ataque-bem-sucedido-1>. Acesso em: 12 out. 2025.

SILVA, Guilherme Araújo. **Os impactos psicológicos, sociais e penais nas vítimas de crimes cibernéticos**. 2025. Trabalho de conclusão de curso. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/8902/1/TCC-%20Guilherme%20Ara%20c3%ba%20-%20Monogr%20a1fia.pdf>. Acesso em: 20 out. 2025.

SOARES, Matias Gonsales. **A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política**. Universidade Autônoma de Lisboa, 2018. Tese de doutorado. Disponível em: https://www.migalhas.com.br/arquivos/2020/6/B86DDA9403078E_AquartaRevoluc%20Industrialeseu.pdf. Acesso em: 10 out. 2025.

SOARES, Thiago Vinicius de Souza Pinheiro. **Desafios e perspectivas da prevenção e investigação do estelionato online**. 2024. Trabalho de conclusão de curso. Disponível em: <https://repositorio.unirn.edu.br/jspui/bitstream/123456789/1008/5/TCC-%20Thiago%20Vinicius%20de%20Souza%20Pinheiro%20Soares.pdf>. Acesso em: 05 out. 2025.

TEIXEIRA, Filipe Silva; CHAVES, Fábio Barbosa. Os crimes de fraude e estelionato cibernéticos e a proteção ao consumidor no e-commerce. **Boletim Jurídico**, 2019. Disponível em: <https://jus.com.br/artigos/73480/os-crimes-de-fraude-e-estelionatociberneticos-e-a-protecao-ao-consumidor-no-e-commerce>. Acesso em: 15 out. 2025.

**ANEXO A - COMPROVANTE DE SUBMISSÃO OU APROVAÇÃO DO ARTIGO
NA REVISTA ONDE CONSTE O NOME DE TODOS OS AUTORES DO
TRABALHO**

