

UNIVERSIDADE NOVE DE JULHO
DEPARTAMENTO DE PÓS-GRADUAÇÃO *STRICTO SENSU*
PROGRAMA DE MESTRADO EM DIREITO

MAIZA SILVA SANTOS

A FRAUDE ELETRÔNICA COMO NOVA MODALIDADE DE ESTELIONATO

SÃO PAULO – SP
2025

MAIZA SILVA SANTOS

A FRAUDE ELETRÔNICA COMO NOVA MODALIDADE DE ESTELIONATO

Dissertação de Mestrado apresentada à Banca Examinadora do Programa de Pós-Graduação *Stricto Sensu* em Direito, da Universidade Nove de Julho de São Paulo, como exigência parcial para obtenção do título de Mestre em Direito, na área de concentração Estruturas do Direito Empresarial, sob orientação do Prof. Dr. Marcelo Costenaro Cavali.

SÃO PAULO – SP
2025

Santos, Maiza Silva.

A fraude eletrônica como nova modalidade de estelionato. / Maiza Silva Santos. 2025.

121 f.

Dissertação (Mestrado)- Universidade Nove de Julho - UNINOVE, São Paulo, 2025.

Orientador (a): Prof. Dr. Marcelo Costenaro Cavali.

1. Fraude eletrônica. 2. Estelionato tradicional. 3. Evolução do crime de estelionato. 4. Ambiente digital. 5. Impactos financeiros e socioeconômicos. 6. Desafios jurídicos e investigativos. 7. Tendências atuais e futuras.

I. Cavali, Marcelo Costenaro. II. Título

CDU 34

MAIZA SILVA SANTOS

A FRAUDE ELETRÔNICA COMO NOVA MODALIDADE DE ESTELIONATO

Dissertação apresentada e defendida ao programa de pós-graduação *stricto sensu* em Direito da Universidade Nove de Julho, como requisito parcial para a obtenção do título de Mestre em Direito.

Aprovada em: 15/12/2025

Banca Examinadora:

Prof. Dr. Marcelo Costenaro Cavali
Orientador – UNINOVE

Prof. Dr.
Examinador Interno – UNINOVE

Prof. Dr.
Examinador Externo –

Dedico essa dissertação a minha mãe, Dona Irene (*in memoriam*), mulher forte, simples e incansável, que apesar da pouca instrução sempre me incentivou a estudar.

AGRADECIMENTOS

A elaboração desta dissertação representou uma jornada de intensa dedicação e aprendizado, pontuada por momentos de reflexão profunda e superação. Sua concretização foi possível não apenas pelo esforço individual, mas, sobretudo, pelo apoio irrestrito e pela colaboração de pessoas e instituições que foram pilares fundamentais ao longo deste percurso.

Agradeço ao meu amado esposo, meu eterno companheiro e maior incentivador, expresso a mais sincera e profunda gratidão. Seu amor incondicional, sua inabalável crença em meu potencial e seu suporte prático e emocional diário foram a força motriz que me impulsionou a cada etapa, transformando desafios em oportunidades e ausências em um propósito compartilhado.

Aos meus queridos filhos, Vinicius e Victor Luís, à minha nora Rhayane, e aos meus amados netos, Isabella e Vinicius Júnior, dedico um agradecimento especial pela paciência, compreensão e carinho inestimáveis. A capacidade de vocês em entender a importância deste projeto e em me oferecer um ambiente de paz e apoio familiar foi um bálsamo em momentos de maior exigência.

Em particular, estendo meu reconhecimento ao meu filho Victor Luís, cuja perspicácia e assistência tecnológica foram um diferencial crucial. Sua expertise em lidar com ferramentas digitais, na organização de dados e na superação de entraves técnicos permitiu que a pesquisa avançasse com fluidez, transpondo barreiras que, de outra forma, seriam intransponíveis.

Ao meu estimado orientador e professor, Dr. Marcelo Costenaro Cavali, dedico meu mais profundo respeito e gratidão. Sua valiosa condução, seu rigor acadêmico, sua expertise ímpar e sua paciência inesgotável foram determinantes para a qualidade e a profundidade desta pesquisa. Sua orientação não foi apenas um farol que iluminou o caminho, mas uma bússola que garantiu a coerência e a relevância do trabalho, sempre com um olhar crítico e construtivo.

Aos colegas de pesquisa, à instituição de ensino – Universidade Nove de Julho – que me acolheu e a todos aqueles que, direta ou indiretamente, contribuíram com um conselho, uma palavra de incentivo ou um recurso essencial para a concretização deste trabalho, o meu muito obrigado.

A todos os professores que integraram esta caminhada acadêmica, em especial aqueles que compuseram a banca de qualificação e defesa, deixo registrada minha mais sincera gratidão. Cada disciplina, cada debate e cada orientação representaram não apenas a transmissão de conhecimento técnico, mas também a formação de uma visão crítica, ética e humanista do Direito.

O exemplo de dedicação, rigor intelectual e generosidade acadêmica de cada docente foi essencial para o amadurecimento desta pesquisa. Agradeço, especialmente, pela paciência, pelo estímulo constante e por acreditarem no poder transformador da educação.

Cada contribuição, de todos elencados acima, por menor que pareça, foi parte integrante deste trabalho.

"Bendita seja a crise que te faz crescer, a queda que te faz olhar para o Céu, o problema que te faz buscar a Deus".

São Pio de Pietrelcina

RESUMO

Esta pesquisa tem como objetivo analisar a figura típica do crime de estelionato eletrônico, previsto no artigo 171, § 2º-A, introduzido pela Lei nº 14.155/2021, que alterou o Código Penal Brasileiro, bem como fornecer informações acerca da evolução do crime de estelionato e seus impactos financeiros e socioeconômicos. A fraude eletrônica representa uma evolução significativa do estelionato tradicional para o ambiente digital. Enquanto o estelionato clássico, previsto no artigo 171 do Código Penal brasileiro, consiste em obter vantagem ilícita mediante artifício, ardil ou qualquer outro meio fraudulento, a modalidade eletrônica transporta essas características para o mundo virtual, potencializando seu alcance e complexidade. O estudo parte da percepção de que vivemos em uma sociedade cada vez mais digitalizada, em que as transações financeiras, comunicações e serviços essenciais ocorrem predominantemente via internet, o que impõe a realização de pesquisas contínuas sobre as fraudes eletrônicas, a fim de acompanhar a rápida evolução das técnicas fraudulentas, usadas como *modus operandi* dos criminosos, e possibilitar a atualização legislativa, sempre que necessária para desenvolver tipificações específicas que contemplem as peculiaridades de novos crimes digitais. Finalmente, o estudo visa demonstrar que a compreensão aprofundada desses fenômenos permitirá enfrentar os desafios jurídicos e investigativos e, por consequência, auxiliará, não apenas o combate às tendências atuais, mas também poderá antecipar e prevenir futuras modalidades criminosas, conferindo maior segurança jurídica e tecnológica para toda a sociedade.

Palavras-chave: fraude eletrônica; estelionato tradicional; evolução do crime de estelionato; ambiente digital; impactos financeiros e socioeconômicos; desafios jurídicos e investigativos; tendências atuais e futuras.

ABSTRACT

This research aims to analyze the typical figure of the crime of electronic fraud, provided for in art. 171, § 2º-A, introduced by Law No. 14.155/2021, which amended the Brazilian Penal Code, as well as to provide information about the evolution of the crime of fraud and its financial and socioeconomic impacts. Electronic fraud represents a significant evolution of traditional fraud to the digital environment. While classic fraud, provided for in article 171 of the Brazilian Penal Code, consists of obtaining illicit advantage through artifice, trickery or any other fraudulent means, the electronic modality transports these characteristics to the virtual world, enhancing its scope and complexity. The study is based on the perception that we live in an increasingly digitalized society, in which financial transactions, communications and essential services occur predominantly via the internet, which requires ongoing research into electronic fraud in order to keep up with the rapid evolution of fraudulent techniques used as a *modus operandi* by criminals, and to enable legislative updates whenever necessary to develop specific classifications that take into account the peculiarities of new digital crimes. Finally, the study aims to demonstrate that an in-depth understanding of these phenomena will allow us to face legal and investigative challenges and, consequently, will help not only combat current trends, but will also be able to anticipate and prevent future criminal activities, providing greater legal and technological security for society as a whole.

Keywords: electronic fraud; traditional fraud; evolution of fraud; digital environment; financial and socioeconomic impacts; legal and investigative challenges; current and future trends.

ABSTRACTO

Esta investigación tiene como objetivo analizar la figura típica del delito de fraude electrónico, prevista en el art. 171, § 2º-A, introducido por la Ley n.º 14.155/2021, que modificó el Código Penal brasileño, así como proporcionar información sobre la evolución del delito de fraude y sus impactos financieros y socioeconómicos. El fraude electrónico representa una evolución significativa del fraude tradicional al entorno digital. Mientras que el fraude clásico, previsto en el artículo 171 del Código Penal brasileño, consiste en la obtención de una ventaja ilícita mediante artificios, engaños o cualquier otro medio fraudulento, la modalidad electrónica traslada estas características al mundo virtual, aumentando su alcance y complejidad. El estudio se basa en la percepción de que vivimos en una sociedad cada vez más digitalizada, en la que las transacciones financieras, las comunicaciones y los servicios esenciales se realizan predominantemente a través de Internet, lo que requiere una investigación continua sobre el fraude electrónico para mantenerse al día con la rápida evolución de las técnicas fraudulentas utilizadas como *modus operandi* por los delincuentes y para permitir actualizaciones legislativas cuando sea necesario para desarrollar clasificaciones específicas que consideren las peculiaridades de los nuevos delitos digitales. Finalmente, el estudio pretende demostrar que una comprensión profunda de estos fenómenos nos permitirá afrontar los retos legales y de investigación y, en consecuencia, nos ayudará no solo a combatir las tendencias actuales, sino también a anticipar y prevenir futuras actividades delictivas, brindando mayor seguridad jurídica y tecnológica a la sociedad en su conjunto.

Palabras clave: fraude electrónico; fraude tradicional; evolución del fraude; entorno digital; impactos financieros y socioeconómicos; retos legales y de investigación; tendencias actuales y futuras.

LISTA DE ABREVIATURAS E SIGLAS

2FA	Dois Fatores
AC	Ação Criminal
ACR	Apelação Criminal
AES	Algoritmo de Criptografia Avançada
AI	Automação Inteligente
APK	<i>Android Package Kit</i>
BCB	Banco Central do Brasil
BEC	<i>Business Email Compromise</i>
BPC	Benefício de Prestação Continuada
BPM	Gerenciamento de Processos de Negócios
CC	Código Civil
CP	Código Penal
CPF	Cadastro de Pessoa Física
CVV	<i>Card Verification Value</i> (Código de Segurança)
CVC	<i>Corporate Venture Capital</i>
DFIR	<i>Digital Forensics & Incident Response</i>
DFIR	Forense Digital na Resposta a Incidentes
DKIM	<i>DomainKeys Identified Mail</i>
DLP	Prevenção Contra Perdas de Dados
DMARC	<i>Domain-based Message Authentication, Reporting, and Conformance</i>
DNS	Sistema de Nomes de Domínio
DOC	Documento de Ordem de Crédito
ENUL	Embargos de Nulidade e Infringentes
FEBRABAN	Federação Brasileira de Bancos
FOMO	<i>Fear Of Missing Out</i>

HC	Habeas Corpus
IA	Inteligência Artificial
IAM	Gerenciamento de Identidade e Acesso
IBM	<i>International Business Machines</i>
IDEC	Instituto de Defesa de Consumidores
INSS	Instituto Nacional do Seguro Social
IOF	Imposto sobre Operações Financeiras
LGPD	Lei Geral de Proteção de Dados
LOAS	Lei Orgânica da Assistência Social
MED	Mecanismo Especial de Devolução
MFA	Autenticação Multifator
ML	<i>Machine Learning</i>
MLATs	<i>Mutual Legal Assistance Treaties</i>
OSINT	<i>Open-Source Intelligence</i>
OTPs	<i>One-Time Passwords</i>
PB	Política Nacional de Cibersegurança
PL	Projeto de Lei
PNCiber	Política Nacional de Cibersegurança
PR-MFA	Implementação de Autenticação Multifator Resistente a <i>Phishing</i>
RPA	Automação de Processos Robóticos
RATs	<i>Remote Access Trojans</i>
SIEM	<i>Security Information and Event Management</i>
SMS	<i>Short Message Service</i>
SOC	Centro de Operações de Segurança
SPC	Serviço de Proteção ao Crédito
SPF	<i>Sender Policy Framework</i>
STF	Supremo Tribunal Federal

STJ	Superior Tribunal de Justiça
TED	Transferência Eletrônica Disponível
TLS/SSL	<i>Transport Layer Security/Secure Sockets Layer</i>
TRF4	Tribunal Regional Federal da Quarta Região
UPS	Fonte de Alimentação Ininterrupta
URL	<i>Uniform Resource Locator</i>
VPN	<i>Virtual Private Network</i>

SUMÁRIO

1	INTRODUÇÃO	15
1.1	Relevância da fraude eletrônica como novo tipo de estelionato	16
1.2	Problema de pesquisa, objetivos e metodologia	17
2	CONTEXTO DE CRIMINALIZAÇÃO E O BEM JURÍDICO TUTELADO	21
2.1	O crime de estelionato: o conceito de patrimônio e o prejuízo patrimonial	22
2.2	Os avanços da tecnologia e o volume crescente das fraudes digitais	25
3	ESTELIONATO: CARACTERÍSTICAS ESSENCIAIS	28
3.1	Tipo objetivo	28
3.1.1	Ação nuclear	28
3.1.2	Sujeitos ativo e passivo	31
3.1.3	Momento consumativo, tentativa e arrependimento posterior	34
3.2	Tipo subjetivo	40
3.3	Torpeza bilateral (fraude bilateral)	41
3.4	Fraude penal e fraude civil	46
3.5	Formas	50
3.5.1	Simples (art. 171, <i>caput</i>)	50
3.5.2	Privilegiada (art. 171, § 1º)	52
3.5.3	Figuras equiparadas (art. 171, § 2º)	55
3.5.4	Fraude eletrônica e o aparente concurso com o crime de fraude com a utilização de ativos virtuais, valores mobiliários e ativos financeiros	59
3.5.5	Majorantes (art. 171, §§ 3º e 4º)	65
3.5.6	Ação Penal (art. 171, § 5º)	66
3.6	Análise crítica da tipificação penal do estelionato eletrônico	77
4	A FRAUDE ELETRÔNICA	82
4.1	O estelionato eletrônico e as fraudes digitais mais comuns utilizadas para a sua prática (golpes digitais)	83
4.1.1	<i>Phishing</i>	86
4.1.2	Categorização dos ataques de <i>phishing</i>	90
4.1.2.1	Golpe do Whatsapp	94
4.1.2.2	Golpe do Pix	95
4.1.2.3	Golpe da Falsa central telefônica/Falso funcionário	98
4.1.2.4	Golpe do falso empréstimo ou da devolução de empréstimo	99

4.2	Impactos econômicos e sociais do estelionato por fraude eletrônica e os desafios de enfrentamento.....	101
5	CONCLUSÃO.....	109
	REFERÊNCIAS	112

1 INTRODUÇÃO

A era digital transformou de modo radical a sociedade mundial, impulsionando o desenvolvimento da comunicação, do comércio e do acesso à informação¹. Não obstante isso, essa revolução tecnológica também abriu portas para novas formas de criminalidade, com a fraude eletrônica surgindo como uma das condutas mais ameaçadoras e desafiantes do cenário criminal².

Grupos vulneráveis, como idosos e pessoas com menor alfabetização digital, são alvos preferenciais dos criminosos cibernéticos. Esses crimes provocam imensuráveis impactos psicológicos nas vítimas, que, além das perdas financeiras, sofrem traumas, ansiedade e desconfiança no sistema financeiro.

Como consectário, a tutela do patrimônio na era da conectividade passou a exigir a adoção de medidas tecnológicas e jurídicas (inclusive penais) que busquem proteger bens e direitos dos indivíduos e empresas diante das crescentes ameaças das fraudes digitais. Evidentemente, a digitalização e automação inteligente (AI)³ dos processos financeiros e comerciais ampliou as oportunidades para fraudes eletrônicas, exigindo soluções inovadoras e eficazes.

Este estudo visa analisar a fraude eletrônica como uma nova modalidade de estelionato, explorando sua relevância, dados estatísticos e objetivos, os elementos do tipo penal e suas principais modalidades, com base em fontes bibliográficas relevantes. A análise abordará a evolução do estelionato no contexto histórico e no âmbito da evolução digital, as nuances das legislações pertinentes e as estratégias de prevenção e combate a essa modalidade criminosa.

¹ AGRA, Andressa D.; BARBOZA, Fabrício F M. **Segurança de sistemas da informação**. Porto Alegre: SAGAH, 2019. *E-book*, p. 5. ISBN 9788595027084. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788595027084/>. Acesso em: 30 mai. 2025.

² DFNDR Blog. Inteligência artificial traz novas ameaças para celulares e computadores. **Cibersegurança**. Disponível em: <https://www.psafes.com/blog/inteligencia-artificial-traz-novas-ameacas-para-celulares-e-computadores/>. Acesso em: 30 mai. 2025.

³ Automação inteligente (AI), às vezes chamada de automação cognitiva, é o uso de tecnologias de automação como inteligência artificial (IA), gerenciamento de processos de negócios (BPM) e automação de processos robóticos (RPA) para otimizar e escalar a tomada de decisões em toda a organização. IBM. **O que é automação inteligente?** Disponível em: <https://www.ibm.com/br-pt/topics/intelligent-automation>. Acesso em: 06 abr. 2025.

1.1 Relevância da fraude eletrônica como novo tipo de estelionato

A fraude eletrônica, também agora conceituada como crime cibernético ou cibercrime financeiro⁴, abrange uma vasta gama de atividades ilícitas que exploram a tecnologia para obter vantagens financeiras indevidas. Essas atividades incluem, mas não se limitam às fraudes mais conhecidas como *phishing*, *malware*, fraudes em comércio eletrônico, golpes financeiros e roubo de identidade – que serão tratados neste trabalho –, mas sim a uma gama infindável de fraudes que surgem a todo instante, na mesma medida em que evoluem os recursos tecnológicos.

A relevância da fraude eletrônica como novo tipo penal reside em seu impacto generalizado e crescente no patrimônio particular. Indivíduos, empresas e instituições financeiras são alvos constantes, resultando em perdas financeiras substanciais e danos à sua reputação. Relevante também destacar que a natureza transnacional da internet dificulta a investigação e a punição dos criminosos, tornando a fraude eletrônica um desafio complexo para as autoridades. A utilização de tecnologias de anonimato, como a rede Tor e VPNs⁵, de igual modo dificulta o rastreamento dos fraudadores. A rápida evolução das tecnologias digitais exige uma constante e eficaz atualização das estratégias de combate à fraude eletrônica.

Além disso, dessas fraudes sobrevém um significativo impacto financeiro. Estima-se que fraudes eletrônicas causem prejuízos de bilhões de reais anualmente no Brasil⁶. Esse problema afeta tanto pessoas físicas quanto instituições financeiras

⁴ BRANQUINHO, Thiago; Marcelo. **Segurança Cibernética Industrial**. Rio de Janeiro: Editora Alta Books, 2021. *E-book*, p. 65. ISBN 9786555204117. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786555204117/>. Acesso em: 06 jun. 2025.

⁵ A utilização de tecnologias de anonimato como a rede Tor e VPNs visa proteger a privacidade online, mascarando o endereço IP do utilizador e ocultando a sua localização e atividades de navegação. O Tor é um navegador que utiliza uma rede descentralizada de servidores que são escolhidos aleatoriamente para criptografar e encaminhar o tráfego, dificultando o rastreamento do utilizado. É frequentemente usado para acessar a *dark web* ou para proteger a privacidade online em situações onde o anonimato é essencial. Já as VPNs criptografam o tráfego e o encaminham por meio de servidores próprios e são usadas como uma opção mais fácil e rápida para proteger a privacidade em atividades online diárias, como *streaming*, jogos e navegação na internet. LAMEIRAS, André. Tor ou VPN: qual é a melhor opção? **Welivesecurity**. Publicado em: 20 mar. 2023. Disponível em: <https://www.welivesecurity.com/br/2023/03/20/tor-ou-vpn-qual-e-a-melhor-opcao>. Acesso em: 06 jun. 2025

⁶ SERASA EXPERIAN. Tentativas de fraudes bancárias cresceram 10,4% em 2024 e poderiam gerar prejuízo de até R\$ 51,6 bilhões, revela Serasa Experian. **Prevenção à Fraude**. Publicado em: 11 mar. 2025. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraudes-bancarias-cresceram-104-em-2024-e-poderiam-gerar-prejuizo-de-ate-r-516-bilhoes-revela-serasa-experian/> Acesso em: 21 abr. 2025.

e empresas e gera custos indiretos com cibersegurança, seguros e procedimentos de verificação.

1.2 Problema de pesquisa, objetivos e metodologia

O principal problema desta pesquisa é investigar como a fraude eletrônica se configura como uma nova modalidade de estelionato, adaptada às características do ambiente digital. Para bem demonstrar a magnitude do problema, é fundamental apresentar dados estatísticos relevantes.

De acordo com a Federação Brasileira de Bancos (FEBRABAN), as tentativas de golpe e fraudes financeiras digitais no Brasil aumentaram 17% de 2023 a 2024. As perdas financeiras decorrentes dessas fraudes saltaram de R\$ 8,6 bilhões para R\$ 10,1 bilhões. As fraudes envolvendo o Pix, sistema de pagamentos instantâneos do Banco Central, representaram uma parcela significativa desse montante, com prejuízos de R\$ 2,7 bilhões no período, o que representa um crescimento de 43% nas transações por meio de fraudes⁷.

O Brasil é o segundo país mais impactado por crimes cibernéticos na América Latina. As informações constam em uma pesquisa realizada pela empresa de segurança Fortinet⁸. Outro estudo realizado em 2022, pela empresa de cibersegurança Norton, já havia divulgado os resultados de sua pesquisa, conduzida em parceria com o The Harris Poll, que destacava o Brasil como o terceiro país com mais dispositivos infectados por ameaças cibernéticas entre os 10 países examinados

⁷ WHATELY, Marussia. Acesso a água e saneamento reflete desigualdades do Brasil. **PODER 360**. Publicado em: 11 mar. 2024. Disponível em: <https://www.poder360.com.br/poder-economia/golpes-causaram-prejuizo-de-r-101-bi-em-2024-diz-febraban/> Acesso em: 22 abr. 2025.

⁸ DI LORENZO, Alessandro; Capozzi, BRUNO. Brasil é o segundo maior alvo de crimes cibernéticos na América Latina. **Olhar Digital**. Publicado em: 02 fev. 2024. Disponível em: <https://olhardigital.com.br/2024/02/02/seguranca/brasil-e-o-segundo-maior-alvo-de-crimes-ciberneticos-na-america-latina/> Acesso em: 22 abr. 2025.

(Austrália, Brasil, França, Alemanha, Índia, Itália, Japão, Nova Zelândia, Reino Unido e Estados Unidos)⁹.

Este estudo também apontou um aumento na sofisticação dos ataques, com a utilização de técnicas de engenharia social cada vez mais elaboradas, o que demonstra a urgência de compreender e combater o crime de estelionato praticado por meio de fraude eletrônica.

Nesse sentido, a presente pesquisa tem como foco o exame dos elementos do tipo penal do artigo 171, § 2º-A, do Código Penal, a fim de verificar a possibilidade de adequação típica das principais fraudes eletrônicas como uma nova modalidade de estelionato e as características que a diferem das formas tradicionais, considerando a utilização de tecnologias como a internet, dispositivos móveis e redes sociais, como vetores para a sua prática.

Essa temática se justifica em razão do avanço das tecnologias digitais que não obstante tenham proporcionado inúmeros benefícios e facilidades à sociedade, na mesma escala de velocidade, vem possibilitando o surgimento de novas formas de práticas criminosas, dentre as quais destaca-se a fraude eletrônica.

Esta prática, caracterizada pela utilização de meios digitais para obter vantagem ilícita, configura uma nova modalidade do crime de estelionato, desafiando os mecanismos tradicionais de prevenção e repressão criminal. No panorama brasileiro, em especial após a Lei nº 14.155/2021, tornou-se fundamental analisar os impactos jurídicos e sociais dessas fraudes, envolvendo tanto a adaptação do ordenamento quanto os efeitos sobre as vítimas.

A relevância deste estudo decorre da necessidade de compreender a eficácia das respostas legislativas e institucionais, bem como as repercussões para a segurança e confiança da sociedade no meio eletrônico. O aumento significativo das fraudes eletrônicas representa um desafio crescente na sociedade digital, exigindo uma análise aprofundada de suas características, implicações jurídicas e medidas de

⁹ PANCINI, Laura. Tecnologia. Inteligência Artificial. **EXAME**. Publicado em: 11 mar. 2022. Disponível em: <https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/> Acesso em: 22 abr. 2025.

prevenção. Esta pesquisa busca contribuir para a compreensão desse fenômeno, fornecendo dados relevantes e buscando soluções para mitigar seus riscos.

O presente estudo, ao abordar a fraude eletrônica como uma nova modalidade de estelionato, procura promover uma reflexão crítica sobre as práticas de segurança no ambiente digital, a fim de analisar a sua eficácia na proteção dos direitos e interesses dos cidadãos. A conscientização da população e a colaboração entre os diferentes atores da sociedade são fundamentais para o combate eficaz à fraude eletrônica.

O trabalho está organizado em cinco seções, de forma lógica e detalhada, abordando a fraude eletrônica como uma evolução do crime de estelionato, contextualizada no cenário jurídico e tecnológico atual.

A primeira seção contempla a introdução que apresenta a relevância do fenômeno das fraudes eletrônicas como um novo tipo de estelionato, focando na gravidade do problema no contexto contemporâneo e explicitando os seguintes aspectos: a importância do tema; a delimitação do problema de pesquisa, apoiada por dados estatísticos atuais; objetivos, estrutura do trabalho e metodologia, ressaltando os motivos que conduziram a pesquisa.

Na segunda seção, é analisado o contexto em que as fraudes eletrônicas se proliferam, especialmente em razão dos avanços tecnológicos. São discutidos nesta fase o impacto da tecnologia e o crescimento das fraudes digitais; as principais tipologias dessas fraudes e a proteção do patrimônio enquanto bem jurídico relevante na sociedade conectada.

Já na terceira seção, é aprofundado o estudo do crime de estelionato no ordenamento jurídico brasileiro, detalhando as suas características essenciais, quais sejam: tipo objetivo com a descrição dos sujeitos ativo e passivo, momento consumativo, arrependimento posterior e tentativa; tipo subjetivo; definição de fraude bilateral (torpeza bilateral); distinções entre fraudes penais e civis e análise das várias formas do crime de estelionato, desde a forma simples até a eletrônica, incluindo figuras equiparadas, privilegiadas e majorantes; também são examinadas as peculiaridades da ação penal, finalizando com uma análise crítica da tipificação penal.

A quarta seção é dedicada a um exame prático das principais fraudes eletrônicas praticadas atualmente que caracterizam a conduta típica do estelionato, em especial: a fraude de boleto; o *phishing*; o *pharming* e outras fraudes digitais relevantes. Também aborda o impacto econômico que atingem as atividades empresariais de um modo geral, as instituições financeiras e, por conseguinte, a sociedade.

A pesquisa adotou uma abordagem qualitativa, de natureza exploratória e descritiva, utilizando-se de pesquisas bibliográficas e documentais, que envolveram a consulta a livros, artigos acadêmicos, legislação, decisões judiciais e notícias relevantes sobre o tema, além de aspectos empíricos sobre fraudes eletrônicas para embasar a análise social.

Finalizando, a quinta seção traça uma conclusão que sintetiza os principais achados da pesquisa, retomando os objetivos iniciais e indicando possíveis encaminhamentos para futuras reflexões e estudos, bem como sugerindo medidas preventivas e repressivas ao fenômeno das fraudes eletrônicas. Por fim, o trabalho apresenta a lista das obras, artigos, leis e demais fontes utilizadas ao longo do desenvolvimento do estudo, demonstrando o rigor científico adotado.

2 CONTEXTO DE CRIMINALIZAÇÃO E O BEM JURÍDICO TUTELADO

No cenário dos delitos contra o patrimônio, o estelionato figura indiscutivelmente como um dos principais protagonistas, compartilhando essa relevância com o furto. Enquanto o furto caracteriza-se essencialmente pela subtração, o estelionato distingue-se fundamentalmente pelo emprego da fraude como meio para obtenção de vantagem econômica, manipulando a vontade da vítima. Esta característica nuclear do estelionato merece importantes considerações.

Diferentemente dos crimes baseados na subtração, em que há uma agressão unilateral contra a vítima, o estelionato configura-se como um crime de interação. Nesta modalidade delitiva, o êxito do agente na obtenção da vantagem indevida depende necessariamente de uma participação ativa da vítima, que realiza voluntariamente um ato de disposição patrimonial. Estabelece-se, portanto, uma interação específica entre autor e vítima: o primeiro utiliza artifícios fraudulentos para contaminar a vontade do segundo, que, induzido a erro, entrega bens ou valores ao agente. Esta dinâmica peculiar, em que um se beneficia diretamente do prejuízo alheio, suscita complexas questões sobre a fronteira entre condutas criminosas e meros negócios desvantajosos.

É fundamental esclarecer que, embora a fraude seja elemento constitutivo do estelionato, ela também aparece em outras figuras delitivas, como no furto mediante fraude. A distinção crucial reside no comportamento da vítima afetado pelo ardil: no furto, a fraude visa criar um estado de desatenção que facilite a subtração; no estelionato, por sua vez, ela induz a vítima a praticar um ato deliberado de disposição patrimonial, aparentemente vantajoso, mas que efetivamente resultará em seu prejuízo econômico¹⁰.

O bem jurídico tutelado no estelionato é o patrimônio em sua totalidade. Apesar das diversas interpretações doutrinárias existentes, pode-se afirmar que este crime invariavelmente resulta na diminuição patrimonial da vítima, consequência direta da disposição patrimonial motivada pelo engano. Vale ressaltar que a fraude pode não apenas criar o erro, mas também mantê-lo. Conforme esclarece a própria exposição

¹⁰ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **AgRg no AgRg no AREsp: 2026865 SP 2021/0383539-0**, Data de Julgamento: 09/08/2022, T5 - QUINTA TURMA, Data de Publicação: DJe 15/08/2022.

de motivos do Código Penal de 1940, o silêncio intencional diante do erro preexistente da vítima constitui meio fraudulento caracterizador do estelionato¹¹.

Para Bittencourt, o bem jurídico protegido é a inviolabilidade do patrimônio, particularmente em relação aos atentados que podem ser praticados mediante fraude¹². Essa tutela abarca tanto o interesse social, representado pela confiança recíproca que deve imperar nos relacionamentos patrimoniais individuais e comerciais, quanto o interesse público de refrear e evitar a fraude que provoca o dano alheio.

A criminalização desta conduta visa salvaguardar a integridade nas transações comerciais e na esfera econômica, estabelecendo a expectativa normativa de comportamento honesto nas relações negociais.

Importante destacar a distinção do crime estelionato com a prática de infidelidade patrimonial, porque enquanto o estelionato é cometido “de fora para dentro”, a infidelidade patrimonial ocorre de “dentro para fora”, provocada por quem tem uma posição de destaque diante do bem jurídico tutelado¹³. De fato, o estelionato pode materializar-se nas mais diversas e rotineiras interações do dia a dia.

2.1 O crime de estelionato: o conceito de patrimônio e o prejuízo patrimonial

Não surpreende, que o estelionato tenha se consolidado como o delito patrimonial que mais suscita controvérsias e discussões na dogmática penal, refletindo a tensão permanente entre a criatividade ilícita e a resposta legislativa.

¹¹ CAMPOS, Francisco. **Exposição de Motivos do Código Penal**, § 61, *in verbis*: "Com a fórmula do projeto, já não haverá dúvida que o próprio silêncio, quando malicioso ou intencional, acerca do preexistente erro da vítima, constitui meio fraudulento característico do estelionato". E.M. Código Penal - DL nº2.848/40. p. XXXVI. Imprensa Nacional. Rio de Janeiro, 1941. Disponível em <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-exposicaodemotivos-pe.pdf>. Acesso em: 08 jun. 2025.

¹² BITENCOURT, Cezar R. **Tratado de direito penal: parte especial**. v. 3. 20. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*, p. 285. ISBN 9788553622436. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553622436/>. Acesso em: 23 abr. 2025.

¹³ DE GRANDIS, Rodrigo. **O Delito de Infidelidade Patrimonial e o Direito Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo - SP. 2018.

Nos anos recentes, a legislação penal brasileira tem se adaptado às transformações sociais e econômicas, resultando em um tratamento mais rigoroso para o estelionato. A pena básica atual estabelece reclusão de um a cinco anos e multa, com possibilidade de agravamento em circunstâncias específicas, particularmente quando há emprego de recursos tecnológicos na execução do delito patrimonial.

Estas mudanças refletem o reconhecimento do legislador sobre a necessidade de proteção do patrimônio e da confiança nas relações sociais e econômicas, elemento fundamental para o funcionamento harmonioso da sociedade contemporânea.

Por esse viés, a intrincada conceituação do crime patrimonial revela uma fundamental dicotomia doutrinária, que merece uma análise crítica aprofundada. Uma vertente teórica, de cunho mais tradicional e por vezes influenciada pelo direito civil clássico, insiste na estrita vinculação do delito à lesão de um interesse mensurável economicamente, erigindo a apreciação pecuniária como baliza intransponível para a caracterização do prejuízo. Essa perspectiva, que remonta a uma visão mais restritiva da propriedade e do patrimônio, tende a desconsiderar bens que, embora desprovidos de valor de mercado imediato, possuem inegável utilidade ou significado para o indivíduo.

Contudo, em contraposição a essa visão por vezes redutora, emerge uma perspectiva mais abrangente e humanizada: embora inegavelmente a dimensão econômica figure como elemento predominante na maioria dos crimes patrimoniais, argumenta-se que o conceito de "coisa" no sentido jurídico-penal transcende o mero valor de mercado. Ele engloba bens de cunho moral, afetivo ou simbólico que, ao serem objetivados e incorporados à esfera de interesses do indivíduo, adquirem relevância patrimonial. É nesse ponto que a subjetividade da vítima se impõe como um fator crucial, pois o que para o agente pode ser desprovido de valor (como uma fotografia antiga, um diário pessoal, um objeto de herança familiar sem valor venal), para o lesado pode representar uma perda incomensurável e insubstituível.

O patrimônio, sob essa ótica, não é apenas um somatório de ativos financeiros, mas um complexo de bens materiais e imateriais que compõem a esfera de disponibilidade e gozo de uma pessoa, contribuindo para sua identidade e bem-estar.

A ortodoxia defendida por Heleno Fragoso, que postula a imprescindibilidade de um interesse juridicamente e economicamente apreciável, alinhando-se à rigidez civilista da avaliação monetária dos bens e à teoria objetiva do patrimônio¹⁴, é confrontada pela visão mais elástica e progressista de Nélson Hungria. Este, ao reconhecer a primazia econômica na maioria dos casos, expande a noção de patrimônio para incluir aquelas “coisas que, embora sem valor venal, representam uma utilidade, ainda que simplesmente moral ou afetiva”¹⁵.

Tal sofisticação conceitual é ecoada por Manzini¹⁶, que desvincula o valor patrimonial do estritamente econômico, e por Antolisei¹⁷, que sagazmente inclui no conceito de patrimônio não apenas direitos monetizáveis, mas também objetos de mero valor de afeição (como recordações familiares, cartas pessoais, obras de arte de valor sentimental inestimável, ou mesmo animais de estimação). A subtração desses itens, portanto, configura, sem sombra de dúvida, uma diminuição patrimonial e, por conseguinte, um dano jurídico relevante, pois afeta a esfera de bens e interesses do indivíduo, mesmo que não se traduza em uma perda financeira direta.

Incontestavelmente, o estelionato se revela como um crime de resultado material por excelência, exigindo a concretização do *eventus damni* para sua plena configuração. Isso significa que não basta a mera conduta de enganar a vítima, mediante artifício ardil; é imperativo que haja uma efetiva diminuição patrimonial para esta, que se materializa pela obtenção de vantagem ilícita pelo autor e o prejuízo patrimonial para terceira pessoa. É incontestável que a ausência de uma diminuição patrimonial efetiva para a vítima descaracteriza o delito, podendo, no máximo, configurar uma tentativa.

A crítica aqui se aprofunda ao notar que o objeto da vantagem ilícita, para integrar o patrimônio jurídico-penal, precisa transcender a mera avaliação monetária, devendo encarnar alguma forma de utilidade, seja ela material, afetiva, simbólica ou de uso, para o sujeito passivo. Isso reforça a tese de que o patrimônio não é um mero somatório de cifras, mas um complexo de bens e direitos que conferem valor e

¹⁴ FRAGOSO, Heleno Cláudio. **Lições de Direito Penal**. Parte Especial, v. 1. 11. ed. Rio de Janeiro: Forense, 1995, p. 186.

¹⁵ HUNGRIA, Nélson. **Comentários ao Código Penal**. v. 7, 2. ed. Rio de Janeiro: Forense, 1958.

¹⁶ *Apud* BATISTA, Weber Martins. **O furto e o roubo no direito e no processo penal**. 3ª ed. São Paulo: Lumen Juris, 2014, p. 4.

¹⁷ ANTOLISEI, Francesco. **Manuale di Diritto Penale**. Parte Speciale, Milano, 1954, v. 1, p. 189.

significado à esfera de interesses do indivíduo, e cuja privação gera um prejuízo real, ainda que não exclusivamente financeiro.

Notadamente a descrição típica do estelionato no ordenamento jurídico brasileiro explicita a exigência do *animus lucrandi*, ou seja, a intenção de obtenção de vantagem ilícita ou lucro por parte do agente.

2.2 Os avanços da tecnologia e o volume crescente das fraudes digitais

A era digital trouxe inúmeros benefícios para a sociedade, desde a facilidade de comunicação instantânea até sistemas complexos de automação e inteligência artificial. No entanto, junto com essa evolução, testemunhamos um crescimento alarmante das fraudes digitais, que se adaptam e evoluem na mesma velocidade que as tecnologias que visam combatê-las. Este paradoxo tecnológico representa um dos maiores desafios da sociedade contemporânea.

O avanço acelerado da tecnologia criou um ambiente propício para o desenvolvimento de novos métodos fraudulentos. A transformação digital das últimas décadas não apenas modificou a forma como interagimos e realizamos transações, mas também abriu caminho para novas vulnerabilidades. A digitalização de serviços financeiros, governamentais e comerciais transferiu para o ambiente virtual operações que antes eram exclusivamente presenciais, criando assim novos vetores de ataque.

Dados da Febraban – Federação Brasileira de Bancos, indicam que, em 2024, o orçamento em tecnologia do setor bancário atingiu quase R\$ 50 bilhões, sendo 10% desse valor destinado exclusivamente à prevenção de fraudes¹⁸. Estes dados refletem a necessidade urgente de combater a sofisticação crescente dos golpes digitais, que acompanham de perto as inovações tecnológicas.

O estudo global da Norton do ano de 2023 indica que as fraudes cibernéticas causaram prejuízos estimados em US\$ 8 trilhões em 2022, com projeção de alcançar

¹⁸ FEBRABAN TECH. **Congresso de Prevenção e Repressão a Fraudes, Segurança Cibernética e Bancária.** Disponível em: <https://febrabantech.febraban.org.br/evento/congresso-prevencao-fraudes/sobre> Acesso em: 23 abr. 2025.

US\$ 10,5 trilhões anuais até 2025. Somente no Brasil em 2024, segundo um levantamento realizado pelo FortiGuard Labs, que é um laboratório de análise e inteligência de ameaças da Fortinet, as empresas sofreram cerca de 356 bilhões de tentativas de ataques cibernéticos. Isso coloca o Brasil no topo do ranking da América Latina, entre os países mais alvejados por *malwares*, na frente de México, Colômbia e Peru¹⁹.

O crescimento das fraudes digitais segue uma curva ascendente desde 2015, com uma aceleração significativa durante e após a pandemia de COVID-19. Este período marcou uma adoção forçada e acelerada de tecnologias digitais por parte de muitos usuários sem o devido preparo para identificar e se proteger de possíveis fraudes.

Diversos são os fatores que contribuem para o crescimento das fraudes digitais. Em primeiro lugar, a democratização de ferramentas maliciosas: *softwares* e *kits* de desenvolvimento de *malware* estão cada vez mais acessíveis no mercado negro digital. Em segundo lugar, lacunas regulatórias: a legislação frequentemente não acompanha a velocidade da inovação tecnológica. Em terceiro lugar, a baixa literacia digital: grande parte da população carece de conhecimentos básicos sobre segurança digital. Em quarto lugar, anonimato e alcance global: a internet permite que criminosos operem de qualquer parte do mundo com relativa impunidade. Em quinto lugar, a evolução da IA: ferramentas de inteligência artificial tornam ataques mais sofisticados e difíceis de detectar.

No que concerne aos seus impactos socioeconômicos, vemos que as fraudes digitais ultrapassam o âmbito individual e afetam toda a estrutura socioeconômica. Essas consequências incluem a perda de confiança em sistemas digitais e instituições financeiras; o aumento dos custos operacionais para empresas, que acabam sendo repassados à sociedade; a sobrecarga dos sistemas judiciários com processos relacionados a crimes cibernéticos; os impactos psicológicos severos nas vítimas, incluindo ansiedade, depressão e trauma; redução da inclusão digital, especialmente entre populações mais vulneráveis.

¹⁹ TISAFE. **Ciberataques em alta no Brasil: empresas registam mais de 350 bilhões de tentativas de invasão em 2024.** Publicado em: 28 mar. 2025. Disponível em: <https://tisafe.com/pt/ciberataques-em-alta-no-brasil-empresas-registam-mais-de-350-bilhoes-de-tentativas-de-invasao-em-2024/>. Acesso em: 30 mai. 2025.

Para enfrentar este cenário, são necessárias medidas de prevenção e combate, que incluem uma abordagem multidimensional com investimento em educação digital desde o ensino fundamental; cooperação internacional para combater crimes que frequentemente transcendem fronteiras; desenvolvimento de marcos regulatórios eficientes e adaptáveis às novas tecnologias; adoção de tecnologias de autenticação multifator e biometria avançada e uso de inteligência artificial para detectar padrões suspeitos de comportamento.

Especialistas dos setores de cibersegurança apontam que o futuro da segurança digital residirá na capacidade de desenvolver sistemas que se adaptem rapidamente às novas ameaças. Segundo eles, a combinação de *blockchain*, computação quântica e inteligência artificial apresenta tanto desafios quanto oportunidades no combate às fraudes digitais²⁰.

Segundo a empresa de consultoria Gartner, os líderes de segurança cibernética devem lidar com o esgotamento na cibersegurança para garantir a eficácia de programas, apontando as principais tendências segurança cibernética para 2025, destacando que as organizações que adotarem uma abordagem proativa de segurança digital, baseada em inteligência de ameaças e resposta automática, reduzirão em até 60% os impactos financeiros de ataques cibernéticos²¹.

O avanço tecnológico continuará a moldar nossa sociedade de maneiras cada vez mais profundas, e as fraudes digitais evoluirão em paralelo. Estamos diante de uma corrida armamentista digital, em que medidas de segurança e técnicas fraudulentas competem em um ciclo contínuo de inovação. O futuro da segurança digital dependerá tanto de avanços tecnológicos quanto de mudanças comportamentais e educacionais que promovam uma cultura de prevenção e conscientização sobre os riscos do mundo digital²².

²⁰ PRESCOTT, Roberta. Blockchain, computação quântica, IoT e IA desafiam a proteção de dados. **Convergência Digital 20 anos**. Publicado em: 29 jan. 2025. Disponível em: <https://convergenciadigital.com.br/mercado/blockchain-computacao-quantica-iot-e-ia-desafiam-a-protecao-de-dados/>. Acesso em: 09 jun. 2025.

²¹ ITFORUM. Disponível em: <https://itforum.com.br/noticias/gartner-9-tendencias-impactar-negocios-2025/>. Acesso em: 30 mai. 2025.

²² MARINHO, Wederson. O futuro da Cibersegurança e Inteligência Artificial: Uma nova era de riscos e oportunidades. **Medium**. Publicado em: 21 abr. 2025. Disponível em: <https://medium.com/@marinhobusiness/o-futuro-da-ciberseguran%C3%A7a-e-intelig%C3%Aancia-artificial-uma-nova-era-de-riscos-e-oportunidades-b9185130c5c2>. Acesso em: 30 mai. 2025.

3 ESTELIONATO: CARACTERÍSTICAS ESSENCIAIS

3.1 Tipo objetivo

Tipo objetivo incriminador é todo aquele que não diz respeito à vontade do agente, apesar de estar envolvido por ela, podendo ser descritivos, ou seja, são elementos do tipo captáveis pelos sentidos humanos e normativos, que são elementos do tipo revelados por juízo de valoração²³. A tipificação do crime de estelionato decorre do emprego de meio fraudulento com o objetivo de obter vantagem econômica indevida.

A fraude pode se manifestar por meio de artifício, entendido como a utilização de instrumentos ou recursos que alteram, de forma aparente, o aspecto material de determinado objeto ou situação. Pode ainda ocorrer mediante ardil, caracterizado por discurso enganoso; por astúcia, por meio de estratégias persuasivas; por simples mentira, ou por qualquer outro expediente apto a induzir a vítima em erro. Entre as formas mais recorrentes incluem-se o inadimplemento contratual previamente planejado, a emissão de cheques falsificados, subtraídos ou prestados como garantia de dívida, dentre outras condutas. Ressalte-se que, para a configuração do ilícito, exige-se que o mecanismo fraudulento empregado seja a causa determinante da entrega do bem pela vítima²⁴.

3.1.1 Ação nuclear

A essência do crime de estelionato está na fraude: trata-se do ardil empregado pelo agente para induzir ou manter a vítima em erro, visando obter vantagem patrimonial indevida.

²³ NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 2ª ed.revista, atualizada e ampliada: parte geral: parte especial. São Paulo. Ed. Revista dos Tribunais, 2006, p.183.

²⁴ MIRABETE, Júlio Fabrini. **Código Penal Interpretado**. São Paulo. Ed. Atlas, 1999, p. 1094/1095.

Para enganar a vítima, seja induzindo-a ou mantendo-a em erro, o sujeito pode utilizar artifício, ardil ou qualquer outro meio fraudulento. Artifício refere-se ao engano realizado por meio de instrumentos materiais, como uma encenação – exemplo clássico é o golpe do bilhete premiado. Ardil, por sua vez, é a fraude praticada mediante astúcia ou ardileza, como declarar falsamente uma qualificação profissional.

Além disso, o tipo penal menciona "qualquer outro meio fraudulento", recorrendo, assim, à interpretação analógica: após citar artifício e ardil, utiliza uma fórmula genérica que engloba qualquer forma de engano da mesma natureza, como mentiras ou omissões (silêncio quando há obrigação de falar).

Como ensina Miguel Realles Junior, a norma legal, ao optou por lançar mão de uma enumeração de caráter marcadamente exemplificativo – mencionando expressamente "artifício" e "ardil" – para, em seguida, abranger uma gama mais ampla de situações por meio da generalização "qualquer outro meio fraudulento". Essa técnica visa conferir à lei a flexibilidade necessária para se adaptar à multiplicidade de formas que a fraude pode assumir, sem se restringir a um rol exaustivo que poderia ser facilmente contornado. Tal abordagem garante que o espírito da lei, que é coibir a conduta enganosa, prevaleça sobre a literalidade estrita, permitindo que o sistema jurídico alcance novas modalidades de fraudes²⁵.

O meio fraudulento usado deve ser suficiente para enganar a vítima. Se o recurso empregado for grosseiro, revelando facilmente a intenção fraudulenta, sequer há tentativa, pois o fato é considerado atípico, podendo ser considerada a hipótese de tentativa inidônea²⁶.

Erro, nesse contexto, é a percepção equivocada da realidade, induzida pela conduta do autor do crime. Podem-se distinguir dois casos: a vítima é levada a erro pelo agente, em razão da fraude praticada ou a vítima já se encontra em erro espontaneamente, e o agente se vale de meios fraudulentos para mantê-la nessa situação. No primeiro, o agente provoca o erro da vítima, mediante fraude. No segundo, a fraude consiste em manter o equívoco preexistente por meio de manobras fraudulentas.

²⁵ REALE JÚNIOR, Miguel. **Código Penal Comentado** - 2ª Edição 2023. 2. ed. Rio de Janeiro: Saraiva Jur, 2023. *E-book*, p. 610. ISBN 9786555599510. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555599510/>. Acesso em: 25 abr. 2025.

²⁶ BRUNO, Aníbal. **Direito Penal**: Parte Geral. 3ª ed. Tomo II. Rio de Janeiro: Forense, 1967, p. 247-250.

O estelionato exige um resultado duplo: a obtenção de vantagem ilícita pelo autor e o prejuízo patrimonial para terceira pessoa. Para Damásio de Jesus, a ação nuclear do estelionato é "obter" vantagem ilícita, sendo este o cerne da conduta criminosa. Todos os demais elementos (meio fraudulento, indução ao erro) são instrumentais para a realização desta ação principal que constitui o núcleo do tipo penal. O agente precisa obter vantagem ilícita que cause dano patrimonial a outrem. Caso obtenha a vantagem, mas não cause prejuízo, não se verifica o resultado típico do crime, caracterizando-se apenas a tentativa²⁷.

A vantagem almejada é sempre de natureza patrimonial, pois o estelionato é crime contra o patrimônio, e deve ser ilícita. Caso a vantagem seja legítima, pode haver apenas a incidência de outro delito, como o previsto no artigo 345 do Código Penal. Nisso reside a ação nuclear da conduta típica do crime de estelionato.

Portanto, várias e imprevisíveis são as formas que o estelionato pode assumir, mas todas devem apresentar elementos comuns, cuja ausência poderá descaracterizar o crime, podendo surgir outro delito. A forma genérica encontra-se no caput: Obter vantagem, induzindo ou mantendo a vítima em erro. Sendo assim, é possível que o autor do crime de estelionato provoque a situação de engano ou apenas dela se aproveite, mas de qualquer modo, comete a conduta proibida²⁸.

Fazendo uma decomposição dos elementos objetivos do crime de estelionato, de modo amplo, e afastados o sujeito ativo e o passivo, que aparecem em todo o tipo, temos as seguintes particularidades: a) a consecução da vantagem ilícita; b) o emprego do meio fraudulento; c) o erro causado ou mantido por esse meio; d) o nexo de causalidade entre o erro e a prestação da vantagem; e) a lesão patrimonial. Resumindo, o crime se subsume ao seguinte polinômio: meio fraudulento + erro + vantagem ilícita + lesão patrimonial = estelionato²⁹. O prejuízo decorrente da conduta deve ser concreto, não apenas potencial.

A reparação do dano, restituição ou apreensão do objeto obtido, se eliminar ou diminuir o prejuízo real, não afasta a configuração do crime nem gera a forma

²⁷ JESUS, Damásio de. **Direito penal**: parte especial (arts. 121 a 183). v. 2. 35. ed. Rio de Janeiro: Saraiva Jur, 2015. *E-book*, p. 166. ISBN 9788502619302. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788502619302/>. Acesso em: 24 abr. 2025.

²⁸ NUCCI, Guilherme de Souza. **Manual de Direito Penal**, 2ª ed. revista, atualizada e ampliada: parte geral: parte especial. São Paulo. Ed. Revista dos Tribunais, 2006, p. 699/700.

²⁹ NORONHA, Edgard Magalhães. **Direito Penal**. Vol. 2 - 13ª ed. São Paulo: Saraiva, 1977, p. 378/379

privilegiada (art. 171, § 1º do Código Penal), embora possa servir como circunstância judicial (art. 59), atenuante genérica (art. 65, III, b, CP) ou motivo para reduzir a pena (art. 16, CP). Parte da jurisprudência, contudo, admite a aplicação da forma privilegiada em tais situações³⁰.

3.1.2 Sujeitos ativo e passivo

O crime de estelionato é qualificado como crime comum, podendo ser praticado por qualquer pessoa na modalidade genérica do *caput*, ou seja, tanto a responsável pelo emprego da fraude como aquela beneficiada pela vantagem ilícita, ressaltando que, normalmente tais condições reúnem-se na mesma pessoa. O estelionato também admite a coautoria e a participação.

Não há exigência de uma condição especial para que alguém seja sujeito ativo desse delito. Contudo, é importante destacar que, se o agente for empresário e utilizar fraude para prejudicar seus credores, seja antes ou depois de decretada a falência, sua conduta pode configurar crime falimentar, nos termos do artigo 168 da Lei nº 11.101/2005. Também deve ser observado que nas modalidades previstas no § 2º, é preciso ser pessoa envolvida em algum negócio ou o dono, ou legítimo possuidor de determinada coisa³¹.

Também encontramos na doutrina a figura do delito de infidelidade patrimonial, que a despeito de guardar semelhanças com o delito de estelionato na proteção do bem jurídico patrimônio, com ele não se confunde³².

De Grandis, preleciona, em sua tese de Doutorado, intitulada “O delito de Infidelidade Patrimonial e o Direito Penal Brasileiro”, que as semelhanças estruturais entre o estelionato e a administração desleal (ou infidelidade patrimonial, a *Untreue*

³⁰ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. HC: 121460 DF 2008/0258029-0, Relator.: Ministro JORGE MUSSI, Data de Julgamento: 06/04/2010, T5 - QUINTA TURMA, Data de Publicação: DJe 03/05/2010.

³¹ NUCCI, Guilherme de Souza. **Manual de Direito Penal**, 2ª ed. revista, atualizada e ampliada: parte geral: parte especial. São Paulo. Ed. Revista dos Tribunais, 2006, p. 699.

³² DE GRANDIS, Rodrigo. **O Delito de Infidelidade Patrimonial e o Direito Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo - SP. 2018.

do direito alemão) são limitadas. Ambos os tipos penais, de fato, compartilham a característica de serem crimes patrimoniais praticados sem o emprego de violência ou grave ameaça à pessoa, culminando invariavelmente em uma lesão patrimonial para a vítima. Ressalta que embora a conduta do agente na infidelidade patrimonial possa, em certas circunstâncias, envolver o uso de fraudes pontuais ou a omissão de informações relevantes (silêncio malicioso), a essência da *Untreue* reside fundamentalmente na quebra de um dever específico de proteção ou administração do patrimônio alheio que foi previamente assumido pelo agente. Este dever surge de uma relação jurídica especial, como um mandato, uma tutela, uma curatela, um contrato de administração, ou a posição de administrador em uma empresa³³.

Essa circunstância, a existência de um dever fiduciário violado, simplesmente não se faz presente na estrutura típica do estelionato, em que o cerne da ação criminosa é a provocação ou manutenção do erro da vítima por meio da fraude, sem que haja uma relação prévia de confiança qualificada sobre a gestão do bem lesado. A criminalização da infidelidade patrimonial baseia-se, portanto, em uma injustiça de natureza distinta daquela que fundamenta o estelionato: a violação de um dever de lealdade e diligência na gestão de bens confiados. Conclui, adicionalmente o citado autor, que a maneira pela qual o objeto material do crime (o patrimônio lesado) chega à esfera de disponibilidade do agente, constitui um divisor crucial entre os dois delitos. Na infidelidade patrimonial, o patrimônio é confiado ao agente de forma legítima, em razão da relação jurídica que lhe impõe o dever de administrá-lo ou protegê-lo. O agente já detém a posse ou o controle lícito sobre o bem. No estelionato, por outro lado, o agente obtém o patrimônio unicamente por meio da fraude, induzindo a vítima a entregá-lo ou dispor dele. O agente não possuía o bem lícitamente antes da fraude³⁴.

O sujeito passivo do estelionato é, em geral, o titular do patrimônio lesado. Pode ser tanto a pessoa que é enganada pela fraude quanto aquela que efetivamente experimenta o prejuízo patrimonial, sendo possível que esses sujeitos não coincidam, embora sejam frequentemente a mesma pessoa. O entendimento consolidado do

³³ DE GRANDIS, Rodrigo. **O Delito de Infidelidade Patrimonial e o Direito Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo - SP. 2018.

³⁴ DE GRANDIS, Rodrigo. **O Delito de Infidelidade Patrimonial e o Direito Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo - SP. 2018.

Supremo Tribunal Federal é de que o sujeito passivo pode ser qualquer pessoa, física ou jurídica, de direito público ou privado³⁵ e ³⁶.

Para a configuração do estelionato, é imprescindível a existência de uma vítima certa e determinada, como exige o tipo penal ao tratar de “prejuízo alheio, induzindo ou mantendo alguém em erro”. Em situações em que a conduta ilícita visa atingir pessoas indeterminadas, como na adulteração de balanças em estabelecimentos comerciais ou de bombas de combustível, não estará configurado o estelionato, mas sim crimes contra a economia popular (Lei nº 1.521/1951) ou contra a ordem econômica (Lei nº 8.176/1991), respectivamente. Caso, porém, uma vítima específica seja identificada e sofra prejuízo, pode haver concurso formal entre o crime contra a economia popular e o estelionato³⁷.

No contexto de crimes como pirâmide financeira, a identificação de algumas vítimas não autoriza, por si só, a responsabilização por estelionato, permanecendo a conduta enquadrada como crime contra a economia popular, conforme entendimento do Superior Tribunal de Justiça³⁸.

Também é relevante mencionar que fraudes direcionadas a máquinas ou dispositivos eletrônicos, como a clonagem de cartões bancários para saques em caixas eletrônicos, não configuram estelionato, pois inexiste uma pessoa humana diretamente enganada; nesses casos, o delito caracterizado é o furto.

A vítima, além de ser determinada, deve possuir capacidade de discernimento. Se a pessoa lesada for criança ou portar deficiência mental, a conduta será enquadrada como crime de abuso de incapazes (art. 173 do Código Penal). Em relação a ébrios em estado de inconsciência, o crime configurado será furto, salvo se o agente for responsável por tal estado, hipótese em que se poderá falar em roubo impróprio (art. 157, § 1º do CP).

³⁵ STF. SUPREMO TRIBUNAL FEDERAL. **HC 84735 / PR – Habeas Corpus nº 84735**, julgado em 17/05/2005, Relator: Ministro Eros Grau. Fonte: site do STF, visto em 06/05/2025.

³⁶ STF. SUPREMO TRIBUNAL FEDERAL. **Ext 1029 / PT - PORTUGAL. EXTRADIÇÃO**, julgado em 13/09/2006, Relator Ministro Cezar Peluso. Fonte: Site do STF, visto em 06/05/2025.

³⁷ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **RHC: 161635 DF 2022/0065612-3**, Data de Julgamento: 23/08/2022, T5 - QUINTA TURMA, Data de Publicação: DJe 30/08/2022.

³⁸ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **RHC: 132655 RS 2020/0206191-0**, Relator.: Ministro ROGERIO SCHIETTI CRUZ, Data de Julgamento: 28/09/2021, T6 - SEXTA TURMA, Data de Publicação: DJe 30/09/2021.

Há ainda previsão de aumento de pena nos casos em que a vítima é idosa (com 60 anos ou mais) ou, de modo geral, vulnerável — causa de aumento prevista no § 4º do artigo 171 do CP. No caso de crianças (menores de 12 anos), aplica-se prioritariamente o artigo 173 do CP. Se a vítima for adolescente, cabe verificar se houve abuso de inexperiência própria da menoridade (quando poderá ser caracterizado o crime de abuso de incapazes) ou, ausente tal abuso, a aplicação do estelionato em sua forma majorada.

Ainda no tocante à vulnerabilidade — como aquela prescrita no § 1º do artigo 217-A do CP, relativa a pessoas com deficiência cognitiva ou incapazes de oferecer resistência —, é necessário harmonizar o conceito com a proteção do patrimônio, considerando situações em que a deficiência mental impeça a compreensão da fraude ou a possibilidade de resistir ao engano.

Ademais, é indispensável que o agente saiba, ou deva saber, que a vítima é idosa ou vulnerável; do contrário, ocorrerá erro de tipo (art. 20 do CP), afastando a causa de aumento prevista no § 4º do artigo 171 do CP, embora remanescendo o crime. No tocante à aplicação da exasperante, considera-se a idade da vítima no momento da ação ou omissão do agente, à luz da teoria da atividade (art. 4º do CP).

Na aplicação da majorante, o juiz deve pautar-se pela gravidade do resultado produzido no caso concreto, podendo ajustar a fração de aumento da pena conforme a intensidade do prejuízo.

Por fim, caso o agente, em benefício próprio ou de terceiros, explore a necessidade, paixão, inexperiência, alienação ou debilidade mental de alguém, levando-o à prática de ato suscetível de produzir efeito jurídico prejudicial, o crime será o de abuso de incapazes, conforme o artigo 173 do Código Penal.

3.1.3 Momento consumativo, tentativa e arrependimento posterior

O estelionato constitui um crime material e de duplo resultado, cuja consumação depende da conjunção de dois elementos essenciais: a obtenção de vantagem ilícita pelo agente e a ocorrência de efetivo prejuízo à vítima.

Conforme entendimento consolidado pelo Superior Tribunal de Justiça: "a doutrina penal ensina que o resultado, no estelionato, é duplo: benefício para o agente e lesão ao patrimônio da vítima"³⁹. Sem a concretização desse binômio proveito ilícito-prejuízo alheio, configura-se apenas a tentativa do delito.

A jurisprudência dos tribunais superiores firmou o entendimento de que o crime se consuma no momento em que o agente obtém a vantagem indevida, quando se produz o resultado naturalístico. Após um período de oscilação jurisprudencial por volta de 2016, quando o STJ chegou a considerar a consumação no momento do efetivo prejuízo da vítima, a Corte restabeleceu a posição de que a consumação ocorre no momento e local da obtenção da vantagem indevida.

Para melhor elucidar, cita-se alguns exemplos práticos de consumação: a) Transferência bancária: Consumação ocorre quando o valor é creditado na conta do autor do fato⁴⁰; b) Depósito em dinheiro: Momento em que o valor é creditado na conta destinatária⁴¹; c) Cheque adulterado/falsificado: Quando o banco sacado efetua o pagamento do cheque⁴²; d) Venda de produto pela internet com falsa simulação de pagamento: Consumação com o recebimento e retirada da mercadoria pelo estelionatário⁴³; e) Importante fazer um destaque quanto à natureza temporal do estelionato previdenciário, visto que embora o estelionato seja, em regra geral, crime instantâneo, no caso específico do estelionato previdenciário (contra o INSS), ele pode ser classificado como crime instantâneo de efeitos permanentes. Isso ocorre quando, por exemplo, alguém apresenta documentos falsos para obter indevidamente benefícios previdenciários que se prolongam por meses ou anos. Nessa hipótese, o crime se consuma com o recebimento da primeira parcela do benefício previdenciário, ainda que seus efeitos se estendam no tempo. Por consequência, a prescrição da

³⁹ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 36.760/RJ**, rel. Min. Paulo Medina, 6.^a Turma, j. 1.^o.03.2005.

⁴⁰ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **CC: 169053 DF 2019/0317771-7**, Relator.: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 11/12/2019, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 19/12/2019.

⁴¹ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **CC: 169053 DF 2019/0317771-7**, Relator.: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 11/12/2019, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 19/12/2019.

⁴² STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **CC: 169053 DF 2019/0317771-7**, Relator.: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 11/12/2019, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 19/12/2019.

⁴³ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **CC: 160053 SP 2018/0194677-4**, Relator.: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 22/08/2018, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 27/08/2018.

pretensão punitiva tem como termo inicial o recebimento da primeira prestação, conforme estabelece o artigo 111, inciso I, do Código Penal, entendimento já consolidado pelo Supremo Tribunal Federal⁴⁴.

É relevante mencionar que, com a edição da Lei nº 14.155/2021, que acrescentou o § 4º ao artigo 70 do Código de Processo Penal, a competência territorial em casos de estelionato passou a ser do local do domicílio da vítima, exceto na hipótese da vítima vendedora de mercadoria, em que se aplica a regra geral prevista no *caput*.

A reforma penal brasileira de 1984, por meio da Lei nº 7.209/84, introduziu no ordenamento jurídico o instituto do "arrependimento posterior" (art. 16 do Código Penal). Este dispositivo funciona como um redutor de pena aplicável a determinados delitos cometidos sem violência ou grave ameaça à pessoa, desde que haja reparação do dano ou devolução da coisa subtraída antes do recebimento formal da acusação.

No crime de estelionato (art. 171 do CP), esse instituto ganha contornos específicos e relevância prática significativa, gerando debates entre os penalistas sobre sua aplicação e efeitos.

Apesar das críticas recebidas, este mecanismo representa um avanço no direito penal contemporâneo, flexibilizando a rigorosa abordagem que o século XX dispensou aos crimes patrimoniais, tendo sido interpretado de forma progressista tanto pela doutrina quanto pela jurisprudência.

Para Bitencourt, o arrependimento posterior no estelionato representa importante mecanismo de política criminal, constitui causa obrigatória de redução de pena e não faculdade judicial⁴⁵.

⁴⁴ "É crime instantâneo de efeitos permanentes o chamado estelionato contra a Previdência Social (art. 171, § 3.º, do Código Penal) e, como tal, consuma-se com o recebimento da primeira prestação do benefício indevido, contando-se daí o prazo de prescrição da pretensão punitiva". STF. SUPREMO TRIBUNAL FEDERAL. **HC 95.379/RS**, rel. orig. Min. Ellen Gracie, red. p/ o acórdão Min. Cezar Peluso, 2.ª Turma, j. 25.08.2009, noticiado no Informativo 557. E ainda: HC 103.407/RJ, rel. Min. Joaquim Barbosa, 2.ª Turma, j. 10.08.2010, noticiado no Informativo 595; HC 91.716/PR, rel. Min. Joaquim Barbosa, 2.ª Turma, j. 31.08.2010, noticiado no Informativo 598; e HC 82.965/RN, rel. Min. Cezar Peluso, 2.ª Turma, j. 12.02.2008. É também o entendimento do Superior Tribunal de Justiça: HC 48.412/SP, rel. Min. Og Fernandes, 6.ª Turma, j. 23.02.2010, noticiado no Informativo 424; REsp 689.926/PE, rel. Min. Maria Thereza de Assis Moura, 6.ª Turma, j. 29.09.2009, noticiado no Informativo 409; e HC 121.336/SP, rel. Min. Celso Limongi (Desembargador convocado do TJ-SP), 6.ª Turma, j. 10.03.2009, noticiado no Informativo 386.

⁴⁵ "O arrependimento posterior constitui causa obrigatória de redução de pena, que varia de um a dois terços. Não se trata de faculdade judicial, mas de direito público subjetivo do agente, preenchidos os

Bitencourt destaca que a reparação deve ser integral e voluntária, não bastando o mero oferecimento de pagamento parcelado ou a devolução parcial do valor obtido mediante fraude. Para que se configure este benefício legal, é necessária a presença cumulativa dos seguintes requisitos: I) Ausência de violência ou grave ameaça à pessoa, destacando que a violência direcionada apenas contra coisas (como no furto qualificado ou dano) não impede a aplicação da minorante; II) Reparação integral do dano ou restituição completa da coisa. A reparação deve ser: pessoal, completa e voluntária (não necessariamente espontânea). Importante observar que a reparação parcial ou imposta coercitivamente será considerada apenas como atenuante genérica, não como arrependimento posterior; III) Tempestividade da reparação. O ressarcimento ou devolução deve ocorrer antes do recebimento da denúncia ou queixa. Se realizada após este marco processual, funcionará apenas como atenuante genérica (conforme art. 65, III, b, parte final, do CP)⁴⁶.

Vale destacar que a reparação do dano pode ter efeitos diversos em outros tipos penais. No peculato culposo, por exemplo, a reparação, se anterior à sentença irrecorrível, extingue a punibilidade (art. 312, § 3º, CP); se posterior, reduz a pena pela metade. Esta maior benevolência visa incentivar a recomposição do erário, beneficiando toda a coletividade.

É fundamental traçar a interrelação com as súmulas 246 e 554 do Supremo Tribunal Federal que dissipou as controvérsias quanto a necessidade da ocorrência de fraude para configuração do crime de emissão de cheque sem fundos e a fixação da competência para o seu julgamento no lugar onde ocorreu a recusa do pagamento^{47 e 48}.

É importante ressaltar que nos casos abrangidos pela Súmula 554, o crime de estelionato já estaria consumado, e o pagamento antes da denúncia apenas permitiria a aplicação da redução de pena prevista no artigo 16. Contudo, mesmo após a reforma

requisitos legais. No crime de estelionato, em que há efetivo prejuízo patrimonial à vítima, a reparação voluntária do dano antes do recebimento da denúncia deve ser valorizada como estímulo à recomposição do patrimônio lesado". BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte especial**. Vol. 3. 16ª ed. São Paulo: Saraiva, 2020, p. 287-289.

⁴⁶ BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte especial**. Vol. 3. 16ª ed. São Paulo: Saraiva, 2020, p. 287-289.

⁴⁷ STF. SUPREMO TRIBUNAL FEDERAL. **Súmula 246**: "Comprovado não ter havido fraude, não se configura o crime de emissão de cheque sem fundos".

⁴⁸ STF. SUPREMO TRIBUNAL FEDERAL. **Súmula 554**: "O foro competente para o processo e julgamento dos crimes de estelionato, sob a modalidade da emissão dolosa de cheque sem provisão de fundos, é o do local em que se deu a recusa do pagamento pelo sacado".

penal que instituiu o artigo 16, o STF continuou aplicando a súmula 554, como demonstra o RHC 62.912⁴⁹.

A Súmula 554 surgiu do debate sobre a natureza do estelionato na modalidade de emissão de cheques sem fundos – se crime material ou formal. Prevaleceu o entendimento de que, como crime material, a consumação ocorre com o efetivo prejuízo da vítima, verificável na agência bancária onde houve a recusa de pagamento, e não no local da emissão do cheque.

O fundamento dessa súmula difere da justificativa do artigo 16, representando uma construção jurisprudencial mais benéfica ao agente. Por isso, sustenta-se que a súmula mantém sua aplicação específica aos casos do artigo 171, § 2º, inciso VI, enquanto o disposto no artigo 16 se aplica às demais situações.

Por tratar-se o estelionato de um crime material, que permite o seu desdobramento, é plenamente possível a tentativa, considerando que o *iter criminis* pode ser interrompido por fatores alheios à vontade do agente. A caracterização da tentativa no crime de estelionato ocorre quando há início da execução do delito, porém sem consumação devido a circunstâncias alheias à vontade do agente. Conforme entendimento consolidado pelo Superior Tribunal de Justiça⁵⁰.

A doutrina penal distingue a tentativa perfeita, quando todos os atos de execução são concluídos sem que a vantagem se concretize, da tentativa imperfeita, na qual o *iter criminis* é interrompido antes da conclusão, também por fatores externos ao agente⁵¹.

⁴⁹ EMBARGOS INFRINGENTES OPOSTOS, EM CINCO DIAS, A ACÓRDÃO DENEGATORIO DE HABEAS CORPUS. DELES PODE-SE CONHECER, COMO RECURSO ORDINÁRIO, PELO PRINCÍPIO DA FUNGIBILIDADE. PROVA INEQUIVOCA DO PAGAMENTO DO CHEQUE, ANTES DO RECEBIMENTO DA DENUNCIA. RECURSO A QUE SE DA PROVIMENTO PARA ANULAR A SENTENÇA CONDENATÓRIA E TRANCAR A AÇÃO PENAL. STF. SUPREMO TRIBUNAL FEDERAL. **RHC: 62912 RS**, Relator.: Min. OCTAVIO GALLOTTI, Data de Julgamento: 12/04/1985, PRIMEIRA TURMA, Data de Publicação: DJ 17-05-1985 PP-07353 EMENT VOL-01378-02 PP-00262.

⁵⁰ "A consumação do crime de estelionato somente se dá com a efetiva obtenção de vantagem ilícita, em detrimento de outrem, por meio de sua indução ou manutenção em erro, utilização de artifício, artil ou fraude. Não há ilegalidade na decisão que reconhece a figura da tentativa de crime de estelionato, se o réu, preso em flagrante delito, logo após o ludíbrio da vítima, não desfrutou, sequer momentaneamente, do produto da fraude". STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp 142.451/DF**, rel. Min. Gilson Dipp, 5.ª Turma, j. 13.02.2002.

⁵¹ NUCCI, Guilherme de Souza. **Manual de Direito Penal**, 2ª ed. revista, atualizada e ampliada: parte geral: parte especial. São Paulo. Ed. Revista dos Tribunais, 2006, p. 311.

Para que a fraude alcance êxito, o meio utilizado deve possuir idoneidade suficiente para enganar a vítima, ou seja, deve ser capaz de induzi-la ao erro. A ineficácia do meio, entretanto, pode ser de duas ordens: relativa ou absoluta. Quando o meio fraudulento é apenas relativamente ineficaz, poderá estar configurada a tentativa de estelionato desde que os demais requisitos estejam presentes; em contrapartida, sendo absolutamente ineficaz, tratar-se-á de crime impossível (art. 17 do Código Penal).

Nesse sentido, no caso do estelionato – crime que depende da colaboração da vítima – a execução se inicia com o engano da vítima. Se o agente não consegue iludi-la, apenas o uso do artifício ou artil caracteriza atos preparatórios, não se admitindo a tentativa de estelionato nessa hipótese. Assim, não há que se falar em estelionato quando a obtenção da vantagem ilícita, em prejuízo de outrem, ocorre mediante meio que, embora de autoria comprovada, é ineficaz para induzir ou manter a vítima em erro.

Com efeito, o artigo 171, *caput*, do Código Penal permite identificar três cenários distintos em que a tentativa de estelionato se configura: I) Emprego de meio fraudulento sem êxito no engano. Nesta situação, o agente utiliza o artifício fraudulento, mas não consegue iludir a vítima. A análise considera as características subjetivas do ofendido, não o padrão do homem médio. Destaca que a tentativa só se caracteriza se a fraude possuía aptidão para enganar aquela vítima específica. Caso contrário, configura-se crime impossível (art. 17 do CP) por ineficácia absoluta do meio; II) Engano sem obtenção da vantagem. Na hipótese, o agente utiliza o meio fraudulento e consegue enganar a vítima, porém não obtém a vantagem ilícita por circunstâncias alheias à sua vontade; III) Obtenção da vantagem sem causar prejuízo. O agente utiliza o meio fraudulento, engana a vítima e obtém vantagem ilícita, mas não causa prejuízo patrimonial ao ofendido. Como o estelionato é crime de duplo resultado, a mera obtenção da vantagem sem o prejuízo alheio configura tentativa.

Posição divergente apresenta Cezar Roberto Bitencourt que defende que sendo o estelionato um crime que requer a cooperação da vítima, o início da sua execução se dá com o seu engano. Para ele, quando o agente não consegue enganar

a vítima, o simples emprego de artifício ou ardil caracteriza apenas a prática de atos preparatórios, não se podendo cogitar de tentativa de estelionato⁵².

Importante destacar a figura do estelionato e a ocorrência de crime impossível. Isso porque a tentativa de estelionato só se caracteriza quando o meio executório (artifício, ardil ou outro meio fraudulento) apresenta idoneidade para ludibriar a vítima específica. Esta idoneidade é avaliada considerando as condições pessoais do ofendido (experiência de vida, perspicácia) e as circunstâncias do caso concreto (local, contexto social). Se o meio fraudulento for capaz de enganar a vítima, caracteriza-se a tentativa, independentemente da sofisticação da fraude. Porém, se o meio não tiver capacidade de iludir o ofendido, configura-se crime impossível (art. 17 do CP)⁵³.

Para a falsificação de papel-moeda aplica-se a súmula 73 do STJ⁵⁴. Esta súmula refere-se ao papel-moeda com falsificação grosseira que, embora não configure o crime de moeda falsa (art. 289 do CP), ainda é capaz de enganar pessoas. Entretanto, se a falsificação for tão grosseira que não engane nem mesmo a pessoa mais ingênua, estará configurado o crime impossível por impropriedade absoluta do meio executório (art. 17 do CP)⁵⁵.

3.2 Tipo subjetivo

O elemento subjetivo do crime de estelionato é o dolo, acrescido de um especial fim de agir (elemento subjetivo específico) representado pela expressão “para si ou para outrem”. Exige-se a finalidade de obtenção de lucro indevido, em proveito próprio

⁵² BITENCOURT, Cezar Roberto. **Tratado de direito penal**. Parte especial. v. 34. ed. São Paulo: Saraiva, 2008, p. 239.

⁵³ "Não há falar em crime impossível pela inidoneidade do meio empregado, porquanto, não fosse o fato de vir ao conhecimento da vítima a cédula de identidade original, os documentos apresentados teriam eficácia para induzir e/ou manter a vítima em erro". STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp 683.075/DF**, rel. Min. Arnaldo Esteves Lima, 5.^a Turma, j. 18.04.2006.

⁵⁴ STJ. Súmula 73. "A utilização de papel-moeda grosseiramente falsificado configura, em tese, o crime de estelionato, de competência da Justiça Estadual".

⁵⁵ GRECO, Rogério. **Curso de direito penal**: parte especial. v. 3. 6. ed. Niterói: Impetus, 2009, p. 268.

ou alheio, razão pela qual não há estelionato na ausência de conhecimento acerca da ilicitude da locupletação em prejuízo alheio.

Não se admite a modalidade culposa. Isto é, o estelionato é punido apenas quando praticado dolosamente, ou seja, quando há intenção de enganar a vítima para obter vantagem ilícita em prejuízo alheio, mediante artifício, ardil ou outro meio fraudulento. O agente deve estar ciente da ilicitude dessa vantagem.

Desse modo, a conduta do agente deve ser dirigida finalisticamente a induzir ou a manter alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento, a fim de obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio.

Vemos então que o tipo penal ainda exige um elemento subjetivo específico: o proveito deve ser buscado para si ou para terceiro. Não sendo admitida a modalidade culposa, o crime só pode ser atribuído ao agente a título de dolo, sendo a chamada fraude culposa considerada fato atípico.

Damásio de Jesus prelecionava que é necessário que o sujeito tenha consciência da ilicitude da vantagem que obtém da vítima. Segundo ele, o tipo requer um segundo elemento subjetivo, contido na expressão para si ou para outrem⁵⁶.

3.3 Torpeza bilateral (fraude bilateral)

No campo do Direito Civil, prevalece o princípio consagrado pelo brocardo latino *nemo auditur propriam turpitudinem allegans*, o qual estabelece que ninguém pode ser ouvido alegando a própria torpeza em defesa do seu interesse⁵⁷. Essa orientação ético-jurídica encontra respaldo expresso no artigo 883 do Código Civil, que, ao tratar do pagamento indevido, estabelece: “Art. 883. Não terá direito à repetição aquele que deu alguma coisa para obter fim ilícito, imoral, ou proibido por lei”.

⁵⁶ JESUS, Damásio E. de. **Direito penal**, v. 2, 35ª ed. São Paulo: Saraiva, 2014, p. 427-428.

⁵⁷ “Ninguém pode alegar a sua própria torpeza para obter vantagem jurídica”. DINIZ, Maria H. **Curso de Direito Civil Brasileiro** - Vol.1 - 42ª Edição. 42. ed. São Paulo: SaraivaJur, 2025.

Aquele que, movido por um propósito imoral ou ilícito, como a consumação de um crime, fraude, suborno ou lavagem de dinheiro, efetua uma entrega ou transferência de bens, valores ou serviços a outrem, encontra-se subsequentemente impedido de pleitear a restituição do que foi concedido. Este princípio, frequentemente encapsulado pela máxima jurídica *nemo auditur propriam turpitudinem allegans* (ninguém pode ser ouvido alegando a própria torpeza), estabelece que o ordenamento jurídico não confere proteção ou vantagem àquele que busca beneficiar-se de sua própria conduta reprovável. A lei, ao aplicar esta regra, não visa a validar a posse do recebedor (que também pode ter agido ilicitamente), mas sim a sancionar a conduta do doador, recusando-se a ser um instrumento para a convalidação ou o desenlace de atos contrários à moral e à lei⁵⁸.

A natureza antiética da intenção subjacente, a torpeza intrínseca ao propósito e a desonestidade inerente à conduta do agente, desqualificam-no integralmente para qualquer amparo ou reparação legal. A invocação da própria má-fé para reverter uma situação criada por ela mesma é vista como um abuso do direito, incompatível com a boa-fé objetiva e os bons costumes que regem as relações jurídicas. Tal conduta é considerada um impedimento moral e legal para a obtenção de qualquer benefício ou restituição por meio dos tribunais.

O sistema jurídico, alicerçado em princípios éticos fundamentais, na defesa da ordem pública e na preservação da integridade das instituições, recusa-se veementemente a compactuar com a indignidade. Ao invés de oferecer guarida ou proteção àquele cuja ação revela tal vileza e má-fé, a justiça impõe uma barreira intransponível, impedindo que o autor de um ato ilícito utilize os mecanismos legais para reverter as consequências de sua própria transgressão. Este posicionamento visa a dissuadir comportamentos ilícitos, a promover a responsabilidade individual e a preservar a credibilidade e a autoridade moral do próprio direito.

Observa-se, assim, que a lei civil recusa proteção àquele que atua com desonestidade, sendo certo, também, que o Direito Civil possui caráter menos rigoroso quando comparado ao Direito Penal.

⁵⁸ MONTEIRO, Washington de Barros. **Curso de direito civil**. 26ª ed. São Paulo: SaraivaJur, 2025, p. 272.

Diante desse quadro, surge o questionamento: seria possível que o Direito Penal conferisse proteção àquele que, por sua vez, também agiu de forma reprovável, tentando auferir vantagem ilícita ou imoral, e acabou sendo prejudicado por outrem que prometera, mediante fraude, realizar ato ilícito em seu favor?

O crime de estelionato, previsto no artigo 171 do Código Penal, tutela, fundamentalmente, o patrimônio, sendo a vítima tradicionalmente protegida contra lesão patrimonial mediante ameaça penal. Contudo, verifica-se controvérsia na doutrina quanto à incidência do delito de estelionato nos chamados casos de torpeza bilateral, isto é, quando tanto o agente quanto a vítima buscam atingir fins ilícitos ou imorais.

Nelson Hungria, notável jurista, ilustrava situações desse tipo:

Um indivíduo, inculcando-se assassino profissional, arditamente obtém de outro certa quantia para matar um seu inimigo, sem que jamais tivesse o propósito de executar o crime; um falso vendedor de produtos farmacêuticos impinge, por bom preço, a uma *faiseuse d'anges*, como eficiência abortiva, substâncias inócuas; a cafetina recebe dinheiro do velho libertino, prometendo levar-lhe à alcova uma virgem, quando na realidade o que lhe vem a proporcionar é uma jovem meretriz; o simulado falsário capta o dinheiro de outrem, a pretexto de futura entrega de cédulas falsas ou em troca de máquina para fabricá-las, vindo a verificar-se que aquelas não existem ou esta não passa de um truque; o vigarista consegue trocar por bom dinheiro o paco que o otário julga conter uma fortuna; o cliente da prostituta não lhe paga o *pretium carnis*, tendo ocultado não dispor de dinheiro para fazê-lo⁵⁹.

Diante desses exemplos, defende-se que não seria admissível a configuração do estelionato, sob pena de criar distorções jurídicas. Do contrário, apenas aquele que efetivamente praticasse o ato ilícito prometido – como, nos casos narrados, executar um homicídio ou fornecer substância abortiva – deixaria de ser punido.

Parte da doutrina acompanha o entendimento do ilustre jurista, afirmando que, se o Direito Civil já rechaça a tutela de interesses marcados pela torpeza, consoante o artigo 883 do Código Civil, não seria razoável que o Direito Penal viesse a protegê-los.

⁵⁹ HUNGRIA, Nélon. **Comentários ao código penal**, v. VII, Rio de Janeiro: GZ, 2018, p. 192.

O próprio Hungria asseverava:

O patrimônio individual cuja lesão fraudulenta constitui o estelionato é o juridicamente protegido, e somente goza da proteção do direito o patrimônio que serve a um fim legítimo, dentro de sua função econômico-social. Desde o momento que ele é aplicado a um fim ilícito ou imoral, a lei, que é a expressão do direito como mínimo ético indispensável ao convívio social, retira-lhe o arrimo, pois, de outro modo, estaria faltando a sua própria finalidade⁶⁰.

Dessa forma, os doutrinadores se dividem, tendo parte doutrina adotado a posição de não ser cabível a punição do agente em situações de torpeza bilateral, entendimento este perfilhado por destacados penalistas brasileiros, entre eles Rogério Greco⁶¹.

Cumpra assinalar, entretanto, que a doutrina majoritária sustenta a possibilidade de reconhecimento do estelionato ainda que a vítima tenha agido de má-fé ou com finalidade ilícita. Entre os defensores dessa tese está Guilherme de Souza Nucci, que argumenta que não há o afastamento do delito, visto que o tipo penal não exige que a vítima tenha boas intenções. Desse modo, se esta quer levar vantagem, do mesmo modo que o agente, e termina prejudicada, pode entender configurado o estelionato⁶².

Nesse mesmo sentido, a posição de André Estefam, que defende que a torpeza bilateral não exclui o crime, não obstante muitas vezes o agente dela se aproveite para inibir a vítima de comunicar o fato as autoridades⁶³.

⁶⁰ HUNGRIA, Nélson. **Comentários ao código penal**, v. VII, Rio de Janeiro: GZ, 2018, p. 192-193

⁶¹ GRECO, Rogério. **Curso de Direito Penal**. Vol.2 - 22ª Edição 2025. 22. ed. Rio de Janeiro: Atlas, 2025. *E-book*, p. 661. ISBN 9786559776924. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559776924/>. Acesso em: 28 abr. 2025.

⁶² NUCCI, Guilherme de Souza. **Manual de Direito Penal**: parte geral: parte especial. 2 ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2006, p. 701.

⁶³ “A torpeza bilateral – que ocorre quando a vítima também visa a algum fim ilícito – não exclui o crime, embora o agente dela se aproveite com o escopo de inibir o ofendido a comunicar o fato à autoridade policial. Exemplos: o “conto da guitarra”, no qual se vende uma “máquina de fazer dinheiro”; o “conto do bilhete premiado”, em que o agente alega possuir um bilhete de loteria sorteado, mas diz encontrar-se numa situação de extrema necessidade e urgência (a vítima, então, compra o bilhete falso por preço vil, em comparação com o suposto prêmio)”. ESTEFAM, André. **Direito Penal - Parte Especial - Arts.121 a 234-C - Vol. 2**. 12. ed. Rio de Janeiro: SRV, 2025. *E-book*, p. 622. ISBN 9788553625741. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625741/>. Acesso em: 28 abr. 2025.

Na mesma direção, o ministério de Bitencourt,⁶⁴ Heleno Cláudio Fragoso⁶⁵ e Magalhães Noronha⁶⁶.

Ressalte-se, contudo, que nem todo caso em que a vítima busca “tirar proveito” do agente criminoso – e acaba prejudicada – configura hipótese de torpeza bilateral. Exemplo disso é a situação em que alguém, simulando ter um bilhete premiado, aborda a vítima dizendo precisar viajar e lhe vende o bilhete por preço inferior ao valor do suposto prêmio. Ainda que a vítima buscasse um “lucro fácil”, sua conduta não é ilícita, razão pela qual, indiscutivelmente, subsistiria a proteção penal e seria possível responsabilizar o agente por estelionato.

Rogério Greco defende a ideia de que se configuraria evidente absurdo considerar a vítima tutelada pelo Direito Penal, no caso de alguém iludido ao pagar por remessa de substância entorpecente que jamais será entregue⁶⁷.

Os tribunais superiores, por seu turno, adotaram a posição majoritária da doutrina, firmando o entendimento de que: a) O fato de a vítima também estar imbuída de má-fé ou ter interesse em participar de negócio aparentemente vantajoso (ainda que ilícito) não exclui a tipicidade da conduta do estelionato; b) A torpeza bilateral não constitui causa de exclusão da tipicidade, da ilicitude ou da culpabilidade no crime de estelionato; c) O bem jurídico tutelado pelo artigo 171 do Código Penal é o patrimônio, sendo irrelevante se a vítima tinha ou não conhecimento da ilicitude da conduta; d) O delito de estelionato se configura independentemente da boa-fé da vítima, bastando que estejam presentes os elementos do tipo penal: fraude, indução a erro, obtenção

⁶⁴ “Para caracterizar o estelionato, é irrelevante a má-fé da vítima, isto é, a torpeza bilateral”. BITENCOURT, Cezar R. **Tratado de Direito Penal** - Parte Especial - Vol.3 - 21ª Edição 2025. 21. ed. Rio de Janeiro: SRV, 2024. *E-book*, p. 311. ISBN 9788553627561. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553627561/>. Acesso em: 28 abr. 2025.

⁶⁵ FRAGOSO, Heleno Cláudio. **Lições de direito penal**, Parte especial, v. I, 3ª ed. Rio de Janeiro: Forense, 1981, p. 390/391.

⁶⁶ NORONHA, Edgard Magalhães. **Direito penal**, v. 2, São Paulo: Saraiva, 2003, p. 394.

⁶⁷ “Embora o Código Civil englobe a finalidade imoral do agente como impeditiva da repetição, entendemos que a torpeza bilateral somente se aplica aos atos considerados ilícitos. Assim, por exemplo, se o agente contrata os serviços de uma prostituta e, depois do ato sexual, confessa que não possui condições financeiras para pagar-lhe, como a prostituição em si pode ser considerada um comportamento lícito, isto é, que não contraria o ordenamento jurídico-penal, entendemos ser possível, aqui, a sua punição pelo crime de estelionato, ao contrário, como vimos, daquele que paga por uma remessa de substância entorpecente, que nunca chegará, pois, se efetivamente recebesse a “mercadoria”, estaria praticando um comportamento penalmente ilícito”. GRECO, Rogério. **Curso de Direito Penal**. Vol.2 - 22ª Edição 2025. 22. ed. Rio de Janeiro: Atlas, 2025. *E-book*, p. 662. ISBN 9786559776924. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559776924/>. Acesso em: 28 abr. 2025.

de vantagem ilícita e prejuízo alheio. Esta é a posição do Supremo Tribunal Federal⁶⁸: O Superior Tribunal de Justiça também já se manifestou neste sentido⁶⁹.

3.4 Fraude penal e fraude civil

Existe uma notável semelhança entre a fraude que caracteriza o crime de estelionato e aquela que invalida contratos civis de natureza econômica. Ambas compartilham o elemento da malícia visando um enriquecimento indevido. Surge então uma questão fundamental: por que determinados atos fraudulentos são tratados exclusivamente na esfera civil, como o descumprimento intencional de obrigações contratuais, a cobrança de dívida não vencida, o abuso de direito e outros comportamentos similares?

A intrincada relação entre o lícito e o ilícito, especialmente no que tange às modalidades de fraude, tem sido objeto de profunda análise jurídica, revelando a complexidade em traçar linhas divisórias estanques.

A distinção clássica, conforme delineada por Nélson Hungria, reside fundamentalmente na natureza da resposta estatal à transgressão. Para o jurista, o ilícito penal configura uma violação da ordem jurídica de tal intensidade e gravidade que demanda, como única sanção pertinente, a própria pena criminal⁷⁰.

Em contrapartida, o ilícito civil abrange infrações remediáveis por sanções de caráter atenuado, tais como a indenização, a execução forçada (inclusive *in natura*), a restituição ao *status quo ante*, a breve prisão coercitiva ou a anulação do ato. Essa abordagem, embora pragmática, sublinha que a diferenciação inicial não se dá pela

⁶⁸ “Fraude bilateral. Embora reprovável a conduta da vítima que participa da trama de outrem, visando vantagem ilícita, a sua boa-fé não é elemento do tipo previsto no art. 171 do Código Penal. Sanciona-se a conduta de quem arquiteta a fraude, porque o Direito Penal tem em vista, primordialmente, a ofensa derivada do delito”. STF. SUPREMO TRIBUNAL FEDERAL. **RHC 65.186/SP**, rel. Min. Carlos Madeira, 2.^a Turma, j. 19.06.1987.

⁶⁹ “Desde que a ação amolde-se à figura típica do art. 171 do Código Penal, não há como excluir o crime por eventual torpeza bilateral, sendo irrelevante para configuração do delito a participação, maliciosa ou não, da vítima”. STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp 1.055.960**, rel. Min. Laurita Vaz, j. 31.10.2008.

⁷⁰ HUNGRIA, Nélson. **Comentários ao Código Penal**. v. 7, 2. ed. Rio de Janeiro: Forense, 1958, p. 172-173.

essência do ato em si, mas pela gradação da reprovação e das consequências impostas pelo ordenamento jurídico⁷¹.

O universo das relações comerciais, por sua vez, é intrinsecamente pautado pela busca da vantagem econômica, um jogo de inteligência e astúcia que, na sabedoria popular, culminou na máxima de que "o segredo é a alma do negócio". Implícita a essa dinâmica está uma certa tolerância à malícia, mediante o qual as partes, em transações comerciais ou civis, empregam sua sagacidade para, por vezes, velar deficiências e maximizar o lucro.

Magalhães Noronha, perspicazmente, corroborava essa visão, alertando que uma interpretação rigorosa de cada ardil como fraude punível inviabilizaria grande parte das negociações, em que "pequenos ardis, ligeiros artifícios, leves expedientes" são a norma na perseguição de um "resultado rendoso"⁷². Tal perspectiva, todavia, levanta a questão crucial sobre a tênue linha que separa a negociação astuta da ilicitude.

A indagação central, portanto, emerge: mediante o qual se estabelece o limiar em que a malícia comercial ou a habilidade negocial transbordam do moralmente aceitável para adentrar o domínio do ilícito, do proibido, do engodo ou da indução ao erro? A ilicitude, de fato, irrompe quando a "malícia" é superada pelo emprego do engano e do induzimento a erro para a obtenção de vantagem indevida, em detrimento de outrem. Contudo, é fundamental discernir que, mesmo diante de um engano ou burla evidente, a conduta pode configurar-se apenas como fraude civil, resultando na anulação do contrato e na reparação de perdas e danos.

Heleno Fragoso ilustra essa gradação de forma perspicaz: a omissão de um defeito essencial na venda de um automóvel (como a transmissão avariada) constitui fraude civil, passível de anulação contratual⁷³.

No entanto, vender um automóvel desprovido de motor, induzindo o adquirente em erro fundamental, eleva a conduta ao patamar de estelionato, caracterizando uma

⁷¹ HUNGRIA, Nélson. **Comentários ao Código Penal**. v. 7, 2. ed. Rio de Janeiro: Forense, 1958, p. 172-173.

⁷² NORONHA, Edgard Magalhães. **Direito penal**, v. 2, São Paulo: Saraiva, 2003, p. 380.

⁷³ FRAGOSO, Heleno Cláudio. **Lições de Direito Penal**. Parte Especial, v. 1. 11. ed. Rio de Janeiro: Forense, 1995, v. 1, p. 446.

fraude penal⁷⁴. Assim, meros atos maliciosos inerentes ao comércio, que não alcancem a intensidade de uma burla substancial, embora questionáveis, não são suficientes para configurar o estelionato, que exige mais do que a "habitual sagacidade" dos negócios.

A permanente questão sobre a distinção entre fraude civil e penal – e, mais profundamente, se existe uma diferença essencial entre elas ou critérios seguros para sua aferição – tem assombrado a doutrina e a jurisprudência por séculos. Historicamente, inúmeras tentativas foram feitas para desvendar essa dicotomia. Após uma exaustiva análise das diversas correntes teóricas, Nélson Hungria converge para um critério que considera "menos precário", embora ainda com ressalvas, para demarcar a fronteira⁷⁵.

Hungria sugere que a fraude penal se manifesta quase invariavelmente quando, mesmo diante de um meio iludente que se revele "relativamente idôneo", a investigação retrospectiva do fato revela uma ideia preconcebida, um propósito *ab initio* de frustrar o equivalente econômico. Este é o cerne: a intenção dolosa preexistente. Excluem-se, contudo, os casos de "ardil grosseiro" aos quais a vítima sucumbiu por "indesculpável inadvertência ou omissão de sua habitual prudência". Nesse sentido, o inadimplemento preordenado ou preconcebido emerge como o "menos incerto dos sinais orientadores" na árdua tarefa de traçar a divisória nesse campo tão debatido⁷⁶.

Em última análise, o vasto repertório de teorias, tanto objetivas quanto subjetivas, que tentaram desvendar a distinção entre fraude civil e penal, falhou em apresentar fundamentos científicos irrefutáveis. A moderna doutrina, de forma categórica, rejeitou a maioria dessas construções, por mais que não lhes negue a importância histórica.

A conclusão premente é que não existe uma diferença ontológica intrínseca entre fraude civil e fraude penal. Todas as tentativas de estabelecer um princípio *in abstracto* que as distinguisse com segurança provaram-se insuficientes.

⁷⁴ FRAGOSO, Heleno Cláudio. **Lições de Direito Penal**. Parte Especial, v. 1. 11. ed. Rio de Janeiro: Forense, 1995, v. 1, p. 446.

⁷⁵ HUNGRIA, Nélson. **Comentários ao Código Penal**. v. 7, 2. ed. Rio de Janeiro: Forense, 1958, p. 191.

⁷⁶ HUNGRIA, Nélson. **Comentários ao Código Penal**. v. 7, 2. ed. Rio de Janeiro: Forense, 1958, p. 191.

Responsavelmente, não se pode proferir um juízo definitivo *a priori* sobre o tema. A fraude, em sua essência, é uma só, seja no âmbito civil ou penal; a divergência reside, fundamentalmente, em seu grau de intensidade. Embora se possa tentar diferenciar pelo objetivo (lucro do negócio na fraude civil versus "lucro" ilícito na fraude penal), ou pela ausência de dano civil impedindo a configuração do dano penal, tais distinções são reconhecidamente complexas e carecem de pacificação doutrinária.

A verdade inegável é que não há um critério científico inequívoco capaz de separar, com segurança, uma espécie de fraude da outra. Consequentemente, a separação entre fraude civil e penal, no direito positivo, é justificada primariamente por razões político-criminais. Esta escolha legislativa, ainda que orientada pelo interesse social, jamais poderá alçar-se a um padrão abstrato de impecabilidade e segurança científica. O máximo que se pode aspirar, portanto, é a formulação de critérios elucidativos, que ofereçam ao aplicador da lei subsídios para uma opção interpretativa mais segura e fundamentada diante da complexidade fática⁷⁷.

Esta posição reflete o princípio da subsidiariedade. O Direito Penal é contemporaneamente entendido como *ultima ratio* (medida extrema), por constituir um ramo jurídico significativamente severo e invasivo da liberdade individual. Portanto, se a fraude puder ser resolvida por outros campos do Direito menos rigorosos, essa será a via preferencial. A intervenção penal limita-se exclusivamente às situações estritamente necessárias. Nos demais casos, busca-se solucionar o conflito por meios menos prejudiciais aos envolvidos e, consequentemente, ao Estado.

Podemos inferir, portanto, ainda que pareça dispensável, que não existe impedimento para que a mesma conduta, receba, ao mesmo tempo, sanções civis e criminais. Todo estelionato também configura fraude civil, mas o inverso não se verifica. Nem toda fraude civil constitui estelionato⁷⁸, sendo a tipificação penal reservada para os casos mais graves – aqueles que ultrapassam os limites do Direito Civil e, consequentemente, não podem ser adequadamente solucionados por este. O

⁷⁷ BITENCOURT, Cezar R. **Tratado de direito penal: parte especial**. v. 3. 20. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*, p. 288. ISBN 9788553622436. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788553622436/>. Acesso em: 03 nov. 2025.

⁷⁸ LOUREIRO, Antonio Carlos Tovo. **Perfil do Estelionato Contratual no Ordenamento Jurídico-Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo-SP. 2004, p. 50. Disponível em <https://teses.usp.br/teses/disponiveis/2/2136/tde-26082015-113642/publico/tovo.pdf>. Acesso em 18 mai. 2025.

Direito Penal funciona como uma força de retaguarda, justificando-se sua aplicação apenas quando demonstrada a insuficiência do âmbito civil para lidar com a fraude em questão.

3.5 Formas

3.5.1 Simples (art. 171, *caput*)

O estelionato, tipificado no artigo 171 do Código Penal brasileiro, constitui uma das formas mais comuns de crime contra o patrimônio. Sua essência reside na conduta do agente que, empregando fraude, induz ou mantém alguém em erro, com o fim de obter vantagem ilícita para si ou para outrem, causando prejuízo à vítima. O bem jurídico tutelado primariamente pelo crime de estelionato é o patrimônio.

A norma visa proteger a integridade do patrimônio individual contra ataques perpetrados mediante fraude e engano, garantindo a segurança nas relações econômicas e negociais. Qualquer pessoa pode ser o sujeito ativo do crime de estelionato. Trata-se de um crime comum. O agente é aquele que, de forma dolosa (com intenção), emprega o meio fraudulento para enganar a vítima. A conduta fraudulenta é o cerne da ação do sujeito ativo. É perfeitamente configurável o concurso de pessoas no estelionato. Diversos indivíduos podem colaborar para a prática do delito, seja na idealização do golpe, na execução da fraude, na indução ao erro, ou na obtenção da vantagem⁷⁹.

A responsabilidade de cada um será avaliada conforme sua participação e o liame subjetivo que os uniu para o fim criminoso (artigo 29 do Código Penal). Por exemplo, um pode criar a identidade falsa (artifício), outro pode contar a história enganosa (ardil), e um terceiro pode receber o dinheiro.

⁷⁹ JESUS, Damásio de. **Código penal anotado**. 23. ed. Rio de Janeiro: Saraiva Jur, 2015. *E-book*, p. 353. ISBN 9788502634343. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788502634343/>. Acesso em: 18 mai. 2025.

O artigo 171, em sua redação, abrange a conduta de quem obtém a vantagem ilícita "para si ou para outrem". Isso significa que o sujeito ativo não precisa ser o destinatário final da vantagem. Se o agente pratica a fraude para que um terceiro se beneficie, e este terceiro tem conhecimento da origem ilícita da vantagem e concorda em recebê-la (dolo), ambos podem ser responsabilizados: o primeiro como autor da fraude e o segundo como partícipe ou coautor, dependendo de sua colaboração.

O sujeito passivo é a pessoa física ou jurídica que sofre o prejuízo patrimonial direto em decorrência da fraude. É fundamental distinguir o sujeito passivo (quem sofre o dano) da pessoa enganada (quem é induzida ou mantida em erro), embora frequentemente sejam a mesma pessoa. Pode ocorrer, por exemplo, que o gerente de um banco seja enganado pela fraude (pessoa enganada), mas o sujeito passivo seja o próprio banco (pessoa jurídica que sofre o prejuízo)⁸⁰.

Uma característica essencial do estelionato é que o sujeito passivo (a vítima do prejuízo) deve ser uma pessoa determinada ou determinável. Crimes que atingem um número indeterminado de pessoas, como fraudes no mercado de capitais que lesam investidores em geral, ou esquemas de pirâmide que lesam a coletividade, podem configurar outros tipos penais, como crimes contra a economia popular, e não estelionato simples. A identificação da vítima é crucial para a configuração típica e para a persecução penal.

A lei penal é ampla ao descrever os meios de execução: "artifício, ardil, ou qualquer outro meio fraudulento". Isso abrange uma vasta gama de condutas enganosas, desde as mais elaboradas até as mais simples, desde que sejam eficazes para induzir ou manter a vítima em erro.

A expressão "qualquer outro meio fraudulento" confere elasticidade ao tipo penal. A fraude pode se manifestar de diversas formas, incluindo a omissão (silêncio) quando havia um dever legal ou contratual de informar, ou a mentira, desde que inserida em um contexto ardiloso ou artificioso que a torne capaz de enganar. Uma simples mentira isolada, sem um contexto de encenação ou astúcia, geralmente não configura estelionato, a menos que seja o elemento central de um esquema enganoso.

⁸⁰ JESUS, Damásio de. **Código penal anotado**. 23. ed. Rio de Janeiro: Saraiva Jur, 2015. *E-book*, p. 353. ISBN 9788502634343. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788502634343/>. Acesso em: 18 mai. 2025.

A fraude deve ser o antecedente lógico e cronológico da obtenção da vantagem ilícita e do prejuízo. O agente emprega a fraude para conseguir a vantagem. Se a vantagem é obtida legitimamente e, posteriormente, o agente decide não cumprir uma obrigação (exemplo não pagar uma dívida), isso pode configurar ilícito civil ou outro crime (como a apropriação indébita), mas não estelionato, pois a fraude não foi a causa da obtenção da vantagem inicial⁸¹.

A análise do estelionato revela a complexidade na aplicação da lei, exigindo a cuidadosa verificação de todos os seus elementos constitutivos, em especial o nexo causal entre a fraude e o resultado, e a demonstração do dolo do agente em obter vantagem ilícita mediante engano.

3.5.2 Privilegiada (art. 171, § 1º)

No contexto do estelionato privilegiado (§ 1.º do art. 171 do Código Penal), assim como ocorre com o furto e a apropriação indébita em suas formas privilegiadas, a lei permite que a pena seja substituída por detenção (em vez de reclusão), diminuída de um a dois terços, ou que se aplique somente a pena de multa, conforme previsto no artigo 155, § 2º.

Para a concessão deste benefício, é requisito legal expresso que o réu seja primário. A primariedade é definida legalmente pela ausência de condenação criminal transitada em julgado antes da prática do novo crime (art. 63 do Código Penal). É crucial notar que a lei exige apenas a primariedade, não mencionando a necessidade de o agente possuir bons antecedentes (um conceito mais amplo, que abrange a vida pregressa do indivíduo, mesmo sem condenações definitivas). Portanto, a interpretação mais rigorosa e alinhada ao texto legal sustenta que o juiz não deveria condicionar a aplicação do privilégio à comprovação de bons antecedentes, bastando a ausência de reincidência nos termos da lei.

⁸¹ JESUS, Damásio de. **Código penal anotado**. 23. ed. Rio de Janeiro: Saraiva Jur, 2015. *E-book*, p. 353. ISBN 9788502634343. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788502634343/>. Acesso em: 18 mai. 2025.

Divergindo do furto privilegiado, em que o foco legal recai sobre o "pequeno valor" da coisa subtraída, no caso do estelionato privilegiado, a análise para a concessão do benefício se concentra no prejuízo sofrido pela vítima. A lei utiliza a expressão "pequeno valor", mas a interpretação consolidada pela jurisprudência entende que este pequeno valor se refere à vantagem ilícita obtida pelo agente e, consequentemente, ao prejuízo causado à vítima. Predominantemente, considera-se que este prejuízo deve ser de valor não superior a um salário mínimo vigente à época dos fatos. É importante frisar que este limite de um salário mínimo é uma construção pretoriana (jurisprudencial), buscando dar concretude ao conceito legal de "pequeno valor", e não um critério explicitamente fixado pela lei.

Quanto ao momento da avaliação do prejuízo para fins de aplicação do privilégio, a posição majoritária e mais coerente com os princípios do Direito Penal é que a análise deve ser feita no momento da consumação do delito. O estelionato se consuma no instante em que a vítima sofre o efetivo prejuízo patrimonial, decorrente da obtenção da vantagem ilícita pelo agente, mediante fraude ou ardil. Não há justificativa lógica ou legal para que a avaliação do prejuízo ocorra em um momento posterior à consumação, pois o benefício legal está intrinsecamente ligado à natureza e às circunstâncias do crime tal como ele se concretizou. Uma avaliação posterior abriria margem para manipulações. Por exemplo, um agente que causa um prejuízo vultoso (superior a um salário mínimo) poderia, após a descoberta do crime ou durante a investigação/processo, restituir parte dos valores à vítima na tentativa de reduzir o prejuízo final e, assim, pleitear a reclassificação do delito para a forma privilegiada.

Tal conduta, embora possa ser considerada para fins de atenuação da pena (como arrependimento posterior, se voluntária e integral), não deveria ter o condão de alterar a tipificação do crime já consumado. Ainda assim, existe uma corrente minoritária que defende a possibilidade de avaliação do prejuízo em data posterior, considerando, por exemplo, a situação econômica da vítima no momento da sentença, o que adiciona incerteza e potencial iniquidade na aplicação da lei.

Esta reavaliação crítica dos critérios e do momento de avaliação do prejuízo no estelionato privilegiado busca assegurar a aplicação justa e coerente do benefício, alinhada ao propósito legal de tratar com menor rigor crimes de menor potencial ofensivo, mas evitando que a flexibilidade interpretativa ou ações posteriores do agente desvirtuem a aplicação da norma penal.

Sempre que o tipo penal ou a norma processual penal menciona o "poder" do juiz para aplicar ou conceder determinado benefício legal (como a suspensão condicional do processo, o livramento condicional, a substituição da pena privativa de liberdade por restritiva de direitos, etc.), surge uma importante discussão doutrinária e jurisprudencial sobre a natureza dessa faculdade judicial: seria uma discricionariedade pura, uma obrigação vinculada, ou algo intermediário?

Nessas situações, há doutrinador que sustenta com firmeza a posição intermediária, que melhor se alinha com os princípios do Direito Penal e Processual Penal modernos⁸². Essa perspectiva reconhece que, ao avaliar a presença dos requisitos legais para a concessão do benefício, muitos dos quais possuem natureza claramente subjetiva (como a análise da conduta social do agente, sua personalidade, o grau de culpabilidade, a probabilidade de reincidência, a suficiência da medida para reprovação e prevenção do crime, entre outros), o magistrado de fato possui uma margem de liberdade e prudência na valoração desses elementos. Ele não deve ser forçado a uma interpretação automática ou mecanizada em favor do réu, ignorando as particularidades do caso concreto e do agente.

No entanto, e aqui reside o ponto crucial da posição intermediária, uma vez que o juiz, após a devida análise fundamentada dos requisitos objetivos e, principalmente, dos subjetivos, constata que todos os pressupostos legais para a concessão do benefício estão efetivamente atendidos, a concessão deixa de ser uma mera faculdade e se transforma em um dever legal.

Nesses casos, o juiz deve conceder o benefício, pois a lei, ao prever a possibilidade de sua aplicação sob determinadas condições, não deve servir aos caprichos ou à vontade arbitrária de quem a aplica, mas sim garantir a isonomia e a aplicação justa e previsível do direito. A discricionariedade existe na *avaliação* dos requisitos subjetivos, mas não na decisão final quando todos os requisitos, avaliados e considerados presentes, impõem a concessão do benefício. A recusa, nesse

⁸² NUCCI, Guilherme de S. **Curso de Direito Penal** - Vol.2 - 9ª Edição 2025. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*, p. 401. ISBN 9788530996666. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 16 mai. 2025.

cenário, configuraria uma ilegalidade por violação do direito subjetivo do réu ao benefício, uma vez preenchidos os requisitos legais⁸³.

3.5.3 Figuras equiparadas (art. 171, § 2º)

O artigo 171 em seu § 2º, descreve as condutas equiparadas, que configuram também o crime de estelionato. São elas:

Disposição de coisa alheia como própria: Configura-se quando alguém, de forma intencional, realiza atos de disposição (venda, troca, dação em pagamento) ou oneração (aluguel, garantia) de um bem móvel ou imóvel que pertence a outra pessoa, agindo como se fosse o legítimo proprietário⁸⁴. A fraude reside justamente na apresentação do bem como sendo seu, enganando o adquirente ou credor sobre a real titularidade. Por exemplo, vender um carro que está no nome de um amigo sem a devida autorização, apresentando-se como dono.

Alienação ou oneração fraudulenta de coisa própria: Ocorre quando o agente dispõe (vende, troca, dá em pagamento) ou onera (dá em garantia) um bem que, de fato, lhe pertence, mas sobre o qual recaem condições específicas que limitam sua livre disposição ou que já o vinculam a terceiros. A fraude aqui está na omissão dolosa dessas condições ao realizar o negócio jurídico. As condições que, se omitidas, caracterizam o crime são: a) o bem ser inalienável, ou seja, não pode ser legalmente vendido ou transferido; b) estar gravado com ônus, ou seja, possuir uma restrição ou direito real de terceiro registrado ou conhecido, como hipoteca, penhor (contratual), usufruto, servidão, etc.; c) ser litigioso, ou seja, estar sendo objeto de disputa judicial e; d) ter sido prometido a terceiro mediante prestações, como por exemplo, já ter sido objeto de um contrato preliminar (como uma promessa de compra e venda) cujas prestações ainda estão sendo pagas pelo promitente comprador. A omissão dolosa

⁸³ NUCCI, Guilherme de S. **Curso de Direito Penal** - Vol.2 - 9ª Edição 2025. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*, p. 401. ISBN 9788530996666. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 16 mai. 2025.

⁸⁴ SARRUBBO, Mário L. **Direito Penal: Parte Especial**. Barueri: Manole, 2012. *E-book*, p. 87. ISBN 9788520444368. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788520444368/>. Acesso em: 18 mai. 2025.

dessas condições essenciais ao novo adquirente ou credor é o cerne da conduta fraudulenta, pois impede que ele tenha pleno conhecimento da situação jurídica do bem.

Defraudação de penhor: É a hipótese do depositário que aliena coisa própria penhorada. Trata-se do penhor como contrato (agrícola, pecuário, industrial) e não da garantia da execução⁸⁵. Refere-se, portanto, à conduta fraudulenta do devedor que possui a posse direta de um bem dado em penhor contratual e, com dolo, dispõe desse bem de forma a frustrar a garantia do credor pignoratício. O sujeito ativo é o devedor que detém a posse do bem empenhado, e o sujeito passivo é o credor que detém o direito real de garantia sobre o bem. "Defraudar" aqui significa enganar, privar o credor de sua garantia. Isso pode ocorrer por meio da alienação do bem a terceiro sem consentimento do credor, destruição, ocultação, desvio, abandono ou qualquer outro ato que impeça o credor de exercer seu direito sobre a coisa empenhada. A conduta típica é realizar essa disposição fraudulenta quando se tem a posse da coisa empenhada, distinguindo-se do penhor judicial ou legal.

Fraude na entrega da coisa: ocorre quando alguém, legalmente obrigado a entregar coisa móvel, altera dolosamente sua substância, qualidade ou quantidade antes da efetiva entrega. Este delito pressupõe uma relação jurídica preexistente entre o sujeito ativo (o devedor da entrega) e o sujeito passivo (o credor da entrega), geralmente decorrente de um contrato de compra e venda, permuta ou outra negociação. A fraude pode se manifestar, por exemplo, na entrega de mercadoria adulterada (alteração da substância), produto de qualidade inferior à contratada (alteração da qualidade) ou em quantidade menor do que a acordada (alteração da quantidade). O elemento subjetivo é o dolo, a intenção de enganar o adquirente e obter vantagem ilícita. A consumação do crime se dá no momento em que a coisa é entregue ao sujeito passivo com as características fraudulentamente alteradas, causando-lhe prejuízo.

Fraude para recebimento de indenização ou valor de seguro: envolve a conduta de destruir, total ou parcialmente, ou ocultar coisa própria, ou lesar o próprio corpo ou a saúde, ou agravar as consequências de lesão ou doença preexistente, com

⁸⁵ SARRUBBO, Mário L. **Direito Penal: Parte Especial**. Barueri: Manole, 2012. *E-book*, p. 87. ISBN 9788520444368. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788520444368/>. Acesso em: 18 mai. 2025.

o intuito de obter vantagem ilícita em prejuízo de entidade seguradora ou assemelhada. O sujeito ativo é tipicamente o segurado ou alguém agindo em seu nome, e o sujeito passivo é a entidade que deve pagar a indenização, como uma companhia de seguros. Este é considerado um crime formal, o que significa que sua consumação não depende da efetiva obtenção da indenização ou do valor do seguro, bastando a prática dos atos fraudulentos com a finalidade específica de induzir a seguradora em erro. É fundamental para a configuração deste delito a existência de um contrato de seguro válido que cubra o risco relacionado à conduta praticada.

Caso a destruição envolva incêndio, explosão, inundação ou desabamento, e tais eventos gerem perigo comum (risco à vida, integridade física ou patrimônio de um número indeterminado de pessoas), a jurisprudência majoritária entende que o agente responderá pelo crime de perigo comum (art. 250, 254, 255 do CP) em concurso formal com o estelionato qualificado pelo resultado (art. 171, § 2º, V, c/c art. 171, § 1º do CP), pois o estelionato, neste caso, é o motivo do crime de perigo, que tem potencial lesivo mais amplo. A consumação ocorre com a prática dos atos fraudulentos (destruição, ocultação, lesão, agravamento), independentemente do recebimento da indenização.

Fraude no pagamento por meio de cheque: caracteriza-se pela emissão de cheque sem suficiente provisão de fundos em poder do sacado, ou pela frustração do pagamento do cheque já emitido. O autor do crime é o emitente do cheque. A intervenção de terceiros, como o endossante, em regra, não configura este delito para eles, a menos que atuem como coautores ou partícipes da conduta do emitente. As modalidades de fraude incluem: I) a emissão de cheque sem fundos disponíveis na conta bancária; II) a frustração do pagamento do cheque após sua emissão, seja pela retirada dos fundos existentes na conta ou pela emissão de contraordem (sustação ou revogação do cheque) sem motivo legalmente justificado (como furto, roubo ou extravio).

A consumação do crime ocorre no local da agência bancária sacada, no momento em que o cheque é apresentado para pagamento e este é recusado por insuficiência de fundos ou pela contraordem fraudulenta, gerando prejuízo ao portador. A tentativa é possível, por exemplo, se o cheque, embora emitido fraudulentamente, não chega a ser apresentado ao banco. O foro competente para processar e julgar o crime é o do local onde se situa a agência bancária sacada, pois

é ali que o resultado (a recusa do pagamento) se produz. Não há crime se, antes da apresentação do cheque, o emitente providencia a suficiente provisão de fundos, configurando o instituto do arrependimento eficaz, que impede a consumação do delito. Situações específicas, como a emissão de cheque como garantia de dívida (cheque caução), geralmente descaracterizam este crime, pois o cheque não foi emitido para pagamento à vista, podendo configurar, em tese, outro tipo de estelionato ou mero ilícito civil. Da mesma forma, a emissão de cheque de conta bancária já encerrada antes da emissão não se enquadra neste inciso, mas sim no *caput* do artigo 171 (estelionato simples), pois o documento já nasce sem qualquer possibilidade de compensação.

O ressarcimento do prejuízo causado à vítima após a consumação do crime não extingue a punibilidade, mas pode ser considerado uma circunstância atenuante na dosimetria da pena (art. 65, inciso III, alínea "b", do Código Penal). Contudo, o Supremo Tribunal Federal, por meio da Súmula 554, consolidou o entendimento de que o pagamento do cheque emitido sem provisão de fundos antes do recebimento da denúncia pelo juiz é causa de extinção da punibilidade, por ausência de justa causa para a ação penal, presumindo-se, neste caso, a ausência de dolo de fraude desde o início ou a reparação integral do dano antes do início formal do processo criminal. Se o pagamento ocorrer após o recebimento da denúncia, terá apenas o efeito de atenuante⁸⁶.

⁸⁶ STF. SUPREMO TRIBUNAL FEDERAL. **Súmula 554**. "O pagamento de cheque emitido sem provisão de fundos, após o recebimento da denúncia, não obsta o prosseguimento da ação penal." Súmulas do STF. Aprovação: 15/12/1976. Disponível em: <https://portal.stf.jus.br/>. Acesso em: 18 mai. 2025.

3.5.4 Fraude eletrônica e o aparente concurso com o crime de fraude com a utilização de ativos virtuais, valores mobiliários e ativos financeiros

Diante do cenário de crescimento exponencial das fraudes no ambiente digital, impulsionado pela digitalização acelerada e, em parte, pela pandemia de COVID-19, o legislativo brasileiro buscou uma resposta urgente. O Projeto de Lei nº 4.554/2020, posteriormente sancionado como Lei nº 14.155/2021, foi criado com o intuito de coibir essas práticas. Essa legislação, entre outras disposições, introduziu no Código Penal o parágrafo 2º-A ao artigo 171, estabelecendo o crime de "fraude eletrônica".

Essencialmente, a fraude eletrônica é uma modalidade qualificada de estelionato. Isso significa que ela compartilha os elementos constitutivos do estelionato comum (previsto no *caput* do art. 171), mas se diferencia pela forma específica e tecnológica pela qual a fraude é cometida. O parágrafo 2º-A do artigo 171 não define uma conduta completamente nova, mas qualifica uma já existente, remetendo aos elementos do *caput*.

Assim, os elementos que configuram o crime são: a) **Obtenção de Vantagem Ilícita:** O agente busca um benefício indevido para si ou para terceiros, que pode ser financeiro, material ou de outra natureza; b) **Prejuízo Alheio:** A ação do agente resulta em dano patrimonial à vítima, que pode ser uma perda financeira direta, o comprometimento de bens ou o uso indevido de informações; c) **Induzimento ou Manutenção da Vítima em Erro:** O agente utiliza artifícios, ardis ou qualquer outro meio fraudulento para enganar a vítima, fazendo-a crer em algo falso ou mantendo-a em uma situação de engano. Este é o cerne da fraude; d) **Meio Fraudulento Específico:** A fraude é realizada utilizando informações fornecidas pela própria vítima ou por um terceiro enganado, por meio de: d.1) **Redes sociais:** Como a criação de perfis falsos, envio de mensagens enganosas ou anúncios fraudulentos em plataformas como Instagram, Facebook, WhatsApp. d.2) **Contatos telefônicos:** Incluindo chamadas de *call center* falsas, *vishing* ou envio de SMS (*smishing*) com *links* maliciosos. d.3) **Envio de e-mails:** A clássica técnica de *phishing*, com mensagens que simulam ser de bancos, empresas ou órgãos governamentais. d.4) **Qualquer outro meio fraudulento análogo:** Esta cláusula de abertura permite a inclusão de novas tecnologias e métodos que surjam, desde que mantenham a essência da fraude à distância e mediada por tecnologia.

É relevante notar que, embora a lei tenha sido criada para combater fraudes intrinsecamente eletrônicas (como as via redes sociais e e-mail), a inclusão de "contatos telefônicos" demonstra a abrangência da *ratio legis* (razão da lei). O foco parece estar na maior reprovabilidade da captação de vítimas de forma remota, à distância, por meio tecnológico e sem contato pessoal direto. Essa interpretação deve guiar a aplicação analógica da cláusula de abertura, abrangendo, por exemplo, aplicativos de mensagens instantâneas ou plataformas de *e-commerce* fraudulentas. Apesar de sua abrangência, a Lei nº 14.155/2021 não tinha como foco principal a proteção da poupança popular de forma massiva, mas sim a defesa do patrimônio individual⁸⁷.

O crime tipificado consiste na obtenção de dados pessoais das vítimas para, posteriormente, conseguir vantagem patrimonial. Este tipo penal, com sua pena rigorosa (quatro a oito anos de reclusão, com possível aumento em caso de uso de servidor estrangeiro), poderia, em tese, ser considerado uma ferramenta mais adequada no combate às pirâmides financeiras modernas, que invariavelmente utilizam a tecnologia para atrair um grande número de investidores. Contudo, a jurisprudência atual do Superior Tribunal de Justiça (STJ) tende a afastar a aplicação desse tipo penal para esquemas de pirâmide que atingem um número indeterminado de pessoas (captação difusa), privilegiando o crime contra a economia popular (art. 2º, IX, da Lei nº 1.521/1951) pelo princípio da especialidade⁸⁸.

O STJ entende que, se a fraude atinge a coletividade de forma genérica, o crime contra a economia popular é mais específico. Apenas em casos de contato direto com vítimas específicas, além da captação difusa, poderia haver concurso de crimes. Vale ressaltar que a Lei nº 14.478/2022 trouxe modificações que impactam essa discussão, especialmente ao tratar de ativos virtuais. Mais recentemente, a Lei nº 14.478/2022, que regulamenta a prestação de serviços de ativos virtuais e entrou em vigor em 20 de junho de 2023, introduziu um novo tipo penal no Código Penal: o artigo 171-A. Este artigo representa uma resposta legislativa direta ao crescente

⁸⁷ CAVALI, Marcelo Costenaro. Concurso material de confusões: primeiras impressões sobre os novos tipos penais relativos a fraudes financeiras eletrônicas. In: TOLDO, Nino Oliveira; LACERDA, Fernando Hideo Iochida (orgs.). **Crimes Federais**. São Paulo: Editora Contracorrente, 2023.

⁸⁸ CAVALI, Marcelo Costenaro. Concurso material de confusões: primeiras impressões sobre os novos tipos penais relativos a fraudes financeiras eletrônicas. In: TOLDO, Nino Oliveira; LACERDA, Fernando Hideo Iochida (orgs.). **Crimes Federais**. São Paulo: Editora Contracorrente, 2023.

número de fraudes envolvendo criptoativos e outros instrumentos financeiros digitais⁸⁹.

Diferentemente da fraude eletrônica (§ 2º-A do art. 171 do CP), que é uma qualificação do estelionato, o crime do artigo 171-A apresenta características próprias e independentes, configurando um tipo penal *sui generis*. Embora a técnica legislativa pudesse ter sido mais precisa ao incluí-lo em leis específicas (como a Lei nº 1.521/1951 sobre crimes contra a economia popular ou a Lei nº 7.492/1986 sobre crimes contra o sistema financeiro nacional), sua criação como artigo autônomo no Código Penal denota a intenção de dar-lhe um tratamento específico.

Apesar de ambos os crimes (estelionato e o novo tipo do art. 171-A) envolverem a intenção de obter "vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", há uma distinção crucial. O estelionato, para sua consumação, exige a efetiva obtenção da vantagem indevida e o efetivo prejuízo alheio (é um crime de dano).

Já o novo tipo penal do artigo 171-A não exige a ocorrência de dano patrimonial para sua consumação, sendo suficiente a intenção do agente de obter a vantagem ilícita e a prática das condutas descritas⁹⁰. Isso o caracteriza como um crime de perigo abstrato, em que a mera conduta fraudulenta, com potencial lesivo, já é punível, independentemente do resultado. Tal característica reflete uma política criminal mais preventiva diante da complexidade e do potencial de dano massivo dessas fraudes⁹¹.

É notável a diferença nas penas: enquanto o estelionato simples (crime de dano) prevê reclusão de um a cinco anos, e a fraude eletrônica (modalidade qualificada) de quatro a oito anos, o novo crime do artigo 171-A (crime de perigo) também estabelece pena de quatro a oito anos de reclusão. Essa equiparação de

⁸⁹ CAVALI, Marcelo Costenaro. Concurso material de confusões: primeiras impressões sobre os novos tipos penais relativos a fraudes financeiras eletrônicas. In: TOLDO, Nino Oliveira; LACERDA, Fernando Hideo Iochida (orgs.). **Crimes Federais**. São Paulo: Editora Contracorrente, 2023.

⁹⁰ AMARAL, Rodrigo; LOBATO, José Rodrigo Tavares. Crime de Fraude com Utilização de Ativos Virtuais, Valores Mobiliários ou Ativos Financeiros. **Consultor Jurídico**. Publicado em: 6 out. 2024. Disponível em <https://www.conjur.com.br/2024-out-06/crime-de-fraude-com-utilizacao-de-ativos-virtuais-valores-mobiliarios-ou-ativos-financeiros/#:~:text=1%2D%20O%20artigo%20171%2DA,%2C%20ou%20seja%2C%20crime%20material,Acesso em 05/11/2025>.

⁹¹ CAVALI, Marcelo Costenaro. Concurso material de confusões: primeiras impressões sobre os novos tipos penais relativos a fraudes financeiras eletrônicas. In: TOLDO, Nino Oliveira; LACERDA, Fernando Hideo Iochida (orgs.). **Crimes Federais**. São Paulo: Editora Contracorrente, 2023.

pena entre um crime de perigo e uma modalidade qualificada de estelionato de dano sublinha a gravidade que o legislador atribuiu às fraudes envolvendo ativos virtuais.

A razão para essa pena severa é que o artigo 171-A não visa proteger primariamente o patrimônio individual de uma vítima específica, mas sim o patrimônio de um número indeterminado de pessoas, normalmente por meio de ações voltadas a um público amplo. As condutas tipificadas incluem: a) **Organizar, gerir, ofertar ou distribuir carteiras que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros.** "Carteiras" são entendidas como portfólios de investimentos geridos com o objetivo de rentabilidade, podendo envolver recursos de múltiplas pessoas. Por exemplo, uma empresa que promete altos retornos sobre investimentos em criptomoedas, mas opera de forma fraudulenta, sem lastro real ou com manipulação de mercado; b) **Intermediar operações com esses mesmos ativos, aproximando vendedores, compradores, emprestadores e tomadores.** Isso abrange plataformas de *exchange* ou *brokers* que, ao invés de facilitarem transações legítimas, manipulam preços, executam ordens falsas ou desviam fundos.

Trata-se de um delito que guarda semelhança com a gestão fraudulenta de instituição financeira (art. 4º, *caput*, da Lei nº 7.492/1986). A Lei nº 14.478/2022 também ampliou o conceito de instituição financeira na Lei nº 7.492/1986, para incluir pessoas jurídicas que oferecem serviços relacionados a operações com ativos virtuais, como intermediação, negociação ou custódia. Isso inevitavelmente gerará discussões sobre a correta tipificação de fraudes envolvendo ativos virtuais, criando um complexo cenário de conflito aparente de normas. Em uma análise inicial, aplicando o princípio da especialidade, o crime do artigo 171-A só seria considerado nos casos em que a atuação não configure uma instituição financeira.

Com a expansão do conceito de instituição financeira pela Lei nº 14.478/2022, qualquer pessoa jurídica (ou física que atue como tal) que ofereça oportunidades de investimento em ativos virtuais – seja intermediando, negociando ou custodiando-os – seria considerada instituição financeira para fins penais. Nesse caso, fraudes praticadas por essa entidade seriam enquadradas como gestão fraudulenta (art. 4º, *caput*, da Lei nº 7.492/1986) ou condutas temerárias (art. 4º, parágrafo único, da mesma lei), que preveem penas ainda mais severas e são consideradas crimes mais graves por atingirem a higidez do Sistema Financeiro Nacional.

A sobreposição de tipos penais é evidente: o legislador, ao ampliar o conceito de instituição financeira e criar o artigo 171-A do Código Penal na mesma lei, estabeleceu duas normativas para combater o mesmo problema, com diferentes alcances e penas. Isso soma-se aos tipos penais já existentes, como o estelionato (art. 171, *caput*), a fraude eletrônica (§ 2º-A do art. 171) e o crime contra a economia popular (art. 2º, IX da Lei nº 1.521/1951).

Pode haver ainda a incidência do artigo 7º, inciso IV, da Lei nº 7.492/1986 se os ativos virtuais forem ofertados como contrato de investimento coletivo, o que é comum em esquemas de pirâmide. Importante diferenciar: se não houver negociação real de ativos virtuais, mas apenas um pretexto ilusório para enganar, não haverá gestão fraudulenta ou fraude em operações com ativos virtuais. Por exemplo, se uma "plataforma de investimento" em criptoativos for, na verdade, uma fachada para um "esquema Ponzi" mediante o qual não há compra e venda real de ativos, mas apenas um fluxo de dinheiro de novos investidores para os antigos, o enquadramento poderá ser estelionato simples ou fraude eletrônica, a depender do meio utilizado para a captação.

Uma complicação adicional reside na competência judicial: crimes como estelionato, fraude eletrônica e o novo artigo 171-A, bem como o crime contra a economia popular, geralmente são de competência da Justiça Estadual. Já os crimes da Lei nº 7.492/1986 (crimes contra o sistema financeiro nacional) são de competência Federal. Essa distinção certamente resultará em inúmeros e complexos conflitos de competência, que atrasam a persecução penal, dificultam a coleta de provas e, em última instância, favorecem a impunidade⁹².

Resumindo, as reformas legislativas no Brasil, impulsionadas pela necessidade de modernizar o combate às fraudes digitais e financeiras, demonstraram um ímpeto legislativo positivo e uma preocupação legítima com um problema crescente. No entanto, a execução desse ímpeto pecou pela falta de coesão, clareza e técnica legislativa, resultando em um emaranhado de normas que, em vez de simplificar e fortalecer a justiça, complexificam-na e, paradoxalmente, podem perpetuar a impunidade.

⁹² NUCCI, Guilherme de S. **Curso de Direito Penal** - Vol.2 - 9ª Edição 2025. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*, p. 413. ISBN 9788530996666. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 20 de maio. 2025.

O grande desafio agora é para o Judiciário, que terá a árdua tarefa de harmonizar esse complexo arcabouço normativo, e para futuras reformas legislativas que possam organizar e clarificar o sistema penal para crimes digitais e financeiros. Assim, a referida reforma legislativa, embora represente um avanço na legislação penal para acompanhar a crescente sofisticação dos crimes cibernéticos, levanta questões importantes sobre sua efetividade, alcance e a real proteção que oferece às vítimas de crimes cibernéticos, especialmente em um cenário digital em constante evolução⁹³.

A configuração do estelionato praticado por fraude eletrônica com pena mais severa, reflete a preocupação do legislador com o aumento da sofisticação e do impacto financeiro dos golpes *online*.

A lei, portanto, define dois requisitos essenciais para a configuração do crime qualificado: a) O emprego de fraude com a utilização de informações fornecidas pela vítima ou por terceiro. Este requisito sublinha a importância do engano como elemento central do crime. A vítima, sem saber, contribui para a ação criminosa ao fornecer dados que serão utilizados contra ela; b) A obtenção dessas informações por meio de redes sociais, contatos telefônicos, e-mails fraudulentos ou outros meios fraudulentos análogos. Este requisito delimita os meios pelos quais a fraude é praticada, focando nos canais de comunicação digital mais comuns. A expressão "meios fraudulentos análogos" busca abranger novas tecnologias e táticas que possam surgir.

A ausência de um desses requisitos resulta na configuração do estelionato simples, previsto no *caput* do artigo 171, com uma pena de reclusão de um a cinco anos e multa, significativamente menor do que a pena para a forma qualificada. Essa distinção demonstra a intenção do legislador de punir mais severamente as fraudes eletrônicas que exploram a vulnerabilidade das vítimas no ambiente digital⁹⁴.

⁹³ NUCCI, Guilherme de S. **Curso de Direito Penal** - Vol.2 - 9ª Edição 2025. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*, p. 413. ISBN 9788530996666. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 20 de maio. 2025.

⁹⁴ GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado Direito Penal** - Parte Especial. 12. ed. Rio de Janeiro: Saraiva Jur, 2022. *E-book*, p. 528. ISBN 9786555597738. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555597738/>. Acesso em: 20 de maio. 2025.

3.5.5 Majorantes (art. 171, §§ 3º e 4º)

Dispõe o § 3º do artigo 171 do Código Penal: “A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência”.

A conduta tipificada no referido dispositivo não prevê uma figura qualificada do crime de estelionato, mas sim um aumento de pena que, frequentemente e incorretamente, é considerado como qualificadora pela doutrina⁹⁵. Contudo, é fundamental entender que majorante e qualificadora são conceitos distintos. A pena deve ser aumentada em um terço (§ 3º) quando a infração afeta uma entidade de direito público ou institutos de economia popular, assistência social ou beneficência, conforme a súmula 24 do STJ⁹⁶.

Importante destacar que em direito penal, é inadmissível a interpretação extensiva ou analógica que agrave a situação do réu, incluindo elementos que a lei não prevê. Não se pode justificar o aumento de pena com base em interesses indiretos de entidades públicas administradas por entidades privadas. A exemplo disso, temos o Banco do Brasil S/A, por exemplo, que por ser uma sociedade de economia mista, é uma entidade de direito privado, não se encaixando como “entidade de direito público” mencionada no § 3º do artigo 171.

Por seu turno, o § 4º, trata da majorante para o estelionato cometido contra pessoa idosa. A presente causa especial de aumento de pena foi introduzida no Código Penal pela Lei nº 13.228/15, para a hipótese de cometimento do crime de estelionato contra a pessoa idosa, acrescentando ao artigo 171 do Código Penal a seguinte o § 4º que assim prevê: “aplica-se a pena em dobro se o crime for cometido contra idoso”.

⁹⁵ BITENCOURT, Cezar R. **Código penal comentado**. 10. ed. Rio de Janeiro: Saraiva Jur, 2019. *E-book*, p. 855. ISBN 9788553615704. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553615704/>. Acesso em: 12 de maio. 2025.

⁹⁶ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula nº 24**. “Aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da previdência social, a qualificadora do § 3º, do art. 171 do Código Penal.” Súmulas do STJ. Disponível em: www.stj.jus.br. Acesso em: 13 maio 2025.

Com a publicação e entrada em vigor da lei em 29 de dezembro de 2015, o crime de estelionato cometido contra idosos (pessoas com 60 anos ou mais) passou a ser punido com uma pena de reclusão de 2 a 10 anos e multa. Essa alteração legislativa reflete uma preocupação crescente com a vulnerabilidade dessa faixa etária a golpes e fraudes financeiras. É importante ressaltar que, como já dito, por se tratar de uma norma penal mais severa, ela não se aplica retroativamente a casos ocorridos antes dessa data, em respeito ao princípio constitucional da irretroatividade da lei penal mais gravosa (*nulla poena sine lege*).

Essa nova legislação também impede a aplicação da suspensão condicional do processo, conforme previsto no artigo 89 da Lei nº 9.099/95, para os casos de estelionato contra idosos. A impossibilidade de aplicar esse benefício nesses casos demonstra a intenção do legislador de tratar com maior rigor o estelionato contra idosos.

Um aspecto peculiar é que a lei estabelece um aumento de pena, e não uma qualificação do crime, embora a pena seja significativamente elevada (podendo ser mais que dobrada, dependendo da interpretação do juiz) quando a vítima tem mais de 60 anos (sendo 65 anos o critério considerado em algumas interpretações, seguindo o Estatuto do Idoso⁹⁷). Essa distinção é relevante porque, em geral, crimes qualificados possuem elementos específicos que os diferenciam do crime base, enquanto o aumento de pena é uma circunstância que agrava a punição dentro do mesmo tipo penal.

3.5.6 Ação Penal (art. 171, § 5º)

A redação original do Código Penal estabelecia que a maioria das ações penais referentes ao crime de estelionato (art. 171) era pública incondicionada. Havia exceções específicas, em que a ação era condicionada à representação do ofendido, limitadas a casos em que o crime fosse cometido contra cônjuge judicialmente

⁹⁷ BITENCOURT, Cezar R. **Código penal comentado**. 10. ed. Rio de Janeiro: Saraiva Jur, 2019. *E-book*, p. 856. ISBN 9788553615704. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553615704/>. Acesso em: 12 de maio. 2025.

separado, irmão, tio ou sobrinho que coabitassem com o agente. Essa regra buscava, em parte, preservar relações familiares em delitos de menor potencial ofensivo dentro desse contexto.

Com a promulgação da Lei nº 13.964/2019, conhecida como Lei Anticrime, houve uma mudança significativa: o estelionato passou a ser, em regra, crime de ação penal pública condicionada à representação do ofendido⁹⁸. Essa alteração abrange não apenas o tipo básico previsto no *caput* do artigo 171, mas também as formas privilegiadas (§ 1º) e equiparadas (§§ 2º, 3º e 4º) do delito. O objetivo principal dessa mudança foi desafogar o sistema de justiça criminal, transferindo a decisão de iniciar a persecução penal para a vítima em casos que não envolvem especial vulnerabilidade ou interesse público direto, permitindo que o Estado concentre seus recursos em crimes mais graves. A "representação" aqui significa a manifestação formal da vítima ou de seu representante legal, demonstrando interesse em que a investigação e o processo criminal prossigam⁹⁹.

É de suma importância compreender a natureza dessa alteração. Mudanças na natureza da ação penal são consideradas normas de caráter híbrido, pois possuem reflexos tanto no direito processual penal (condição de procedibilidade) quanto no direito penal material (introdução de causas extintivas da punibilidade, como a decadência e a renúncia). Devido a esse caráter híbrido e por serem mais benéficas ao réu (*lex mitior*), as novas regras de ação penal para o estelionato são aplicáveis retroativamente, alcançando fatos ocorridos antes da vigência da Lei Anticrime, desde que não haja trânsito em julgado da sentença penal condenatória¹⁰⁰.

Para os fatos criminosos de estelionato ocorridos antes da entrada em vigor da Lei nº 13.964/2019, e cujos processos ainda estavam em andamento (sem denúncia oferecida ou com denúncia oferecida, mas sem sentença transitada em julgado), o artigo 90 da Lei nº 9.099/95 (aplicado por analogia conforme entendimento

⁹⁸ SALVADOR NETTO, Alamiro Velludo; BRUNI, Aline T.; AMARAL, Cláudio do P.; SAAD-DINIZ, Eduardo; HERME. **Pacote Anticrime** - Comentários à Lei N. 13.964/2019. São Paulo: Almedina Brasil, 2020. *E-book*, p. 30. ISBN 9786556270579. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786556270579/>. Acesso em: 21 mai. 2025.

⁹⁹ GONÇALVES, Victor Eduardo R. **Curso de Direito Penal** - Parte Especial Vol.2 - 8ª Edição 2024. 8. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*, p. 337. ISBN 9788553620982. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553620982/>. Acesso em: 21 mai. 2025.

¹⁰⁰ ESTEFAM, André. **Direito Penal** - Parte Especial Vol.2 - 11ª Edição 2024. 11. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*, p. 614. ISBN 9788553620685. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553620685/>. Acesso em: 20 de maio. 2025.

jurisprudencial) determina a necessidade de intimação da vítima para que manifeste seu interesse em apresentar a representação no prazo decadencial de 30 dias. Caso a vítima, após intimada, não apresente a representação dentro deste prazo, ocorrerá a decadência do direito de representar, resultando na extinção da punibilidade do agente^{101 e 102}.

Inicialmente, houve divergências interpretativas entre as Turmas de Direito Penal do Superior Tribunal de Justiça (STJ) sobre o marco temporal para a aplicação da nova regra em casos pretéritos^{103 e 104}.

Contudo, a 3ª Seção do STJ pacificou o entendimento no sentido de que a necessidade de representação só se aplica se a denúncia ainda não havia sido oferecida antes da vigência da nova lei (23/01/2020). Para os processos em que a denúncia já havia sido apresentada antes dessa data, considerou-se o ato jurídico perfeito da propositura da ação penal, mantendo-se a natureza incondicionada da ação, em respeito ao princípio do *tempus regit actum* no que tange aos atos processuais já praticados¹⁰⁵.

Ressalta-se, contudo, que o estelionato permanece como crime de ação penal pública incondicionada em algumas hipóteses específicas, mesmo após a Lei Anticrime. São elas: I) Se a vítima for a Administração Pública (direta ou indireta), em razão do interesse público na proteção do patrimônio estatal; II) Se a vítima for criança ou adolescente, em razão de sua vulnerabilidade presumida e da necessidade de proteção especial; III) Se a vítima for pessoa com deficiência mental, pela mesma razão de vulnerabilidade e necessidade de proteção; IV) Se a vítima for idoso com idade igual ou superior a 70 (setenta) anos ou incapaz, também pela presunção de maior vulnerabilidade.

¹⁰¹ Vale destacar que não se exige formalidade para a representação, bastando a demonstração inequívoca da vontade de ver o agente processado.

¹⁰² STF. SUPREMO TRIBUNAL FEDERAL. **HC 208.817**, rel. Min. Cármen Lúcia, j. 13-4-2023.

¹⁰³ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 573.093/SC**, rel. Min. Reynaldo Soares da Fonseca, 5ª T., j. 9-6-2020, DJe 18-6-2020

¹⁰⁴ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 583.837**, rel. Min. Sebastião Reis Júnior, j. 4-8-2020.

¹⁰⁵ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 610.201/SP**, rel. Min. Ribeiro Dantas, j. 24-3-2021.

Nesses casos excepcionais, a persecução penal independe da manifestação de vontade da vítima, cabendo ao Ministério Público promover a ação penal de forma incondicionada, visando a proteção de grupos vulneráveis ou do interesse público¹⁰⁶.

Contudo, essa delineação legal suscita uma análise crítica, posto que a redação legal, ao detalhar as exceções, parece contrariar o axioma de que a lei penal não conteria palavras inúteis (*verba cum effectum sunt accipienda*). De fato, a inclusão expressa de "criança e adolescente" e "pessoas com deficiência" após a menção genérica a "incapazes" soa como uma redundância desnecessária.

No ordenamento jurídico brasileiro, a categoria de "incapazes" já abrange, por força de lei (e.g., Código Civil, Estatuto da Criança e do Adolescente – Lei nº 8.069/90, Estatuto da Pessoa com Deficiência – Lei nº 13.146/15), indivíduos que não possuem discernimento pleno para atos da vida civil ou que necessitam de proteção especial. Por exemplo, menores de 16 anos são considerados absolutamente incapazes, e entre 16 e 18 anos, relativamente incapazes, assim como pessoas com certas deficiências que afetem sua capacidade de exprimir vontade. Tal prolixidade legislativa poderia ter sido evitada com uma formulação mais concisa, como "incapazes e vulneráveis", ou simplesmente "incapazes", que por interpretação sistemática já incluiria as demais categorias, minimizando potenciais ambiguidades interpretativas¹⁰⁷.

Ademais, a possibilidade de estender essa regra, considerada mais benéfica (*lex mitior*), a outros delitos patrimoniais análogos, como o furto (art. 155 do Código Penal), mostra-se questionável e, a nosso ver, descabida. O silêncio do legislador a respeito de tais extensões não deve ser interpretado como uma lacuna a ser preenchida por analogia (*analogia in bonam partem*), mas sim como uma escolha deliberada de restringir a nova modalidade de ação penal ao estelionato. Em direito penal, vigora o princípio da legalidade estrita (*nullum crimen, nulla poena sine praevia lege*), que impede a aplicação analógica de normas incriminadoras ou de restrição de direitos.

¹⁰⁶ FIGUEIREDO, Patrícia V.; JUNQUEIRA, Gustavo OD.; FULLER, Paulo H A.; e outros. **Lei Anticrime Comentada** - 2ª Edição 2021. 2. ed. Rio de Janeiro: Saraiva Jur, 2021. *E-book*, p. 30. ISBN 9786555595512. Disponível em:

<https://integrada.minhabiblioteca.com.br/reader/books/9786555595512/>. Acesso em: 21 mai. 2025.

¹⁰⁷ BITENCOURT, Cezar R. **Tratado de direito penal: parte especial**. v. 3. 20. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*, p. 316. ISBN 9788553622436. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788553622436/>. Acesso em: 03 nov. 2025.

Embora a norma em questão seja processual penal, ela possui caráter material por afetar a *punibilidade* e a *persecução penal*, devendo ser interpretada restritivamente, especialmente quando se trata de exceções à regra geral. A ausência de previsão expressa para outros crimes patrimoniais reforça o caráter *numerus clausus* das hipóteses de ação penal condicionada.

A razão fundamental para essa distinção reside na peculiaridade intrínseca do estelionato: a invariável, ainda que por vezes sutil, participação da vítima no ardil que culmina no prejuízo. Diferentemente do furto, em que há uma subtração sem consentimento da vítima, ou do roubo, que envolve violência ou grave ameaça, no estelionato o agente induz ou mantém a vítima em erro, levando-a a realizar uma disposição patrimonial voluntária em seu próprio prejuízo ou de terceiro.

Essa característica singular, que frequentemente turva as fronteiras entre a mera astúcia civil e a conduta criminosa, dificultando a exata delimitação entre o moralmente legítimo e o ilícito, é o que o diferencia de outros crimes contra o patrimônio. A complexidade dessa distinção, sublinha a natureza *sui generis* do estelionato, mediante o qual o dolo específico do agente em enganar e a *colaboração* da vítima, ainda que viciada, são elementos cruciais, que justificam o tratamento legislativo diferenciado conferido a este delito.

No que concerne à competência para julgamento da ação penal, a atenção maior se inclina para o estelionato praticado contra a administração pública, em que a competência para julgamento vai depender da classificação quanto à pessoa federativa do ente da administração pública lesado, seja federal, estadual, municipal ou distrital. Caso seja o crime de estelionato cometido em detrimento de órgão da administração pública federal, a competência será da Justiça Federal, se estadual ou municipal, a competência será da Justiça Estadual e se for contra órgão distrital, a competência para julgamento será da Justiça Comum do Distrito Federal e Territórios.

Especial destaque deve ser dado ao patrimônio da União, de suas autarquias e empresas federais, que representa o interesse público e a coletividade e que, frequentemente, se torna alvo de condutas delituosas. Tais fraudes buscam obter vantagem ilícita em detrimento do erário ou de fundos geridos por essas entidades e, em razão de suas particularidades estão na esfera da competência da Justiça Federal, nos termos do artigo 109 da Constituição Federal. Um exemplo notório e recorrente é a fraude na obtenção de empréstimos consignados junto à Caixa Econômica Federal.

Nesses casos, criminosos se valem do uso de documentos falsificados ou dados de terceiros¹⁰⁸, muitas vezes sem o conhecimento da vítima, para simular a contratação de crédito e desviar os valores, gerando não apenas prejuízo financeiro à instituição, mas também graves transtornos aos cidadãos lesados. Entretanto, deve-se atentar que já foi sumulado pelo Superior Tribunal de Justiça que, em caso de estelionato praticado mediante falsificação de guias de recolhimento das contribuições previdenciárias, sem que haja lesão à autarquia federal, a competência para julgamento será da Justiça Estadual¹⁰⁹.

Contudo, a maior incidência de casos de estelionato sob a competência da Justiça Federal concentra-se no âmbito da autarquia previdenciária, o Instituto Nacional do Seguro Social (INSS). O estelionato previdenciário, tipificado no § 3º do artigo 171 do Código Penal, configura-se pela obtenção indevida de benefícios assistenciais ou previdenciários – tais como aposentadorias (por idade, tempo de contribuição, invalidez), pensões por morte, auxílios-doença, auxílios-reclusão, salário-maternidade ou o Benefício de Prestação Continuada (BPC/LOAS) – mediante a utilização de fraude. Essa fraude pode manifestar-se por meio de declarações falsas, omissão de informações relevantes, apresentação de documentos adulterados ou falsificados, ou qualquer outro ardil que induza o INSS a erro na concessão ou manutenção do benefício.

É fundamental sublinhar que a Constituição Federal de 1988, em seu artigo 7º, reconhece os direitos previdenciários como direitos sociais fundamentais, essenciais para a dignidade da pessoa humana e a garantia de um mínimo existencial. Complementarmente, o artigo 195 da mesma Carta Magna estabelece as fontes de custeio da Seguridade Social, visando a assegurar a sustentabilidade e a perenidade desses benefícios para toda a sociedade. Desse modo, qualquer prejuízo ao patrimônio do INSS, provocado por fraudes destinadas à aquisição ou manutenção indevida de benefícios, não representa apenas uma perda financeira, mas uma

¹⁰⁸ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **ACR 5056950-87.2013.4.04.7000/PR**, 8ª Turma, Des. Federal LEANDRO PAULSEN, jun./2016.

¹⁰⁹ “Compete à Justiça Comum Estadual processar e julgar crime de estelionato praticado mediante falsificação de guias de recolhimento das contribuições previdenciárias, quando não ocorrente lesão à autarquia federal”. STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula 107**. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2010_7_capSumula107.pdf Acesso em: 6 out. 2025.

transgressão direta e indireta a esses direitos sociais fundamentais e ao pacto de solidariedade que sustenta o sistema previdenciário.

Diante da natureza pública dos recursos envolvidos e da relevância social dos bens jurídicos tutelados – que transcendem a mera lesão patrimonial e atingem a credibilidade e a sustentabilidade do sistema de Seguridade Social –, a aplicação do princípio da insignificância ao estelionato previdenciário é tratada com extrema cautela pela jurisprudência. Sua admissão deve ser reservada a situações excepcionálssimas, em que a lesão patrimonial seja comprovadamente irrisória, desprovida de qualquer reprovabilidade social e que não comprometa a confiança no sistema, considerando-se não apenas o valor monetário, mas o impacto qualitativo da conduta no bem jurídico protegido. Assim decidiu o TRF4, na ACR 5000839-31.2010.404.7213/2014¹¹⁰.

Um ponto crucial a ser analisado diz respeito à natureza do estelionato previdenciário. Sua caracterização pode variar significativamente, dependendo de quem o pratica, de quem se beneficia e da forma como a fraude é executada. A jurisprudência brasileira, tanto do Supremo Tribunal Federal (STF) quanto do Superior Tribunal de Justiça (STJ), estabelece uma importante distinção entre o agente que comete a fraude para obter o benefício previdenciário para si mesmo e aquele que fraudula o sistema para que outra pessoa receba a vantagem indevida.

No primeiro cenário, quando a fraude é perpetrada pelo próprio beneficiário, que passa a receber e manter o benefício de forma contínua, a conduta é classificada como crime permanente. Isso significa que a lesão ao bem jurídico (o patrimônio da Previdência Social) se prolonga no tempo, e o agente tem a capacidade de interromper a situação ilícita a qualquer momento. Tanto o STF quanto o STJ têm entendimento pacífico nesse sentido.

O STF já afirmou que a prática de crime por parte do beneficiário da previdência, considerada relação jurídica continuada, é enquadrável como crime permanente, posto que se renova face a periodicidade do benefício¹¹¹. De forma

¹¹⁰ “Não é possível a aplicação do princípio da insignificância ao crime de estelionato cometido contra a Previdência Social, independentemente dos valores obtidos indevidamente pelo agente, pois, segundo jurisprudência majoritária do E. STJ e E. STF, em se tratando de estelionato contra entidade de direito público, considera-se o alto grau de reprovabilidade da conduta do agente, que atinge a coletividade como um todo”. TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **ACR 5000839-31.2010.404.7213**, 8a TURMA, Des. Federal LEANDRO PAULSEN, jun./2014.

¹¹¹ STF. SUPREMO TRIBUNAL FEDERAL. **HC 99.112**, rel. Min. MARCO AURÉLIO, 1ª T., 2010.

similar, o STJ também consolidou o entendimento de que o estelionato praticado contra a Previdência Social (art. 171, § 3º, do CP), em relação ao beneficiário, é crime permanente, cuja consumação ocorre a cada saque feito indevidamente, e não no recebimento da primeira parcela da prestação previdenciária¹¹².

Portanto, o prazo prescricional para a pretensão punitiva do Estado começa a contar a partir do momento em que cessa a permanência, ou seja, quando o último saque indevido é realizado ou o benefício é interrompido. Já na segunda situação, mediante o qual o crime é cometido para favorecer uma terceira pessoa, a natureza jurídica é diferente.

Nesses casos, o delito é considerado instantâneo com efeitos permanentes. Isso significa que a consumação do crime ocorre no momento em que a primeira parcela do benefício é recebida indevidamente pelo terceiro, ainda que os pagamentos continuem ao longo do tempo. Assim, o marco inicial para a contagem do prazo prescricional da pretensão punitiva estatal é a data do efetivo recebimento da primeira parcela do benefício fraudulento^{113 e 114}.

Há, ainda, uma terceira e complexa situação que se destaca no cenário do estelionato previdenciário: aquela em que um terceiro, após o falecimento do beneficiário, e sem que o Instituto Nacional do Seguro Social (INSS) tenha sido notificado do óbito, continua a efetuar saques do benefício utilizando o cartão magnético do falecido. A natureza jurídica dessa conduta (se constitui um crime permanente ou instantâneo), ainda é objeto de intensa discussão nos tribunais, com implicações diretas na contagem da prescrição e na aplicação da lei penal.

O Tribunal Regional Federal da 4ª Região (TRF4), por exemplo, tem se posicionado no sentido de que o agente, ao realizar saques mensais, age com desígnios autônomos a cada vez. Assim, considera que há uma série de fraudes reiteradas sob as mesmas condições de tempo, lugar e modo de execução, o que remete à figura da continuidade delitiva (art. 71 do Código Penal). Conforme decidido nos Embargos de Nulidade e Infringentes (ENUL) 5000855-24.2010.4.04.7103, cada

¹¹² STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 247.408/RJ**, rel. Min. GURGEL DE FARIA, 5ª T., 2015.

¹¹³ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **EDecI AgRg REsp 1651521**, rel. Min. JORGE MUSSI, 5ª Turma, 2017

¹¹⁴ STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **AgRg no REsp 1112184/RS**, rel. Min. ROGERIO SCHIETTI CRUZ, 6ª Turma, 2015.

saque é classificado como um crime instantâneo, pois cada ato de retirada do dinheiro representa uma nova lesão ao patrimônio do INSS e uma nova manifestação da vontade criminosa do agente. A sucessão de saques, por sua vez, configura a continuidade delitiva, resultando na aplicação de uma pena única, aumentada de um sexto a dois terços, em vez de um concurso material de crimes, que somaria as penas individualmente¹¹⁵.

Entretanto, a tese que defende a natureza de crime permanente para essa conduta também possui argumentos consistentes e já foi acolhida pelo próprio TRF4 em outros momentos¹¹⁶. Os defensores dessa corrente argumentam que a essência da fraude reside na omissão – ou seja, na deliberada falta de comunicação do óbito do beneficiário ao INSS. Essa omissão induziria a autarquia a erro, levando-a a continuar depositando valores para um segurado já falecido.

Dessa forma, o agente (geralmente um parente ou pessoa próxima do falecido) apropria-se indevidamente desses valores. Segundo essa perspectiva, não haveria um novo "desígnio autônomo" a cada saque, mas sim a manutenção de uma situação fraudulenta iniciada pela omissão inicial. O agente, enquanto "beneficiário" da fraude e ciente do falecimento, teria o poder de fazer cessar a conduta ilícita a qualquer momento, seja comunicando o óbito ao INSS, seja pela inércia nos saques por período superior a 60 dias (conforme o art. 166, § 3º, do Decreto nº 3.048/99), característica típica dos crimes permanentes.

A principal implicação dessa tese é que o prazo prescricional não começa a correr enquanto a situação ilícita perdura, ou seja, enquanto os saques continuam ou a omissão do óbito não é sanada. É possível ainda cogitar que, se considerarmos que cada saque implica um desígnio autônomo, a conduta poderia se enquadrar mais adequadamente no delito de furto qualificado pelo emprego de fraude (art. 155, § 4º, II, do Código Penal). Isso porque o agente estaria, a cada mês, subtraindo "coisa alheia móvel" (o dinheiro depositado), valendo-se da fraude consistente no uso indevido do cartão de terceiro.

¹¹⁵ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **ENUL 5000855-24.2010.4.04.7103**, 4ª Seção, rel. Des. Fed. JOÃO PEDRO GEBRAN NETO, dez./2015. 51 TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 012145-58.2009.404.7200**, 8ª T., Juíza Federal SIMONE BARBISAN FORTES, fev./2015.

¹¹⁶ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 012145-58.2009.404.7200**, 8ª Turma, Juíza Federal SIMONE BARBISAN FORTES, fev./2015.

A distinção crucial aqui reside no fato de que, no estelionato, a vítima é induzida a erro e entrega voluntariamente o bem; no furto mediante fraude, a fraude é utilizada para diminuir a vigilância da vítima e possibilitar a subtração, sem que haja uma entrega voluntária. Neste cenário, o INSS não entrega o dinheiro ao agente, mas o deposita na conta do falecido, e o agente o subtrai usando o cartão.

A classificação legal de um crime como permanente, instantâneo ou furto qualificado possui repercussões significativas tanto para a análise da prescrição da pretensão punitiva quanto para a aplicação das regras do concurso de crimes ou continuidade delitiva. Em um crime permanente, o prazo prescricional não começa a correr enquanto a situação ilícita perdura, sendo a conduta considerada única. Já nos crimes instantâneos, a prescrição inicia-se de imediato, mas a repetição de condutas pode levar ao reconhecimento da continuidade delitiva, que, embora unifique a pena, ainda se baseia em crimes que se exaurem no tempo. Importante ressaltar que, se o benefício supostamente fraudulento for posteriormente concedido ou revalidado por via judicial, a ausência de "vantagem ilícita" e de "prejuízo alheio" descaracteriza o estelionato, não havendo justa causa para a persecução penal, pois faltam elementos essenciais do tipo penal¹¹⁷.

Independentemente da modalidade, o estelionato previdenciário atrai, invariavelmente, a aplicação do § 3º do artigo 171 do Código Penal. Este dispositivo prevê um aumento de pena de um terço quando o crime é cometido em prejuízo de entidade de direito público – como o INSS –, ou de institutos de economia popular, assistência social ou beneficência, qualificando-o como estelionato majorado¹¹⁸. Essa majorante reflete a maior reprovabilidade da conduta que prejudica a coletividade.

No que tange aos meios fraudulentos empregados, a falsidade ideológica é frequentemente utilizada, como a adulteração de documentos para simular a sobrevivência do beneficiário. Contudo, se a falsificação esgota sua potencialidade lesiva na consumação do estelionato, ela será absorvida por este último, aplicando-se o princípio da consunção. Não haverá, nesse caso, concurso de crimes, mas a

¹¹⁷ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 5000196-96.2012.404.7118**, Des. Federal LEANDRO PAULSEN, 8ª Turma, out./2015.

¹¹⁸ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 5011701-17.2012.404.7205**, Des. Federal LEANDRO PAULSEN, 8ª Turma, set./2015.

responsabilização ocorrerá apenas pelo estelionato, visto que o falso foi o "crime-meio", um mero instrumento para a obtenção da vantagem ilícita¹¹⁹.

Entretanto, o princípio da consunção não se aplica quando a potencialidade lesiva do documento falso não se exaure na prática do estelionato. O STF já decidiu que, se os documentos falsificados podem ser reutilizados para outros delitos (como falsificações em série para fraudar múltiplas instituições financeiras ou obter outros benefícios), a falsidade ideológica não é absorvida, e os crimes coexistem em concurso formal ou material, a depender da situação¹²⁰.

Ademais, não são raros os casos em que se identificam verdadeiras associações criminosas, com a participação de "agenciadores", "intermediários" e até mesmo de servidores da própria autarquia, que atuam em conjunto para a concessão fraudulenta de um grande número de benefícios. Essas organizações criminosas podem ser responsabilizadas pelo crime de associação criminosa (art. 288 do Código Penal) ou organização criminosa (Lei nº 12.850/2013), além dos estelionatos praticados. Embora tal contexto possa lançar uma sombra sobre a lisura dos benefícios concedidos por determinada agência ou servidor, é fundamental que cada caso seja analisado individualmente, distinguindo quais benefícios foram objeto da ação criminosa e quais não foram, o que é especialmente relevante para a responsabilização penal dos beneficiários¹²¹ e para evitar a revogação indevida de benefícios legítimos.

No contexto do estelionato previdenciário, dado que o montante do prejuízo causado ao patrimônio do INSS é sempre passível de aferição e quantificação, a condenação frequentemente implica a obrigação de indenizar o dano, conforme previsto no artigo 91, I, do Código Penal. Essa indenização visa a recompor o erário do valor indevidamente apropriado, atualizado monetariamente.

¹¹⁹ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 005658-39.2004.404.7009**, 8ª Turma, Juíza Federal SIMONE BARBISAN FORTES, por unanimidade, fev./2015.

¹²⁰ STF. SUPREMO TRIBUNAL FEDERAL. **HC 116979 AgR**, rel. Min. ROSA WEBER, 1ª Turma, out./2013.

¹²¹ TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 5000772-72.2010.404.7114**, Des. Federal LEANDRO PAULSEN, 8ª Turma, jun./2014.

3.6 Análise crítica da tipificação penal do estelionato eletrônico

Cerne do objeto de nosso estudo, a figura do estelionato qualificado praticada com utilização de fraude eletrônica, foi introduzida pela Lei nº 14.155/2021 e representou um marco legal fundamental para o enfrentamento do crescente volume de fraudes praticadas por meios eletrônicos e informáticos. Essa lei buscou adequar o tipo penal do estelionato à realidade digital, em que a criação de armadilhas virtuais para enganar pessoas se tornou mais sofisticada e disseminada, especialmente considerando a maior exposição dos indivíduos a essas situações pelas inovações tecnológicas. É notório que a vasta maioria das transações bancárias, comerciais e pessoais são realizadas hoje pela internet, aplicativos móveis e outros meios digitais, muitas vezes sem qualquer interação física¹²².

Observamos com isso que a incessante marcha da tecnologia tem redefinido os alicerces da interação humana, projetando-nos para uma era de conectividade sem precedentes, em que as fronteiras geográficas se desvanecem e o acesso à informação se torna um pilar inseparável da existência no século XXI. Contudo, essa digitalização profunda da sociedade com a realização de negócios exclusivamente *online*, embora revolucionária, carrega consigo um paradoxo sombrio: a mesma plataforma que impulsiona o progresso é perversamente utilizada como vetor para a criminalidade cibernética, tornando a proteção das informações e a segurança digital uma urgência inadiável frente à proliferação global de novas e variadas fraudes virtuais como *ransomware*, *data breaches*, *phishing*, *smishing*, criação de sites falsos (*spoofing*), uso de perfis falsos em redes sociais, entre outros.

Neste cenário de evolução vertiginosa do ciberespaço, a resposta legislativa tem se mostrado notavelmente reativa e, por vezes, aquém do desafio. O legislador penal, numa tentativa tardia de alcançar o ritmo do crime digital, frequentemente recorre a estratégias punitivistas que se enquadram na prevenção geral negativa, ou seja, na intimidação por meio do endurecimento das penas. Essa abordagem, é uma aposta em "práticas de criminologia e segurança pública comprovadamente

¹²² NUCCI, Guilherme de S. **Curso de Direito Penal** - Vol.2 - 9ª Edição 2025. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*, p. 413. ISBN 9788530996666. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 20 mai. 2025.

falidas"¹²³, que se manifestam no aumento abstrato de penas e na elevação de frações para a progressão de regime, configurando uma retórica de intimidação psicológica que ignora a complexidade do fenômeno criminal.

Para o crime cibernético, essa ineficácia é ainda mais acentuada, pois os criminosos digitais frequentemente operam transnacionalmente, valem-se de anonimato e são motivados por ganhos financeiros substanciais, tornando a simples ameaça de uma pena mais alta um dissuasor fraco diante da dificuldade de identificação e extradição.

Com esse viés, a lei veio, portanto, para tipificar de forma mais clara e com pena mais severa o estelionato praticado por esses meios. A pena cominada para o estelionato praticado mediante fraude eletrônica, conforme previsto no § 2º-A do artigo 171 do Código Penal (introduzido pela Lei nº 14.155/2021), é de reclusão, de 4 a 8 anos, além de multa. Essa qualificadora se aplica quando a fraude é cometida utilizando informações fornecidas pela vítima ou por terceiros induzidos a erro por meio de redes sociais, contatos telefônicos, envio de *e-mails* fraudulentos, ou quaisquer outros meios eletrônicos, digitais ou informáticos semelhantes. A lei reconhece a gravidade intrínseca desse tipo de delito, dada a facilidade de execução em massa e a dificuldade inicial de rastreamento¹²⁴.

Por isso, a lei busca punir com mais rigor os casos em que a vítima é induzida a fornecer informações que facilitam a ação do criminoso, que explora a sua confiança ou a sua falta de conhecimento técnico.

Contudo, a redação do dispositivo pode gerar interpretações restritivas, limitando sua aplicação em casos complexos de fraude eletrônica, em que as técnicas utilizadas pelos criminosos são cada vez mais sofisticadas, difíceis de rastrear e nem sempre necessita de informação fornecida pela vítima, ficando evidenciada uma das limitações da lei, como é o caso do *hacker* que invade a conta de *e-mail* da vítima, explorando uma vulnerabilidade de segurança ou utilizando técnicas de *phishing* para obter a senha, e obtém dados para aplicar um golpe, como enviar *e-mails* fraudulentos para os contatos da vítima solicitando dinheiro ou informações pessoais.

¹²³ AMARAL, Cláudio do Prado. **Pacote Anticrime** – Comentários à Lei nº 13.964/2019. São Paulo: Almedina, 2020, p. 8.

¹²⁴ GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado Direito Penal** - Parte Especial. 12. ed. Rio de Janeiro: Saraiva Jur, 2022. *E-book*, pág.529. ISBN 9786555597738. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555597738/>. Acesso em: 20 de maio. 2025.

Nesse caso, a princípio, não se configura o crime qualificado, mas sim o delito simples, pois a vítima não forneceu as informações diretamente ao criminoso, mas sim teve seus dados acessados de forma ilícita. Essa distinção pode ser questionável, uma vez que a vítima teve seus dados expostos devido a uma falha de segurança explorada pelo *hacker*, e a ausência da qualificadora pode não refletir a gravidade do dano causado, que pode incluir prejuízos financeiros, danos à reputação e exposição de informações confidenciais.

No entanto, é importante ressaltar que o *hacker* pode responder por outros crimes, como invasão de dispositivo informático (art. 154-A do Código Penal), que antes focava na violação de mecanismo de segurança, agora abrange a obtenção de dados sem autorização, mesmo que o dispositivo não esteja protegido, e pode incluir a instalação de *malware* ou a exploração de vulnerabilidades e o furto de dados (art. 155, § 4º, do Código Penal)¹²⁵, que ganhou uma agravante quando praticado mediante fraude eletrônica, visando a subtração de valores ou ativos financeiros. Nesse particular, percebe-se que embora a intenção seja combater a criminalidade digital, a essência da mudança da lei reside primariamente na elevação das sanções.

Assim, voltando à análise do tipo introduzido no artigo 171, § 2º-A do Código Penal – o “estelionato eletrônico” – que é o tema do nosso estudo, vejo que numa visão mais crítica, fica evidente que essa não é a criação de um novo tipo penal de estelionato, mas uma mera delimitação dos *meios* e *espaços* de sua execução, o que confere maior reprovação à conduta sem, de fato, inovar na conceituação do delito digital. A redação, ao retomar a expressão “qualquer outro meio fraudulento análogo”, espelha o *caput* do artigo 171 original, e falha em incorporar a manipulação do computador ou da rede como núcleo da infração.

Essa omissão é crucial, pois impede uma tipificação mais abrangente e adaptada às múltiplas facetas das fraudes digitais. Por exemplo, enquanto o *phishing* (uma forma de *social engineering* que manipula a vítima) é claramente coberto, uma fraude que explore uma vulnerabilidade técnica em um sistema de pagamento sem qualquer interação humana direta – uma manipulação puramente técnica do sistema – pode não se encaixar perfeitamente, pois o foco da lei ainda recai sobre a indução

¹²⁵ GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado Direito Penal** - Parte Especial. 12. ed. Rio de Janeiro: Saraiva Jur, 2022. *E-book*, pág.529. ISBN 9786555597738. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555597738/>. Acesso em: 12 de maio. 2025.

ao erro da vítima humana. Essa lacuna já era vislumbrada na proposta de Eduardo Azeredo em 2013 (PL 5485/2013)¹²⁶, que buscava tipificar a manipulação digital em si, reconhecendo a distinção entre a fraude contra a pessoa e a fraude contra o sistema.

Em consequência, a dificuldade prévia dos tribunais em classificar essas condutas como atípicas ou de adaptar a legislação existente evidencia a necessidade de um tipo penal robusto. Contudo, a Lei nº 14.155, ao invés de mergulhar na especificidade da manipulação digital, optou por uma abordagem mais superficial. Isso sugere que o legislador ainda patina em sua adaptação às novas tendências criminosas no ciberespaço, deixando os juízes, mais uma vez, dependentes da analogia para interpretar e aplicar a lei em face da inovação criminosa, o que é problemático no direito penal devido ao princípio da estrita legalidade (*nullum crimen sine lege*).

O que se observa é uma prevalência do "direito penal simbólico" – uma resposta estatal que, focada no aumento de penas, alimenta um sistema prisional já superlotado e contribui para a hiperinflação legislativa. É uma criminologia retrógrada que aposta na repressão excessiva, desconsiderando que os incentivos ao crime frequentemente transcendem a capacidade dissuasória da lei penal.

A Lei nº 14.155, ao essencialmente dobrar as penas do estelionato comum para o eletrônico, representa mais uma atualização punitiva do que uma verdadeira evolução conceitual, em contraste com a legislação espanhola.

Na Espanha, o Código Penal (arts. 248 e 249)¹²⁷ tipifica especificamente a "fraude informática" (fraude informático), que abrange a manipulação de dados ou programas informáticos para obter um lucro indevido, sem a necessidade de enganar diretamente uma pessoa. Essa abordagem equipara o *quantum* de pena para estelionato comum e informático, com agravantes específicas para contextos de maior

¹²⁶ CÂMARA DOS DEPUTADOS. **Projeto Lei nº 5485/2013**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=575520>. Acesso em: 19 out. 2025.

¹²⁷ BOE. BOLETIM OFICIAL DEL ESTADO. **Ley Orgánica 10/1995, de 23 de noviembre**, del Código Penal. Espanha. Disponível em: <https://www.boe.es/eli/es/lo/1995/11/23/10>. Acesso em: 19 out. 2025.

gravidade, demonstrando uma compreensão mais profunda do *modus operandi* dos crimes digitais e uma adaptação legislativa mais harmoniosa e eficaz.

Em suma, a meu ver, a legislação brasileira, embora reativa, ainda carece de uma visão crítica e estrutural que realmente compreenda e combata a complexidade do crime na era digital, o que impacta diretamente a capacidade de investigação, a coleta de evidências digitais e a efetiva punição dos criminosos.

4 A FRAUDE ELETRÔNICA

Um levantamento elaborado para o relatório semestral Global de Tendências de Fraude Omnichannel da TransUnion, referente ao primeiro semestre de 2025, indicou que 40% dos cidadãos brasileiros já foram expostos a tentativas de fraude por e-mail, internet, telefone ou mensagens de texto, resultando em consideráveis perdas financeiras.

Essas tentativas abrangem desde e-mails de *phishing* com *links* maliciosos até chamadas telefônicas fraudulentas e mensagens de texto que buscam induzir o usuário a revelar informações confidenciais ou realizar pagamentos indevidos. Os dados também revelaram que 53% dos entrevistados globalmente sofreram esquemas fraudulentos por canais como *e-mail*, internet, telefone e mensagens de texto entre agosto e dezembro de 2024.

Alguns dos respondentes sequer perceberam que haviam sido alvo desses golpes, o que sublinha a sofisticação crescente dos fraudadores e a necessidade urgente de maior conscientização e educação digital. O Brasil registrou um índice de fraude digital de 5,4% em 2024, superior à média global, posicionando-se ao lado de países como Canadá, Colômbia, República Dominicana, Hong Kong, Índia e Filipinas. Isso indica um cenário desafiador para a segurança digital no país, que exige atenção contínua e investimentos em infraestrutura de proteção¹²⁸.

Conforme o estudo, o golpe mais frequente é o *vishing*, uma fusão dos termos *voice* e *phishing*, no qual criminosos realizam chamadas telefônicas simulando representar companhias legítimas, como operadoras de celular, planos de saúde, bancos ou instituições financeiras. Utilizando técnicas de *social engineering* e, por vezes, *caller ID spoofing* para mascarar o número de origem, o objetivo é persuadir a vítima a fornecer informações confidenciais, como senhas bancárias, números de cartão de crédito, CPF, dados de acesso a contas e outros dados pessoais. A urgência e o medo são frequentemente explorados para manipular as vítimas¹²⁹.

¹²⁸ TRANSUNION. **Relatório de Tendências de Fraude Omnichannel 2025**. Disponível em: <https://www.transunion.com.br/report/fraude-report-h1-2025>. Acesso em: 27 out. 2025.

¹²⁹ TRANSUNION. **Relatório de Tendências de Fraude Omnichannel 2025**. Disponível em: <https://www.transunion.com.br/report/fraude-report-h1-2025>. Acesso em: 27 out. 2025.

O relatório também indicou que os ambientes de comunidades, como sites de relacionamentos e fóruns virtuais, registraram a maior taxa global de tentativas suspeitas de fraude digital em 2024. Nesses ambientes encontram-se alvos atraentes devido à natureza de confiança e interação entre os usuários, o que favorece a prática de estelionato eletrônico. Em seguida, aparecem os jogos eletrônicos, por meio do qual fraudes podem envolver roubo de itens virtuais ou contas; jogos *on-line* como apostas e pôquer, que atraem fraudadores devido ao alto valor das transações; e o varejo, frequentemente alvo de fraudes¹³⁰.

No Brasil, as comunidades também foram o segmento com a maior taxa de suspeita de fraude digital, no qual os fraudadores se aproveitam da confiança inerente às plataformas de interação social, como aplicativos de relacionamento, para enganar os usuários. Eles criam perfis falsos, muitas vezes utilizando imagens roubadas (*catfishing*), e constroem um relacionamento aparentemente genuíno, manipulando emocionalmente as vítimas em golpes como os *romance scams* ou *pig butchering scams* e, uma vez conquistada a confiança, os criminosos solicitam informações confidenciais ou dinheiro, alegando emergências, problemas de saúde ou oportunidades de investimento falsas. Esse método de exploração não apenas compromete dados privilegiados, mas também pode resultar em perdas financeiras significativas e traumas emocionais para aqueles que acreditam estar seguros nas comunidades online¹³¹.

4.1 O estelionato eletrônico e as fraudes digitais mais comuns utilizadas para a sua prática (golpes digitais)

A figura típica da fraude eletrônica, estabelecida pela Lei nº 14.155/2021 e que constitui uma forma qualificada de estelionato, prevista no artigo 171, § 2º-A, do Código Penal, surgiu em resposta ao crescente número de crimes cibernéticos, buscando adequar o Código Penal à realidade digital e às novas modalidades de

¹³⁰ TRANSUNION. **Relatório de Tendências de Fraude Omnichannel 2025**. Disponível em: <https://www.transunion.com.br/report/fraude-report-h1-2025>. Acesso em: 27 out. 2025.

¹³¹ TRANSUNION. **Relatório de Tendências de Fraude Omnichannel 2025**. Disponível em: <https://www.transunion.com.br/report/fraude-report-h1-2025>. Acesso em: 27 out. 2025.

golpes. Ela se verifica quando a fraude é perpetrada por meio do uso de informações cedidas pela própria vítima ou por um terceiro que foi induzido a erro.

As "informações cedidas" podem incluir dados pessoais (como nome completo, CPF), credenciais de acesso (usuário e senha de bancos ou serviços *online*), dados bancários (número da conta, agência), informações de cartão de crédito (número, validade, código de segurança - CVV/CVC) ou até mesmo senhas de uso único (OTPs - *One-Time Passwords*). Os meios pelos quais essa indução ocorre incluem redes sociais, contatos telefônicos, e-mails fraudulentos, ou qualquer outra prática enganosa similar, geralmente empregando técnicas de engenharia social.

É fundamental compreender, como já dissemos anteriormente, que a fraude é um elemento intrínseco e indispensável para a configuração do crime de estelionato; em outras palavras, a ausência de fraude inviabiliza a caracterização deste delito. A fraude deve ser o meio pelo qual o criminoso obtém a vantagem ilícita.

No contexto do estelionato eletrônico, a fraude se manifesta por meio do uso de dados fornecidos pela vítima ou por um indivíduo ludibriado, utilizando canais como redes sociais, chamadas telefônicas, mensagens eletrônicas enganosas, ou outros expedientes fraudulentos análogos. É justamente essa particularidade no modo de execução, que envolve a utilização de meios eletrônicos ou digitais para induzir a vítima ao erro e obter dela as informações, que distingue essa modalidade delitiva dos demais crimes praticados por meio eletrônico, como por exemplo, o furto¹³².

Nesse contexto, é relevante observar que o legislador empregou a interpretação analógica (ou *intra legem*), reconhecendo que as informações cruciais para a obtenção de vantagem ilícita e o prejuízo econômico à vítima podem ser obtidas por meio de: a) redes sociais; b) contatos telefônicos; c) correio eletrônico fraudulento; ou d) qualquer outro meio fraudulento. Essa fórmula genérica de "qualquer outro meio fraudulento" é primordial, pois confere à lei a flexibilidade necessária para abarcar novas modalidades de golpes que surgem constantemente¹³³.

¹³² CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital. Primeiras impressões e reflexos no CP e no CPP. **MSJ. Meu Site Jurídico**. Publicado em: 28 mai. 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/> Acesso em 01/11/2025.

¹³³ GRECO, Rogério. **Curso de Direito Penal**. Vol.2 - 22ª Edição 2025. 22. ed. Rio de Janeiro: Atlas, 2025. E-book, p. 656. ISBN 9786559776924. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786559776924/>. Acesso em: 01 nov. 2025.

É, de fato, inviável que a legislação preveja todas as possíveis formas de fraude que surgem na realidade, dada a inventividade e audácia dos criminosos, que utilizam desde *deep fakes* até inteligência artificial para criar golpes cada vez mais convincentes. Para assegurar que nenhuma modalidade de fraude eletrônica fique impune, o tipo penal inclui essa formulação abrangente, garantindo a adaptabilidade da norma penal.

Na fraude eletrônica, assim como em qualquer estelionato, o ponto central é a indução da vítima (ou de um terceiro) ao erro, o que leva à entrega voluntária das informações ou do patrimônio ao agente. A vítima, iludida pelo engodo, disponibiliza seus dados ou realiza a transação financeira por sua própria vontade, ainda que viciada pelo engano. Na prática, para identificar o estelionato eletrônico nas principais modalidades de ciberataque, é categórico diferenciar essa modalidade típica da subtração de dados sem consentimento, que caracterizaria o crime de furto (art. 155 do CP), especialmente o furto mediante fraude (art. 155, § 4º, II do CP), em que a fraude visa dificultar a vigilância da vítima para que o agente subtraia o bem, e não para que a vítima o entregue.

Outra distinção importante é com o crime de invasão de dispositivo informático (art. 154-A do CP), que se configura pelo acesso indevido a sistemas ou dados sem o consentimento do titular, sem necessariamente envolver a indução ao erro para a obtenção de vantagem ilícita. A correta tipificação penal é essencial para a aplicação da lei e a punição adequada do cibercriminoso.

Existe uma variedade imensurável de formas de fraudes que surgem a todo momento. As fraudes por meio da rede mundial de computadores podem acontecer por diversas formas de “armadilhas”, sendo as mais utilizadas pelos criminosos, o *malware*, o *ransomware* e o *phishing*.

O *malware* refere-se a qualquer tipo de *software* malicioso projetado para prejudicar um sistema de computador. O *ransomware*, por sua vez, é um tipo específico de *malware* que sequestra dados ou sistemas e, tornando-os reféns, exige um resgate para liberá-los. Na maioria das vezes, o cibercriminoso não necessita ludibriar a vítima para conseguir praticar o ataque criminoso, visto que a invasão ao sistema pode se dar por meio do uso de *softwares* contaminados, sem que a vítima sequer tenha permitido. Portanto, nem sempre o crime praticado com uso de *malware*

ou *ransomware* poderá caracterizar a conduta típica do estelionato eletrônico, mas sim outra conduta criminosa.

Por isso, nos concentramos em abordar o *phishing*, a modalidade mais comum de ataque cibernético para a prática de estelionato eletrônico e as principais medidas de prevenção.

4.1.1 *Phishing*

O *phishing* constitui uma modalidade de ciberataque na qual agentes mal-intencionados empregam táticas de personificação (*impersonation*), simulando ser entidades legítimas e confiáveis, com o objetivo precípuo de subtrair indevidamente informações sensíveis e credenciais de acesso. Este vetor de ataque opera mediante a indução ao erro de indivíduos, que são levados a divulgar dados confidenciais por meio de comunicações fraudulentas, meticulosamente elaboradas para emular a autenticidade de fontes fidedignas. A eficácia do *phishing* reside na exploração de vulnerabilidades humanas, nomeadamente a confiança e a falta de escrutínio, estratégia conhecida como engenharia social, utilizada para manipular o comportamento do alvo¹³⁴.

O objetivo final transcende a mera obtenção de dados, visando frequentemente o ganho financeiro, a violação de dados corporativos, o comprometimento de sistemas ou a disseminação de *malware*. Trata-se de um dos ataques mais comuns no Brasil, segundo a FEBRABAN, mediante o qual o agente, usando *e-mails* com *links*, ligações e mensagens de texto falsas, que parecem ser de fontes confiáveis, como bancos ou empresas conhecidas, acessam dados pessoais e financeiros das vítimas¹³⁵.

A identificação de tentativas de *phishing* pode ser inferida por diversos indicadores contextuais e técnicos, exigindo uma análise crítica por parte do utilizador.

¹³⁴ BRASIL. Engenharia Social: como aspectos psicológicos podem se relacionar com golpes e fraudes. Gov.br Disponível em: <https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1>. Acesso em: 01 nov. 2025.

¹³⁵ FEBRABAN. **Saiba quais foram os 10 golpes mais aplicados contra clientes bancários em 2024**. Publicado em: 14 abr. 2025. Disponível em: <https://portal.febraban.org.br/noticia/4279/pt-br>. Acesso em: 27 out. 2025.

Estes incluem a presença de endereços de correio eletrônico suspeitos (e.g., `micros0ft.com` em vez de `microsoft.com` – um exemplo de *typosquatting*¹³⁶ ou *domain spoofing*¹³⁷), o uso de saudações genéricas ou impessoais ("Caro Cliente" em vez de um nome próprio), a formulação de mensagens com teor urgente ou ameaçador, e a solicitação para ativar ligações (*links*) ou descarregar anexos de proveniência desconhecida.

A inspeção de um *link* ao passar o cursor do *mouse* sobre ele pode revelar um URL de destino diferente do texto exibido, um claro sinal de fraude. Anexos inesperados, especialmente de tipos executáveis (.exe, .zip) ou documentos com macros (.docm, .xlsm), devem ser tratados com extrema cautela.

A prevenção eficaz de ataques de *phishing* requer a adoção de estratégias robustas de segurança a vários níveis. Entre elas, podemos destacar: I) a implementação de autenticação multifator resistente a *Phishing* (PR-MFA), que oferecem uma proteção superior, pois exigem a presença física do utilizador e validam o domínio legítimo; II) a diligência crítica na análise de ligações e anexos, em que o destinatário, antes de interagir com qualquer elemento de uma comunicação, verifica a sua legitimidade. Isto pode envolver a utilização de ambientes isolados (*sandboxing*¹³⁸ ou máquinas virtuais) para abrir anexos suspeitos ou a verificação de URLs por meio de serviços de reputação *online*; III) a atualização contínua sobre metodologias e vetores de ataque, sendo que nesse caso, a educação e o treino de sensibilização para a cibersegurança são cruciais. Os utilizadores devem ser informados sobre as táticas mais recentes empregadas por ciberagentes e as melhores práticas de segurança e por fim, os IV) controles técnicos de segurança, atuando a nível organizacional, com a implementação de *email gateways* avançados com capacidades de filtragem de *spam* e *phishing*, juntamente com a configuração de protocolos de autenticação de e-mail como SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication*,

¹³⁶ KASPERSKY. **O que é typosquatting? - Definição e Explicação.** Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-typosquatting>. Acesso em 01 nov. 2025.

¹³⁷ GLOBO.COM. **Spoofing:** o que é essa fraude digital que finge ser você para roubar seus dados. Publicado em: 02 jun. 2025. Disponível em: <https://g1.globo.com/pb/paraiba/especial-publicitario/hostdime/noticia/2025/06/02/spoofing-o-que-e-essa-fraude-digital-que-finge-ser-voce-para-roubar-seus-dados.ghtml>. Acesso em: 01 nov. 2025.

¹³⁸ FORTINET. **O que é sandboxing?** Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/what-is-sandboxing>. Acesso em: 01 nov. 2025.

Reporting, and Conformance). Prática essencial para mitigar a entrega de e-mails fraudulentos¹³⁹.

Os ataques de *phishing* são orquestrados por atores maliciosos que se apresentam como entidades fidedignas para obter acesso facilitado a um espectro diversificado de dados sensíveis. Embora a natureza e a sofisticação destes ciberataques evoluam em consonância com o avanço tecnológico, os princípios táticos subjacentes demonstram notável consistência, baseando-se fortemente na engenharia social, utilizada para convencer a vítima à prática de atos que permitem, ao agente criminoso, o acesso à sua privacidade, dados pessoais, bancários e etc.

As táticas mais comuns empregadas são: a) a comunicação enganosa: Os atacantes demonstram proficiência na manipulação de vítimas para a revelação de informações confidenciais, dissimulando mensagens e anexos maliciosos em contextos de baixa perspicácia, como caixas de entrada de correio eletrônico. A presunção de legitimidade de comunicações recebidas é frequentemente explorada; entretanto, é crucial reconhecer que e-mails de *phishing* são projetados para aparentar segurança e inofensividade. Atacantes utilizam técnicas como a manipulação do atributo href em HTML para exibir um texto de link aparentemente legítimo, enquanto o URL real aponta para um domínio malicioso, ou o uso de URL *shorteners* (ferramenta que permite transformar links longos em versões mais curtas)¹⁴⁰, para ocultar o destino final. Para mitigar a suscetibilidade a tais ataques, recomenda-se uma análise criteriosa de hiperligações (por meio de ação de posicionar o mouse sobre o link, sem clicar, para revelar o URL real) e endereços de remetentes antes de qualquer interação; b) a criação de urgência perceptual: A suscetibilidade ao *phishing* é frequentemente amplificada pela percepção de uma necessidade iminente de ação. Esta tática explora vieses cognitivos como a aversão à perda e o medo de ficar de fora (FOMO - *Fear Of Missing Out*), que faz as maiores vítimas entre a população de jovens adultos. Exemplos incluem a transferência de malware mascarado como documento de recrutamento em situações de contratação urgente, a inserção de credenciais bancárias em portais duvidosos sob o pretexto de reativar uma conta supostamente expirada, ou avisos falsos de contas comprometidas que

¹³⁹ MICROSOFT. **O que é o phishing?** Disponível em: <https://www.microsoft.com/pt-pt/security/business/security-101/what-is-phishing>. Acesso em: 27 nov. 2025.

¹⁴⁰ ITISE. **Os perigos dos links curtos.** Disponível em: <https://itise.com.br/blog/2023/10/09/os-perigos-dos-links-curtos/>. Acesso em: 01 nov. 2025.

exigem "verificação imediata". A indução de uma falsa sensação de urgência constitui uma tática comprovadamente eficaz para contornar o pensamento crítico. A salvaguarda de dados exige um escrutínio rigoroso ou a implementação de soluções tecnológicas de proteção de correio eletrônico que identifiquem tais padrões¹⁴¹; c) o estabelecimento de falsa confiança: Agentes maliciosos cultivam uma falsa sensação de confiança para ludibriar indivíduos, incluindo aqueles com maior discernimento. Ao personificar fontes amplamente reconhecidas e reputadas, como Google, Wells Fargo, UPS, ou mesmo colegas de trabalho e superiores hierárquicos (em cenários de *Business Email Compromise*), os perpetradores de *phishing* conseguem persuadir as vítimas a tomar ações comprometedoras antes que a fraude seja percebida. Esta tática pode envolver a replicação exata de logotipos, layouts de websites e linguagens de comunicação. Muitas tentativas de *phishing* escapam as defesas sem a presença de medidas avançadas de cibersegurança. A proteção de informações privadas é reforçada por tecnologias de segurança de correio eletrônico projetadas para identificar e neutralizar conteúdos suspeitos antes de chegarem ao usuário final, e pela verificação independente da legitimidade da comunicação; d) a manipulação psicológica e emocional: Os ciberatacantes empregam táticas de engenharia social para explorar vulnerabilidades psicológicas¹⁴², induzindo os alvos a agir impulsivamente. Após estabelecerem confiança por meio da personificação de uma fonte familiar e gerarem uma falsa sensação de urgência, os atacantes exploram emoções como medo, ansiedade, curiosidade ou até mesmo ganância. Indivíduos tendem a precipitar decisões quando confrontados com a perspectiva de perdas financeiras, implicações legais, a privação de recursos essenciais, ou a promessa de um ganho inesperado (e.g., loterias falsas). Nesse sentido, recomenda-se cautela extrema face a qualquer comunicação que exija "ação imediata" ou que evoque uma forte resposta emocional, pois pode indicar uma tentativa de fraude.

¹⁴¹ KLÜTSCH, Jennifer; SCHWAB, Jasmin; BÖFFEL, Christian; ZIMMERMANN, Verena; SCHLITTEMEIER, Sabine. Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media. **Humanities and Social Sciences Communications**. 11. 10.1057/s41599-024-03412-8. 2024. Tradução livre.

¹⁴² BRASIL. Engenharia Social: como aspectos psicológicos podem se relacionar com golpes e fraudes. **Gov.br** Disponível em: <https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1>. Acesso em: 01 nov. 2025.

4.1.2 Categorização dos ataques de *phishing*

A taxonomia dos ataques de *phishing* abrange diversas modalidades, sendo as mais prevalentes as seguintes¹⁴³:

a) *Phishing* por E-mail (*Email Phishing*): a manifestação mais difundida de *phishing*, caracterizada pelo uso de hiperligações fraudulentas ou anexos maliciosos para induzir os destinatários a revelar dados pessoais. Os atacantes frequentemente personificam grandes provedores de serviços (e.g., Microsoft, Google) ou entidades internas (e.g., colegas de trabalho). Estes ataques são muitas vezes de natureza massificada, enviados para um grande número de destinatários.

b) *Phishing* por *Malware* (*Malware Phishing*): Uma abordagem comum mediante o qual software malicioso (e.g., *ransomware*, *info-stealers*, *Remote Access Trojans* - RATs) é disfarçado como anexo legítimo (e.g., currículo, extrato bancário, fatura) em comunicações por e-mail. A abertura de tais anexos, que podem utilizar técnicas de ofuscação para fugir da detecção, pode, em casos severos, comprometer integralmente sistemas de tecnologia da informação.

c) *Spear Phishing*: Diferentemente dos ataques de *phishing* em massa, o *spear phishing* visa alvos específicos, explorando informações detalhadas obtidas sobre suas atividades profissionais e sociais (muitas vezes via OSINT - *Open Source Intelligence*). A alta personalização confere a estes ataques uma eficácia particular na evasão de medidas básicas de cibersegurança e uma taxa de sucesso significativamente maior.

d) *Whaling* (*Whaling Phishing*): Quando os ciberagentes direcionam seus esforços a indivíduos de alto perfil (e.g., executivos C-level, celebridades, gestores financeiros), a prática é denominada *whaling*. Estes impostores frequentemente conduzem investigações aprofundadas sobre seus alvos para identificar o momento mais oportuno para subtrair credenciais ou outras informações sensíveis, muitas vezes com o objetivo de orquestrar esquemas de *Business Email Compromise* (BEC) que podem resultar em perdas financeiras avultadas.

¹⁴³ CARPIO-TALLEUS, Alinhua. Decifrando o ataque de phishing, para que você não morda a isca! **APPVIZER**. Publicado em: 30 abr. 2025. Disponível em: <https://www.appvizer.com.br/revista/ti/seguranca-informatica/ataque-de-phishing>. Acesso em 01 nov. 2025.

e) *Smishing* (SMS *Phishing*): Termo derivado da fusão de "SMS" e "*phishing*", refere-se a ataques veiculados via mensagens de texto, que simulam comunicações autênticas de empresas (e.g., Amazon, FedEx, bancos, serviços governamentais) ou indivíduos. A natureza direta e percebida pessoalidade das mensagens de texto, juntamente com a utilização de *caller ID spoofing* e links encurtados, torna os utilizadores particularmente vulneráveis.

f) *Vishing* (Voice *Phishing*): Em campanhas de *vishing*, os atacantes operam a partir de centrais de atendimento fraudulentas ou por meio de chamadas diretas, empregando chamadas telefônicas para persuadir vítimas a divulgar informações confidenciais. Em muitos cenários, a engenharia social é utilizada para convencer as vítimas a instalar software malicioso, muitas vezes sob a forma de aplicações, nos seus dispositivos, ou a realizar transferências financeiras.

g) *Pharming*: Embora não seja estritamente uma tática de engenharia social direta, o *pharming* é uma forma de *phishing* técnico que redireciona o tráfego de um utilizador de um website legítimo para um website fraudulento sem o seu conhecimento. Isso pode ser alcançado por meio da manipulação de registos DNS (DNS *poisoning*) ou da alteração do ficheiro *hosts* local do utilizador.

h) *Clone Phishing*: Nesta técnica, os atacantes replicam um e-mail legítimo e previamente entregue (por exemplo, um aviso de segurança ou uma fatura), alteram os links ou anexos para versões maliciosas e reenviam-no. A semelhança com uma comunicação anterior legítima aumenta a probabilidade de a vítima confiar na mensagem.

Um ataque de *phishing* bem-sucedido pode acarretar consequências severas e complexas, tanto para o indivíduo quanto para as organizações. Para o indivíduo, pode resultar em perdas financeiras diretas (e.g., transferências fraudulentas, compras não autorizadas), débitos fraudulentos em cartões de crédito, perda de acesso a dados digitais (fotografias, vídeos, ficheiros), danos à pontuação de crédito, e, inclusive, a personificação da vítima por ciberagentes para fins ilícitos (roubo de identidade), o que pode levar a problemas legais e grande stress emocional. Por outro lado, para a pessoa jurídica, os riscos para uma entidade empregadora incluem a

subtração de fundos corporativos (especialmente em ataques BEC)¹⁴⁴, a exposição de dados pessoais de clientes e colaboradores, o roubo ou inacessibilidade de documentos confidenciais e propriedade intelectual, e a interrupção das operações de negócio. Uma violação de segurança de dados pode igualmente infligir um dano reputacional duradouro, em alguns casos, irreparável, resultando em perda de confiança dos clientes e vantagem competitiva, além dos custos significativos de resposta a incidentes, remediação e litígios¹⁴⁵.

Também como modo de prevenção às armadilhas digitais, é essencial a atenção aos sinais distintivos e a adoção de estratégias de mitigação pessoal. A capacidade de discernir ataques de *phishing* é fundamental para a diminuição de riscos. Ciberagentes podem visar um vasto leque de indivíduos, em particular aqueles com acesso a informações sensíveis, como profissionais de TI, finanças e posições executivas. Adicionalmente, agentes maliciosos podem personificar superiores hierárquicos para solicitar credenciais a colaboradores. Consequentemente, todos os membros de uma organização devem manter-se vigilantes face a comunicações suspeitas. A regra de ouro é "nunca clicar primeiro, sempre verificar".

O objetivo primordial de qualquer esquema de *phishing* é a subtração de informações confidenciais e credenciais. É imperativo exercer prudência face a qualquer comunicação (telefônica, eletrônica ou por mensagem de texto) que solicite dados sensíveis ou prova de identidade. Atacantes empenham-se em replicar entidades familiares, utilizando logotipos, designs e interfaces idênticos aos de marcas ou indivíduos conhecidos. A vigilância é crucial: evite clicar em ligações ou abrir anexos a menos que a legitimidade da comunicação seja inequivocamente confirmada por meio de um canal independente (e.g., ligar para o número oficial da empresa, verificar o website oficial).

Além disso, indicadores de um *e-mail* de *phishing* incluem: a) ameaças urgentes ou imperativos de ação imediata: tentações para criar pânico ou ansiedade que levem a decisões precipitadas; b) remetentes incomuns ou desconhecidos: deve ser verificado o endereço de e-mail completo, não apenas o nome de exibição. E-

¹⁴⁴ MICROSOFT. **O que é comprometimento de email comercial (BEC)?** Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-business-email-compromise-bec>. Acesso em: 01 nov. 2025.

¹⁴⁵ BRANQUINHO, Thiago Marcelo. **Segurança Cibernética Industrial**. Rio de Janeiro: Editora Alta Livros, 2021. *E-book*. p. 111. ISBN 9786555204117. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786555204117/>. Acesso em: 02 nov. 2025.

mails de domínios genéricos (e.g., @gmail.com) ou domínios com erros de digitação (*typosquatting*) são suspeitos; c) presença de erros ortográficos ou gramaticais: frequentemente resultantes de traduções deficientes ou de uma execução apressada por parte dos atacantes, por vezes são intencionais para contornar filtros de spam mais sofisticados; d) ligações (links) ou anexos suspeitos: o texto da hiperligação pode divergir do endereço IP ou domínio real (verificável por *hovering*). Anexos inesperados, especialmente ficheiros executáveis ou documentos com macros, são de alto risco; e) pequenos erros tipográficos em domínios ou nomes: como "microsoft.com" ou "microsoft.com", uma tática conhecida como URL *hijacking* ou *typosquatting*¹⁴⁶; f) solicitações de informações pessoais ou credenciais: organizações legítimas raramente solicitam informações sensíveis (senhas, números de cartão de crédito completos, números de segurança social) por e-mail ou SMS; g) comunicações inesperadas ou fora de contexto: e-mails ou mensagens sobre prémios que não se inscreveu, entregas de encomendas que não espera, ou problemas bancários que não reconhece e; h) discrepâncias na marca ou logotipos: imagens de baixa resolução ou logotipos desatualizados podem ser um sinal¹⁴⁷.

Para além da identificação, as estratégias de mitigação pessoal devem adotar as seguintes boas práticas: I) utilizar palavras-passe fortes e únicas para cada serviço, preferencialmente geridas por um *password manager*; II) manter o sistema operativo, navegadores e todas as aplicações atualizadas para beneficiar das últimas correções de segurança; III) instalar e manter atualizado um software antivírus/*anti-malware* robusto; IV) realizar cópias de segurança regulares de dados importantes; V) reportar e-mails ou mensagens suspeitas ao departamento de TI da sua organização ou às autoridades competentes; VI) ser cauteloso ao utilizar redes Wi-Fi públicas para transações sensíveis.

Muito embora o delito de estelionato eletrónico seja predominantemente cometido no ambiente digital, a menção aos "contatos telefónicos" pelo legislador deixa claro que a conduta também pode ocorrer fora da internet. A seguir trazemos as situações mais comuns.

¹⁴⁶ ETECHPT.COM. **Typosquatting**: Proteja-se de URLS Falsas e Seus Perigos! Disponível em: <https://etechpt.com/typosquatting-url-hijacking-explicado-como-se-proteger/>. Acesso em: 02 nov. 2025.

¹⁴⁷ KOSINSKI, Matthew. O que é phishing? **IBM**. Disponível em: <https://www.ibm.com/br-pt/think/topics/phishing>. Acesso em: 01 nov. 2025.

4.1.2.1 Golpe do Whatsapp

Esse golpe, que é um dos mais aplicados via contato telefônico, pode ocorrer majoritariamente de duas maneiras. A primeira delas é a utilização do código de segurança - criminosos, que obtêm o número de telefone do alvo por meio de diversas fontes, como sites de anúncios classificados, plataformas de compra e venda online, ou por meio de vazamentos de dados de serviços digitais, costumam iniciar o contato com as vítimas.

Essa comunicação inicial geralmente ocorre via *WhatsApp* ou por ligação telefônica, utilizando técnicas de engenharia social para ganhar a confiança ou criar um senso de urgência. O golpe se desenrola quando eles solicitam que a vítima confirme um "código de verificação" que, segundo eles, foi enviado por SMS. O ponto crítico é que muitos não percebem que este código não é uma simples confirmação, mas sim o OTP (*One-Time Password*) ou código de autenticação de dois fatores (2FA) que o próprio *WhatsApp* envia para registrar uma conta em um novo dispositivo.

Na realidade, o criminoso já iniciou o processo de registro do seu número de telefone no *WhatsApp* a partir de um aparelho sob seu controle, e o SMS que você recebe é a chave para concluir essa etapa. Ao fornecer esse código aos golpistas, a vítima inadvertidamente concede acesso total à sua conta. Com esse código de registro em mãos, os fraudadores conseguem vincular sua conta *WhatsApp* a um novo aparelho. Este processo, por segurança, desativa automaticamente o seu *WhatsApp* no seu próprio telefone, impedindo que você acesse o aplicativo.

A partir desse momento, os criminosos passam a operar sua conta, explorando a confiança de seus contatos. Eles geralmente utilizam a sua identidade para solicitar transferências de dinheiro (PIX, TED, DOC) a amigos e familiares, alegando emergências, problemas bancários ou outras desculpas convincentes, mas direcionando os pagamentos para contas bancárias sob seu controle, que frequentemente são contas de "laranjas" ou de difícil rastreamento.

A segunda maneira é a utilização da foto de uma pessoa conhecida. Trata-se de um golpe mais simples, porém cada vez mais difundido, que ocorre quando o criminoso se disfarça como um conhecido seu para solicitar dinheiro.

Ele utiliza o nome e uma foto de um amigo ou familiar, frequentemente copiados do WhatsApp original ou de perfis em redes sociais, em um aparelho diferente. A abordagem inicial é uma mensagem informando sobre uma suposta mudança de número de telefone, seguida de um pedido de ajuda financeira. A partir desse ponto, a sequência da fraude é bastante similar a outros esquemas¹⁴⁸.

4.1.2.2 Golpe do Pix

Com a crescente popularidade do Pix como meio de pagamento e transferência, que o consolidou como um dos sistemas de pagamento instantâneo mais bem-sucedidos globalmente, tem havido um aumento significativo nos relatos de fraudes que visam lesar os usuários.

A agilidade e a irrevogabilidade das transações, embora sejam grandes as vantagens, também são exploradas por criminosos. Por isso, um golpe específico, conhecido como "golpe do Pix errado", ganhou notoriedade nas redes sociais. Dados do Banco Central, informam que o Pix registrou em 2024, 224 milhões de transações interbancárias.

Dada a magnitude desse volume, é compreensível que, de fato, algumas transferências ocorram por engano. No entanto, é nesse cenário de volume massivo e potencial para erros genuínos que os golpistas se inserem com a fraude do Pix errado. O processo começa com os fraudadores realizando uma transferência de um valor relativamente baixo para a conta da vítima em potencial.

Como muitas chaves Pix são vinculadas a números de celular, e dados pessoais podem ser obtidos por meio de vazamentos, engenharia social ou até mesmo tentativas aleatórias, torna-se relativamente fácil para o criminoso obter um número e efetuar a transação. Imediatamente após a transferência, o golpista estabelece contato com a pessoa, seja por ligação ou mensagem de *WhatsApp*, utilizando o número para o qual o Pix foi feito.

¹⁴⁸ IDEC. INSTITUTO DE DEFESA DE CONSUMIDORES. Disponível em: <https://idec.org.br/>. Acesso em: 02 nov. 2025.

Essa abordagem direta visa criar um senso de urgência e legitimidade. Uma vez em contato, o criminoso emprega diversas técnicas de persuasão, alegando ter realizado a transferência por engano. As histórias variam: pode ser um pagamento de aluguel, uma conta de emergência, um valor destinado a um familiar, ou até mesmo um erro de digitação.

O objetivo é convencer a vítima a devolver o valor. Um detalhe crucial para o sucesso do golpe reside na solicitação de devolução: o criminoso pede que o dinheiro seja enviado para uma conta diferente daquela que originou a transferência inicial. Este é o ponto de virada da fraude, pois rompe a rastreabilidade direta e prepara o terreno para o duplo prejuízo. Instintivamente, a primeira reação para verificar a veracidade do contato suspeito é checar o extrato bancário.

O que confunde e convence a vítima é que o dinheiro de fato aparece em sua conta, validando a alegação do golpista. A vítima, agindo de boa-fé e com a intenção de corrigir um "erro", sente-se compelida a ajudar. A partir do momento em que a vítima se convence e realiza um novo Pix para a conta indicada pelo golpista, sob a crença de estar devolvendo um valor, ela cai na armadilha. Ela está, na verdade, fazendo uma nova transação que será difícil de reverter.

O prejuízo da vítima se concretiza porque, enquanto tenta convencer o usuário a devolver o dinheiro, o golpista também aciona o Mecanismo Especial de Devolução (MED), uma ferramenta do próprio Pix, criada para combater fraudes. O MED permite que um usuário que foi vítima de um golpe ou fraude solicite ao seu banco o bloqueio e a devolução de valores transferidos. O MED foi desenvolvido para simplificar o processo de estorno em casos de golpe, aumentando as chances de recuperação dos valores.

No entanto, os criminosos o utilizam indevidamente, alegando terem sido as vítimas da fraude e solicitando a devolução do Pix original que eles mesmos enviaram para a vítima. A transação contestada é então analisada pelas instituições financeiras envolvidas. Quando os bancos notam que a verdadeira vítima recebeu um valor (do golpista), e em seguida, o transferiu para uma terceira conta (também do golpista, mas diferente da original), eles identificam essa "triangulação" como um padrão de golpe. Nesse ponto, ocorre a retirada forçada do dinheiro do saldo da pessoa que foi enganada. O banco do golpista, ao processar a solicitação de MED, consegue reaver

o valor da conta da vítima, pois a transação original (do golpista para a vítima) é considerada fraudulenta *pelo golpista*.

Dessa forma, o golpista, que já havia recebido o dinheiro de volta voluntariamente da vítima para sua segunda conta, consegue uma *segunda* devolução do valor original por meio do MED, causando um duplo prejuízo à vítima. A vítima perde o dinheiro que enviou "de volta" e também o dinheiro que foi estornado pelo MED. Após constatar que foi vítima do golpe, a pessoa também pode acionar o mecanismo de devolução.

Contudo, a conta do golpista para a qual o dinheiro foi transferido de "boa-fé" pode já estar zerada, impedindo a recuperação do valor. Além disso, a vítima pode enfrentar um saldo negativo em sua conta, além de possíveis taxas bancárias, caso o valor estornado pelo MED exceda seu saldo disponível¹⁴⁹.

Recentemente o Banco Central publicou a Resolução BCB nº 493/25, que aprimorou o MED, para permitir o rastreio do percurso realizado pelo recurso transferido por fraude. Com essa nova possibilidade, a devolução que antes somente podia ser feita a partir da conta originalmente utilizada na fraude, da qual os fraudadores conseguiam retirar rapidamente os recursos e transferir para uma outra conta, agora vai poder contar com a identificação dos possíveis caminhos dos recursos. Essa identificação será compartilhada com os correntistas das contas envolvidas e permitirá a devolução dos recursos em até 11 dias. Essa nova regra será implementada facultativamente a partir de 23 de novembro de 2025 e, obrigatoriamente, a partir de 02 de fevereiro de 2026¹⁵⁰.

¹⁴⁹ MOURA, Bruno de Freitas. Entenda o golpe do Pix errado e saiba como não ser enganado. **Agência Brasil**. Publicado em: 11 jul. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2024-07/entenda-o-golpe-do-pix-errado-e-saiba-como-nao-ser-enganado>. Acesso em: 02 nov. 2025

¹⁵⁰ BANCO CENTRAL DO BRASIL. **BC aprimora o Mecanismo Especial de Devolução do Pix**. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20817/nota>. Acesso em: 02 nov. 2025.

4.1.2.3 Golpe da Falsa central telefônica/Falso funcionário

O golpe da central falsa de atendimento é uma fraude sofisticada e comum em que criminosos se passam por instituições financeiras legítimas, utilizando-se de diversas táticas de engenharia social por telefone, SMS, e-mail ou *WhatsApp*, com o objetivo primordial de roubar dados sensíveis, acessar contas bancárias e causar prejuízos financeiros significativos às vítimas.

Existem várias modalidades e abordagens que os golpistas empregam. A primeira a ser citada é “problemas em transações”. Os golpistas entram em contato alegando falhas ou inconsistências em operações financeiras recentes, como transferências Pix, TED, DOC ou pagamentos de boletos. Eles criam um senso de urgência e pânico, instruindo a vítima a “corrigir” o problema refazendo a transação manualmente para uma conta bancária controlada por eles, que na verdade são contas de “laranjas” ou mulas financeiras. A narrativa é sempre a de que a ação é necessária para “estornar” ou “validar” a transação original.

Outro exemplo clássico é do engodo da “atualização cadastral”. Sob o pretexto de ser uma medida de segurança ou uma exigência regulatória, os fraudadores solicitam dados pessoais e financeiros altamente sensíveis. Isso inclui CPF, data de nascimento, nome completo da mãe, número de cartão de crédito, código de segurança (CVV), data de validade e, em alguns casos, até senhas de acesso ou respostas a perguntas de segurança. O objetivo é coletar informações suficientes para realizar roubo de identidade, transações não autorizadas ou assumir o controle da conta da vítima.

Seguindo com os exemplos, há ainda, o pretexto da “movimentação atípica”. Os criminosos afirmam ter detectado atividades incomuns, suspeitas ou fraudulentas na conta da vítima, como compras de alto valor ou transferências desconhecidas. Eles utilizam essa tática para gerar medo e levar a vítima a “confirmar” informações. Durante a ligação ou troca de mensagens, podem solicitar a digitação de senhas, códigos de segurança, tokens ou OTPs (senha de uso único) enviados por SMS, sob o pretexto de bloquear a transação fraudulenta ou “proteger” a conta. Na realidade, esses dados são usados para autorizar as próprias transações dos golpistas.

O “APK malicioso”, é uma modalidade frequentemente veiculada via WhatsApp ou SMS, por ela os golpistas simulam um problema crítico na atualização do aplicativo bancário ou na segurança do dispositivo, convencendo a vítima a baixar e instalar um arquivo APK (*Android Package Kit*) falso. Este APK não é um aplicativo legítimo, mas sim um malware (como um RAT - *Remote Access Trojan* ou *keylogger*) que, uma vez instalado, concede aos criminosos controle remoto sobre o celular da vítima. Isso permite que eles interceptem SMS (incluindo OTPs), visualizem a tela, registrem digitações (*keylogging*) e, o mais perigoso, acessem e operem os aplicativos bancários instalados no aparelho, realizando transferências e pagamentos sem o consentimento da vítima.

Os aplicativos falsos são desenvolvidos para serem visualmente idênticos aos originais, dificultando a identificação da fraude. As vítimas mais frequentes incluem pessoas da terceira idade, que podem ter menos familiaridade com as tecnologias digitais e com as táticas de segurança bancária mais recentes, tornando-as mais suscetíveis à manipulação. No entanto, a sofisticação dos golpes significa que qualquer pessoa pode ser alvo¹⁵¹.

4.1.2.4 Golpe do falso empréstimo ou da devolução de empréstimo

O golpe do falso empréstimo ou da devolução de empréstimo são esquemas fraudulentos elaborados por criminosos para enganar indivíduos, principalmente por meio de contatos telefônicos, por ligação, SMS ou *WhatsApp*, prometendo acesso a crédito sob condições excepcionalmente vantajosas e atrativas.

No entanto, o verdadeiro objetivo dessas táticas é extorquir dinheiro das vítimas ou coletar suas informações pessoais sensíveis, frequentemente sob o pretexto de exigências de pagamentos antecipados, como taxas de processamento, depósitos de garantia, seguros obrigatórios ou até mesmo impostos.

¹⁵¹ TECHTUDO. **Golpe da falsa central:** entenda como funciona e saiba se proteger. Disponível em: <https://www.techtudo.com.br/noticias/2023/03/golpe-da-falsa-central-entenda-como-funciona-e-saiba-se-proteger.ghtml>. Acesso em: 02 nov. 2025.

A motivação por trás desses golpes muitas vezes explora a vulnerabilidade financeira e a urgência das pessoas em busca de soluções rápidas. É fundamental manter um estado de alerta constante, especialmente diante de ofertas que parecem "boas demais para ser verdade", e sempre verificar a autenticidade e a legitimidade das propostas diretamente com as instituições financeiras por meio de seus canais oficiais.

Entre as principais modalidades desse golpe podemos destacar as seguintes.

Em primeiro lugar, os depósitos antecipados. Esta é a modalidade mais prevalente e insidiosa. Os golpistas, solicitam um pagamento adiantado, que pode ser mascarado como "taxa de liberação", "custo de avaliação de crédito", "IOF antecipado" ou "depósito de segurança", prometendo que o empréstimo será liberado após essa transação. No entanto, o serviço nunca é entregue, e o dinheiro é perdido. É importante entender que nenhuma instituição financeira legítima e regulamentada exige pagamentos prévios para a liberação de um empréstimo, pois seus custos e riscos são incorporados às taxas de juros e encargos que são pagos *após* a concessão do crédito.

Em segundo lugar, podemos citar as cobranças de comissão ou seguros Indevidas: embora comissões e seguros (como o seguro prestamista) possam ser componentes legítimos de um contrato de empréstimo, neste contexto, são usados como pretexto para solicitar pagamentos antecipados por oportunidades de empréstimo que são inexistentes.

A diferença fundamental é que, em operações legítimas, essas taxas são geralmente deduzidas do valor total do empréstimo no momento da liberação ou incorporadas às parcelas, e não exigidas como um pagamento separado e prévio à concessão do crédito.

Há também o empréstimo *online* fraudulento. Golpistas criam sites falsos, perfis em redes sociais ou aplicativos maliciosos que imitam ou clonam instituições financeiras legítimas ou se apresentam como intermediários de crédito. Eles prometem crédito rápido, sem consulta a órgãos de proteção ao crédito (como Serasa ou SPC) e com juros baixíssimos.

O objetivo é duplo: cobrar taxas adiantadas e, muitas vezes, coletar dados pessoais (como RG, CPF, comprovante de residência e dados bancários) para fins de

roubo de identidade ou outras fraudes. Eles podem até mesmo forjar contratos para pressionar as vítimas a pagar.

Mencione-se, ademais, o empréstimo por telefone (*vishing*): semelhante ao golpe *online*, mas o contato inicial é feito por telefone, geralmente por meio de chamadas não solicitadas. Os golpistas utilizam táticas de engenharia social para criar um senso de urgência e confiança, fazendo as mesmas promessas sedutoras de crédito fácil e rápido, com a subsequente solicitação de pagamentos antecipados.

A categoria do empréstimo falso genérico, por sua vez, abrange uma ampla gama de fraudes em que os criminosos simulam ser empresas legítimas, oferecendo empréstimos com termos atraentes e exigindo taxas antecipadas por diversos canais de comunicação, incluindo telefone, e-mail, SMS e aplicativos de mensagens como WhatsApp. A tática comum é a pressão para que a vítima tome uma decisão rápida, sob a alegação de "ofertas por tempo limitado" ou "condições exclusivas".

O golpe do empréstimo consignado foca principalmente em aposentados, pensionistas e servidores públicos, esta fraude pode ocorrer de duas formas principais: a) exigência de taxas antecipadas: os golpistas prometem um empréstimo consignado com condições irreais e solicitam pagamentos prévios para "liberação", "desbloqueio" ou "seguro"; b) uso indevido de dados: de forma mais grave, os criminosos obtêm os dados da vítima (muitas vezes por meio de vazamentos de dados ou engenharia social) e realizam um empréstimo consignado real em nome da vítima, em um banco legítimo, sem o seu consentimento.

A vítima só descobre a fraude quando as parcelas começam a ser descontadas de seu benefício ou salário. É vital monitorar regularmente extratos bancários e do INSS para identificar lançamentos desconhecidos.

4.2 Impactos econômicos e sociais do estelionato por fraude eletrônica e os desafios de enfrentamento

As repercussões sociais e econômicas do estelionato, particularmente em sua vertente eletrônica, são inegavelmente profundas, complexas e alarmantes. No plano

econômico, as fraudes não se limitam a meros incidentes isolados; elas corroem a solidez financeira tanto de indivíduos quanto de empresas, gerando prejuízos que podem ser estruturalmente desestabilizadores e sistêmicos.

No Brasil, o estelionato digital tem imposto uma carga financeira esmagadora, com perdas estimadas em milhões de reais nos últimos anos, impulsionadas principalmente por golpes envolvendo boletos fraudulentos (*malware* que altera dados bancários em boletos legítimos), transferências ilícitas via PIX (engenharia social para induzir transferências) e compras online não autorizadas (uso de dados de cartão de crédito roubados)¹⁵². A sofisticação desses ataques, que frequentemente empregam técnicas de *phishing*, *vishing* e *smishing* para obter credenciais, torna a detecção e prevenção ainda mais desafiadoras.

Além do impacto financeiro imediato, o estelionato digital mina a confiança fundamental nas transações online e nas plataformas digitais. Vítimas de golpes frequentemente desenvolvem uma aversão a novas compras ou serviços digitais, um comportamento que sufoca o crescimento e a inovação no comércio eletrônico, na adoção de *fintechs* e em outros setores da economia digital. Essa desconfiança se estende, lamentavelmente, à própria inovação tecnológica, pois o temor de ser fraudado estagna a adoção de novas plataformas e tecnologias financeiras, impactando diretamente a inclusão digital e a competitividade do mercado¹⁵³. A percepção de insegurança pode levar à retração do consumo e do investimento em infraestrutura digital.

Sob a ótica social, as fraudes digitais dilaceram a confiança entre os cidadãos e as instituições financeiras e governamentais. O impacto emocional nas vítimas é profundamente traumático, gerando sentimentos avassaladores de insegurança, impotência, vergonha e vulnerabilidade, que podem levar a problemas de saúde mental, como ansiedade e depressão. Em muitos casos, a recuperação dos valores perdidos é uma odisséia frustrante e burocrática, visto que a natureza transnacional

¹⁵² 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.

¹⁵³ LACERDA, Emanuel D. Nunes. A evolução dos crimes cibernéticos e a insuficiência das leis no Brasil. **Repositório Institucional do Unifip**, 2022.

desses crimes e a rápida pulverização dos fundos frequentemente paralisam a atuação das autoridades locais e dificultam o rastreamento dos ativos¹⁵⁴.

Essas consequências sociais tornam-se ainda mais perversas em países como o Brasil, em que vastas parcelas da população estão apenas agora acessando a internet e os serviços bancários digitais. A inclusão digital, que deveria ser um motor de progresso e democratização, transforma-se, ironicamente, em um terreno fértil para a exploração de novas vítimas, especialmente aquelas com conhecimento limitado em segurança digital, proteção de dados e alfabetização tecnológica. Idosos e pessoas com menor escolaridade são frequentemente alvos preferenciais devido à sua menor familiaridade com as nuances das ameaças online¹⁵⁵.

Assim, as fraudes digitais não apenas causam prejuízos financeiros, mas amplificam cruelmente as desigualdades sociais e tecnológicas no país, criando uma barreira adicional para o desenvolvimento equitativo.

A resposta a essa crise exige uma abordagem complexa, interconectada, intransigente e em constante evolução. A implementação de tecnologias de segurança avançadas – como criptografia robusta (AES - Algoritmo de Criptografia Avançada) para comunicações sensíveis¹⁵⁶, TLS/SSL (para conexões web)¹⁵⁷, monitoramento proativo de atividades suspeitas por meio de *Security Information and Event Management* (SIEM) e sistemas de inteligência artificial e *Machine Learning* (AI/ML) para detecção de anomalias comportamentais e padrões de fraude¹⁵⁸ – não é apenas uma opção, mas um imperativo estratégico para detectar e bloquear tentativas de estelionato antes que se concretizem.

¹⁵⁴ 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.

¹⁵⁵ 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.

¹⁵⁶ PRONNUS. **Criptografia AES-256**: O Padrão de Criptografia Inquebrável. Disponível em: <https://pronnus.com.br/blog/criptografia-aes-256-o-padrao-de-criptografia-inquebravel/>. Acesso em: 25 out. 2025

¹⁵⁷ SSL.COM. **O que é um SSL/TLS Certificado?** Disponível em: <https://www.ssl.com/pt/artigo/what-is-an-ssl-tls-certificado/>. Acesso em: 25 out. 2025.

¹⁵⁸ MICROSOFT. **O que é o SIEM?** Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-siem>. Acesso em: 25 out. 2025.

A autenticação multifator (MFA)¹⁵⁹, o uso de biometria e a tokenização de dados sensíveis¹⁶⁰, são exemplos de boas práticas que devem ser amplamente adotadas, face aos números alarmantes de ciberataques apresentados nos últimos tempos no Brasil. Para se ter uma ideia, segundo levantamento da *Check Point Research*, somente no segundo trimestre de 2024, o número de ataques cibernéticos aumentou em quase 70% em todo, sendo o Brasil um dos destaques negativos neste sentido¹⁶¹.

Paralelamente, as empresas carregam a responsabilidade inalienável de investir continuamente na capacitação de seus colaboradores, sobretudo em áreas sensíveis como atendimento ao cliente, suporte técnico e segurança da informação, para que possam identificar e combater eficazmente as táticas de engenharia social.

Do ponto de vista jurídico, embora o Brasil, além da tipificação penal do estelionato eletrônico, também possua legislações pertinentes para enfrentamento das demais fraudes eletrônicas de um modo geral, como o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Carolina Dieckmann (Lei nº 12.737/2012) e a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), que protege dados pessoais frequentemente visados por fraudadores, a eficácia dessas normas é comprometida pela sua aplicação deficiente e pela complexidade da jurisdição em crimes cibernéticos transnacionais. É urgente e inadiável fortalecer a execução dessas leis, garantindo que as violações digitais sejam investigadas com rigor, utilizando técnicas modernas de perícia digital (DFIR - *Digital Forensics & Incident Response*)¹⁶², e que os culpados sejam exemplarmente punidos.

A cooperação internacional também emerge como uma peça-chave e frequentemente subdimensionada, pois a capacidade dos criminosos de operar para além das fronteiras nacionais, explorando as discrepâncias entre as jurisdições e a lentidão dos Tratados de Assistência Jurídica Mútua (MLATs - *Mutual Legal*

¹⁵⁹ MICROSOFT. **O que é:** Autenticação Multifator. Disponível em <https://support.microsoft.com/pt-br/topic/o-que-%C3%A9-autentica%C3%A7%C3%A3o-multifator-e5e39437-121c-be60-d123-eda06bddf661>. Acesso em: 25 out. 2025.

¹⁶⁰ TECH NEWS. **Tokenização de Dados Sensíveis:** Estratégias e Melhores Práticas. Disponível em: <https://tech-news.neostream.com.br/2025-06-24-tokenizacao-de-dados-sensiveis-estrategias-e-melhores-praticas>. Acesso em: 25 out. 2025.

¹⁶¹ OLHAR DIGITAL. **Ataques Cibernéticos Crescem Quase 70% no Brasil em um Ano.** Disponível em: <https://olhardigital.com.br>. Acesso em: 25 out. 2025

¹⁶² IBM. **O que é Perícia Digital e Respostas a Incidentes (DFIR)?** Disponível em: <https://www.ibm.com/br-pt/think/topics/dfir>. Acesso em: 25 out. 2025

Assistance Treaties), é uma brecha crítica que exige atenção imediata¹⁶³. Adicionalmente, o desenvolvimento de políticas públicas assertivas, proativas e ágeis voltadas à proteção dos consumidores digitais e à regulação de serviços financeiros virtuais é absolutamente imprescindível.

O Estado deve superar a negligência histórica e investir substancialmente na capacitação de forças policiais especializadas em crimes cibernéticos, na criação de laboratórios forenses digitais e na formação de parcerias estratégicas com o setor privado, incluindo bancos, *fintechs* e empresas de cibersegurança. Tais medidas, quando articuladas com uma educação digital abrangente e contínua da população, são a espinha dorsal para reduzir a vulnerabilidade dos usuários às fraudes virtuais e conter o avanço implacável do estelionato digital¹⁶⁴.

A tecnologia, apesar de suas inegáveis vantagens no universo das transações digitais, é também uma espada de dois gumes, expondo seus usuários a vulnerabilidades que exigem um aprimoramento constante, ágil e adaptativo das medidas de segurança. O desenvolvimento de soluções tecnológicas robustas para a proteção de dados, como Sistemas de Prevenção Contra Perdas de Dados (DLP) e Gerenciamento de Identidade e Acesso (IAM)¹⁶⁵, não é apenas fundamental, é uma exigência incontornável no combate ao estelionato digital.

Os sistemas de monitoramento e prevenção de fraudes, impulsionados pela inteligência artificial e Aprendizado de Máquina¹⁶⁶, para detectar padrões suspeitos e comportamentos anômalos em tempo real, são instrumentos fundamentais. Eles permitem que empresas e bancos identifiquem e neutralizem tentativas de fraude, como apropriação de contas ou transações fraudulentas, antes que causem danos significativos, resguardando tanto os consumidores quanto as próprias instituições financeiras¹⁶⁷. A adoção de uma arquitetura de segurança *Zero Trust* e o foco na

¹⁶³ OLIVEIRA, Raphael Rodrigues Valença de; CLEMENTINO, Marco Bruno Miranda. Os Mlats Vigentes no Brasil e as Implicações na Soberania Contemporânea: Internacionalização, Territorialidade e Jurisdição. **Revista FIDES**. 23ª edição. Disponível em: <https://revistafides.ufrn.br/index.php/br/article/view/595>. Acesso em: 25 out. 2025.

¹⁶⁴ 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.

¹⁶⁵ IBM. **Tecnologia e emoção na palma da mão**. Disponível em: <https://www.ibm.com/br-pt>. Acesso em: 02 nov. 2025.

¹⁶⁶ IBM. **Tecnologia e emoção na palma da mão**. Disponível em: <https://www.ibm.com/br-pt>. Acesso em: 02 nov. 2025.

¹⁶⁷ CARVALHO, M. S. R. M. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. **Estudos de Ciência e Tecnologia no Brasil**, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

segurança da cadeia de suprimentos (*supply chain security*) são também elementos vitais¹⁶⁸.

Além das ferramentas tecnológicas, a cooperação internacional entre agências de segurança, órgãos reguladores e governos é mais do que essencial; é um imperativo geopolítico e estratégico contra uma ameaça sem fronteiras. Criminosos operam astutamente em diferentes jurisdições, tirando proveito das disparidades legais e da falta de coordenação para dificultar o rastreamento e a responsabilização de suas atividades ilícitas.

Nesse contexto, a criação de tratados e acordos internacionais que facilitem a troca de informações, o compartilhamento de Inteligência de Ameaças e a colaboração em investigações transnacionais é uma urgência diplomática que não pode ser ignorada. Embora organizações como a Interpol e a Europol desempenhem um papel relevante, o esforço global ainda se mostra fragmentado e reativo, clamando por uma estratégia mais coesa, proativa e unificada para enfrentar o problema em larga escala.

Neste particular, é importante ressaltar o papel do Comitê Nacional de Cibersegurança (CNCiber), que é um órgão colegiado presidido por um representante do Gabinete de Segurança Institucional da Presidência da República. Sua composição inclui quatorze representantes da administração pública federal, um do Comitê Gestor da Internet no Brasil e nove de entidades da sociedade civil (sendo três de segurança cibernética/direitos digitais, três de instituições científicas/tecnológicas/ inovação e três do setor empresarial de cibersegurança).

Estão entre seus objetivos principais a orientação da cibersegurança no País, bem como avaliação e propostas de medidas para seu aprimoramento. Entre suas competências podemos destacar, a apresentação de proposta de atualizações para a Política Nacional de Cibersegurança (PNCiber), a Estratégia e o Plano Nacional de Cibersegurança, a avaliação e proposta de medidas para o incremento da segurança cibernética, a formulação de propostas para o aperfeiçoamento da prevenção, detecção, análise e resposta a incidentes cibernéticos, a proposta de medidas para o

¹⁶⁸ CYBEROVERFLOW. **A Evolução da Segurança com a Implementação de Zero Trust**. Disponível em: <https://www.cyberoverflow.com.br/a-evolucao-da-seguranca-com-a-implementacao-de-zero-trust/>. Acesso em: 02 nov. 2025.

desenvolvimento da educação em cibersegurança, a promoção da interlocução com entes federativos e a sociedade em temas de cibersegurança, a apresentação de propostas de estratégias de colaboração para cooperação técnica internacional em cibersegurança e, apresentação de pareceres sobre assuntos de cibersegurança quando solicitado pelo Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo¹⁶⁹.

Outro aspecto crítico é a necessidade incessante de atualização legislativa e regulatória para acompanhar a vertiginosa evolução tecnológica e a criatividade dos fraudadores. O Marco Civil da Internet (Lei nº 12.965/2014) e a LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709/2018) representam avanços importantes, mas essas normas são insuficientes por si só e devem ser complementadas por regulamentações específicas que atendam à crescente sofisticação das fraudes digitais, como as que envolvem criptoativos ou o uso de *deepfakes*.

Além disso, o aprimoramento dos mecanismos de investigação digital é essencial para reverter a impunidade, garantindo que as violações sejam identificadas prontamente e os responsáveis, exemplarmente punidos. A criação de delegacias especializadas em crimes cibernéticos, a capacitação técnica de policiais, peritos e membros do Ministério Público em *cybercrime investigation* e *digital forensics* são investimentos irrecusáveis para fortalecer a resposta do Estado a essas novas e complexas ameaças¹⁷⁰.

Por fim, a conscientização e a educação digital da população emergem como a linha de frente indispensável na prevenção do estelionato digital. Programas educacionais que instruem sobre boas práticas de segurança digital – como o reconhecimento de e-mails fraudulentos (*phishing*), a importância de não compartilhar informações pessoais sensíveis em redes não seguras ou por canais não verificados, a adoção de senhas fortes e exclusivas, e a ativação da autenticação multifator (MFA) – são medidas preventivas urgentes e de alto impacto para mitigar a incidência de golpes.

¹⁶⁹ BRASIL. Comitê Nacional de Cibersegurança. O que é? **Gov.br**. Disponível em: <https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber>. Acesso em: 02 nov. 2025.

¹⁷⁰ MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova**: a investigação criminal em busca da verdade. 2ª Edição Revista e Atualizada. Ed. Juruá, Curitiba/PR. 2015, p. 75.

Campanhas de conscientização pública, promovidas por governos, empresas e organizações da sociedade civil, devem, ademais, reafirmar a responsabilidade compartilhada na proteção cibernética, cultivando uma genuína cultura de cibersegurança no Brasil.

Essa abordagem proativa, que empodera o usuário com conhecimento e ferramentas, é essencial para reduzir significativamente o número de vítimas e os devastadores impactos financeiros e emocionais desses crimes, transformando o cidadão em um agente ativo na sua própria proteção.

5 CONCLUSÃO

A fraude, particularmente em sua manifestação digital, permanece como um entrave significativo para o sistema de justiça criminal e para a salvaguarda cibernética na atualidade. Mesmo com os progressos legislativos e as estratégias de enfrentamento implementadas, a questão não foi erradicada.

Isso ocorre porque o avanço tecnológico, embora benéfico à sociedade, também abriu portas para um leque maior de condutas fraudulentas, com ataques cada vez mais sofisticados, como as práticas aqui citadas, em especial o *phishing*, ransomware e esquemas de engenharia social, demandando uma postura cada vez mais ágil e adaptável por parte dos órgãos governamentais, das entidades bancárias e financeiras, e da coletividade como um todo. A escala global da internet e a facilidade de anonimato exacerbam a complexidade do problema, tornando a detecção e a responsabilização ainda mais desafiadoras.

Este trabalho buscou revelar que o estelionato online transcende as dimensões legais e financeiras, abrangendo igualmente fatores sociais e psicológicos. Os fraudadores exploram vulnerabilidades humanas como a confiança, a urgência e o medo para manipular suas vítimas.

Para conter essa modalidade criminosa, impõe-se a adoção de soluções globalizantes, que incluam o reforço das leis vigentes e a contínua modernização dos marcos regulatórios cibernéticos, como a atualização de legislações de proteção de dados e a criação de mecanismos legais para a cooperação internacional na persecução de crimes cibernéticos.

A fim de reduzir a ocorrência de delitos no ambiente virtual, torna-se essencial fomentar a educação digital entre os cidadãos, por intermédio de ações informativas e iniciativas de conscientização. Isso inclui campanhas sobre a importância de senhas fortes e exclusivas, o uso de autenticação multifator (MFA), a identificação de e-mails e mensagens suspeitas (*phishing* e *smishing*) e a verificação da autenticidade de sites e aplicativos antes de fornecer informações pessoais ou financeiras.

É imprescindível a evolução das tecnologias de segurança, com aporte financeiro em sistemas de vigilância mais eficientes que empreguem inteligência artificial (AI) para identificar e evitar golpes em tempo real. Adicionalmente, a cooperação global deve ser intensificada, dada a importância da parceria entre nações para localizar e sancionar delinquentes que operam transfronteiriçamente, por meio de acordos de extradição, compartilhamento de inteligência e forças-tarefa conjuntas.

Desse modo, o robustecimento das estruturas institucionais e do arcabouço legal, englobando a capacitação de especialistas para investigar ilícitos digitais e a estrita observância das regulamentações em vigor, revela-se indispensável para frear a proliferação dessas atividades.

Isso envolve a formação, dentro dos Órgãos de Segurança Pública e Repressão ao crime, de peritos em Forense Digital na Resposta a Incidentes (DFIR)¹⁷¹, capazes de atuar rapidamente na contenção de ataques e na coleta de evidências digitais. A implementação, nas áreas de Segurança Pública a nível estadual e federal, de Centro de Operações de Segurança (SOCs)¹⁷² e a adoção de arquiteturas de segurança como Zero Trust são passos cruciais para monitorar, detectar e responder a ameaças de forma proativa¹⁷³.

Em suma, embora progressos tenham sido alcançados, o enfrentamento do estelionato eletrônico exige uma mobilização harmonizada entre o poder público, a iniciativa privada e a coletividade. Apenas com uma atuação conjunta e contínua adaptação às novas ameaças será viável edificar um ecossistema digital mais seguro e robusto, apto a salvaguardar eventuais vítimas e a minimizar a ocorrência de fraudes online.

Finalmente, considerando que as comunidades mais vulneráveis são, infelizmente, as que mais sofrem as consequências devastadoras pela carência de informação, baixa literacia digital e acesso limitado a recursos adequados. A promoção e disseminação de campanhas educativas robustas e acessíveis não é meramente uma medida preventiva; é um pilar fundamental da justiça social e um

¹⁷¹ RCZ. **Forense Digital na Resposta a Incidentes (DFIR)**. Disponível em: <https://rcz.com.br/blog/investigacao-forense-digital-dfir/>. Acesso em: 02 nov. 2025.

¹⁷² IBM. **O que é um Centro de Operações de Segurança (SOC)?** Disponível em: <https://www.ibm.com/br-pt/think/topics/security-operations-center>. Acesso em: 02 nov. 2025

¹⁷³ CYBEROVERFLOW. **Etiqueta: Zero Trust Arquitetura de Segurança da Informação e o papel essencial do Arquiteto de Segurança**. Disponível em: <https://www.cyberoverflow.com.br/tag/zero-trust/>. Acesso em: 06 nov. 2025.

imperativo para a inclusão digital plena, protegendo aqueles que são frequentemente alvos devido à sua menor familiaridade com os mecanismos de defesa online.

É absolutamente essencial empoderar essas comunidades com um conhecimento prático e contextualizado sobre os riscos. Isso inclui a compreensão aprofundada de *phishing* (e suas variantes como *smishing* via SMS e *vishing* via chamadas telefônicas, que utilizam engenharia social para manipular a vítima a revelar informações sensíveis ou realizar ações prejudiciais), *scams* online que prometem ganhos fáceis (como o "golpe do falso empréstimo", "golpe do PIX" ou "*romance scam*"), ou auxílios governamentais falsos.

Ao capacitar os cidadãos com as ferramentas cognitivas para reconhecer os sinais de alerta já citados neste trabalho, como a urgência incomum, erros gramaticais em comunicações, endereços de e-mail ou links suspeitos, promessas "boas demais para ser verdade" ou pedidos de dados sensíveis e transferências financeiras, e se protegerem proativamente de ataques, não apenas salvaguardamos suas finanças, que muitas vezes são limitadas, e suas informações pessoais, mas também fortalecemos a resiliência e a segurança digital de toda a sociedade, contribuindo para o combate ao crime.

Além da prevenção, é igualmente fundamental a conscientização sobre a importância de denunciar qualquer tentativa ou consumação de fraude. A denúncia não só ajuda a recuperar possíveis perdas e a proteger outras vítimas ao alertar as autoridades sobre novas táticas de golpe, como também fornece às autoridades dados cruciais para investigar e dismantelar redes criminosas, identificar padrões de ataque e até mesmo congelar ativos ilícitos.

As campanhas devem orientar claramente como e onde denunciar, enfatizando a necessidade de coletar e preservar evidências (capturas de tela, mensagens, comprovantes de transação). A educação é, sem dúvida, a nossa mais potente e abrangente defesa contra a exclusão digital e a exploração em um mundo cada vez mais conectado, transformando cada cidadão em um agente ativo na sua própria proteção e na segurança coletiva.

REFERÊNCIAS

AGRA, Andressa D.; BARBOZA, Fabrício F M. **Segurança de sistemas da informação**. Porto Alegre: SAGAH, 2019. *E-book*, p. 5. ISBN 9788595027084. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788595027084/>. Acesso em: 30 mai. 2025.

AMARAL, Cláudio do Prado. **Pacote Anticrime** – Comentários à Lei nº 13.964/2019. São Paulo: Almedina, 2020.

AMARAL, Rodrigo; LOBATO, José Rodrigo Tavares. Crime de Fraude com Utilização de Ativos Virtuais, Valores Mobiliários ou Ativos Financeiros. **Consultor Jurídico**. Publicado em: 6 out. 2024. Disponível em <https://www.conjur.com.br/2024-out-06/crime-de-fraude-com-utilizacao-de-ativos-virtuais-valores-mobiliarios-ou-ativos-financeiros/#:~:text=1%2D%20O%20artigo%20171%2DA,%2C%20ou%20seja%2C%20crime%20material>. Acesso em: 05 nov. 2025.

ANTOLISEI, Francesco. **Manuale di Diritto Penale**. Parte Speciale. v. 1. Milano, 1954.

BANCO CENTRAL DO BRASIL. **BC aprimora o Mecanismo Especial de Devolução do Pix**. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20817/nota>. Acesso em: 02 nov. 2025.

BATISTA, Weber Martins. **O furto e o roubo no direito e no processo penal**. 3ª ed. São Paulo: Lumen Juris, 2014

BITENCOURT, Cezar R. **Código penal comentado**. 10. ed. Rio de Janeiro: Saraiva Jur, 2019. *E-book*, p. 855. ISBN 9788553615704. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553615704/>. Acesso em: 12 de maio. 2025.

BITENCOURT, Cezar R. **Tratado de Direito Penal - Parte Especial - Vol.3 - 21ª Edição 2025**. 21. ed. Rio de Janeiro: SRV, 2024. *E-book*, p. 311. ISBN 9788553627561. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553627561/>. Acesso em: 28 abr. 2025.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**. Parte especial. v. 34. ed. São Paulo: Saraiva, 2008.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte especial**. Vol. 3. 16ª ed. São Paulo: Saraiva, 2020.

BOE. BOLETIM OFICIAL DEL ESTADO. **Ley Orgánica 10/1995, de 23 de noviembre**, del Código Penal. Espanha. Disponível em: <https://www.boe.es/eli/es/lo/1995/11/23/10>. Acesso em: 19 out. 2025.

BRANQUINHO, Thiago Marcelo. **Segurança Cibernética Industrial**. Rio de Janeiro: Editora Alta Livros, 2021. *E-book*. p. 111. ISBN 9786555204117. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786555204117/>. Acesso em: 02 nov. 2025.

BRASIL. Comitê Nacional de Cibersegurança. O que é? **Gov.br**. Disponível em: <https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber>. Acesso em: 02 nov. 2025.

BRASIL. Engenharia Social: como aspectos psicológicos podem se relacionar com golpes e fraudes. **Gov.br** Disponível em: <https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1>. Acesso em: 01 nov. 2025.

BRUNO, Aníbal. **Direito Penal: Parte Geral**. 3ª ed. Tomo II. Rio de Janeiro: Forense, 1967, p. 247-250.

CÂMARA DOS DEPUTADOS. **Projeto Lei nº 5485/2013**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=575520> Acesso em: 19 out. 2025.

CAMPOS, Francisco. **Exposição de Motivos do Código Penal**, § 61, *in verbis*: "Com a fórmula do projeto, já não haverá dúvida que o próprio silêncio, quando malicioso ou intencional, acerca do preexistente erro da vítima, constitui meio fraudulento característico do estelionato". E.M. Código Penal - DL nº 2.848/40. p. XXXVI. Imprensa Nacional. Rio de Janeiro, 1941. Disponível em <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-exposicaodemotivos-pe.pdf>. Acesso em: 08 jun. 2025.

CARPIO-TALLEUS, Alinhua. Decifrando o ataque de phishing, para que você não morda a isca! **APPVIZER**. Publicado em: 30 abr. 2025. Disponível em: <https://www.appvizer.com.br/revista/ti/seguranca-informatica/ataque-de-phishing>. Acesso em 01 nov. 2025.

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

CAVALI, Marcelo Costenaro. Concurso material de confusões: primeiras impressões sobre os novos tipos penais relativos a fraudes financeiras eletrônicas. In: TOLDO, Nino Oliveira; LACERDA, Fernando Hideo Iochida (orgs.). **Crimes Federais**. São Paulo: Editora Contracorrente, 2023.

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.

CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital. Primeiras impressões e reflexos no CP e no CPP. **MSJ. Meu Site Jurídico**. Publicado em: 28 mai. 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/> Acesso em 01/11/2025.

CYBEROVERFLOW. **A Evolução da Segurança com a Implementação de Zero Trust**. Disponível em: <https://www.cyberoverflow.com.br/a-evolucao-da-seguranca-com-a-implementacao-de-zero-trust/>. Acesso em: 02 nov. 2025.

CYBEROVERFLOW. **Etiqueta:** Zero Trust Arquitetura de Segurança da Informação e o papel essencial do Arquiteto de Segurança. Disponível em: <https://www.cyberoverflow.com.br/tag/zero-trust/> Acesso em: 06 nov. 2025.

DE GRANDIS, Rodrigo. **O Delito de Infidelidade Patrimonial e o Direito Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo - SP. 2018.

DFNDR Blog. Inteligência artificial traz novas ameaças para celulares e computadores. **Cibersegurança**. Disponível em: <https://www.psaf.com/blog/inteligencia-artificial-traz-novas-ameacas-para-celulares-e-computadores/>. Acesso em: 30 mai. 2025.

DI LORENZO, Alessandro; Capozzi, BRUNO. Brasil é o segundo maior alvo de crimes cibernéticos na América Latina. **Olhar Digital**. Publicado em: 02 fev. 2024. Disponível em: <https://olhardigital.com.br/2024/02/02/seguranca/brasil-e-o-segundo-maior-alvo-de-crimes-ciberneticos-na-america-latina/> Acesso em: 22 abr. 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.

DINIZ, Maria H. **Curso de Direito Civil Brasileiro** - Vol.1 - 42ª Edição. 42. ed. São Paulo: SaraivaJur, 2025.

ESTEFAM, André. **Direito Penal** - Parte Especial - Arts.121 a 234-C - Vol. 2. 12. ed. Rio de Janeiro: SRV, 2025. *E-book*, p. 622. ISBN 9788553625741. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625741/>. Acesso em: 28 abr. 2025.

ETECHPT.COM. **Typosquatting:** Proteja-se de URLS Falsas e Seus Perigos! Disponível em: <https://etechpt.com/typosquatting-url-hijacking-explicado-como-se-proteger/>. Acesso em: 02 nov. 2025.

FEBRABAN TECH. **Congresso de Prevenção e Repressão a Fraudes, Segurança Cibernética e Bancária**. Disponível em: <https://febrabantech.febraban.org.br/evento/congresso-prevencao-fraudes/sobre> Acesso em: 23 abr. 2025.

FEBRABAN. **Saiba quais foram os 10 golpes mais aplicados contra clientes bancários em 2024**. Publicado em: 14 abr. 2025. Disponível em: <https://portal.febraban.org.br/noticia/4279/pt-br>. Acesso em: 27 out. 2025.

FIGUEIREDO, Patrícia V.; JUNQUEIRA, Gustavo OD.; FULLER, Paulo H A.; e outros. **Lei Anticrime Comentada** - 2ª Edição 2021. 2. ed. Rio de Janeiro: Saraiva Jur, 2021. *E-book*, p. 30. ISBN 9786555595512. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555595512/>. Acesso em: 21 mai. 2025.

FORTINET. **O que é sandboxing?** Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/what-is-sandboxing>. Acesso em: 01 nov. 2025.

FRAGOSO, Heleno Cláudio. **Lições de direito penal**, Parte especial, v. I, 3ª ed. Rio de Janeiro: Forense, 1981.

FRAGOSO, Heleno Cláudio. **Lições de Direito Penal**. Parte Especial, v. 1. 11. ed. Rio de Janeiro: Forense, 1995, v. 1.

GLOBO.COM. **Spoofing**: o que é essa fraude digital que finge ser você para roubar seus dados. Publicado em: 02 jun. 2025. Disponível em: <https://g1.globo.com/pb/paraiba/especial-publicitario/hostdime/noticia/2025/06/02/spoofing-o-que-e-essa-fraude-digital-que-finge-ser-voce-para-roubar-seus-dados.ghtml>. Acesso em: 01 nov. 2025.

GONÇALVES, Victor Eduardo R. **Curso de Direito Penal - Parte Especial Vol.2 - 8ª Edição** 2024. 8. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*, p. 337. ISBN 9788553620982. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553620982/>. Acesso em: 21 mai. 2025.

GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado Direito Penal - Parte Especial**. 12. ed. Rio de Janeiro: Saraiva Jur, 2022. *E-book*, p. 528. ISBN 9786555597738. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555597738/>. Acesso em: 20 de maio. 2025.

GRECO, Rogério. **Curso de Direito Penal**. Vol.2 - 22ª Edição 2025. 22. ed. Rio de Janeiro: Atlas, 2025. *E-book*, p. 661. ISBN 9786559776924. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559776924/>. Acesso em: 28 abr. 2025.

GRECO, Rogério. **Curso de direito penal: parte especial**. v. 3. 6. ed. Niterói: Impetus, 2009.

HUNGRIA, Nélson. **Comentários ao código penal**, v. VII, Rio de janeiro: GZ, 2018.

HUNGRIA, Nélson. **Comentários ao Código Penal**. v. 7, 2. ed. Rio de Janeiro: Forense, 1958.

IBM. **O que é automação inteligente?** Disponível em: <https://www.ibm.com/br-pt/topics/intelligent-automation>. Acesso em: 06 abr. 2025.

IBM. **O que é Perícia Digital e Respostas a Incidentes (DFIR)?** Disponível em: <https://www.ibm.com/br-pt/think/topics/dfir>. Acesso em: 25 out. 2025.

IBM. **O que é um Centro de Operações de Segurança (SOC)?** Disponível em: <https://www.ibm.com/br-pt/think/topics/security-operations-center>. Acesso em: 02 nov. 2025.

IBM. **Tecnologia e emoção na palma da mão**. Disponível em: <https://www.ibm.com/br-pt>. Acesso em: 02 nov. 2025.

IDEC. INSTITUTO DE DEFESA DE CONSUMIDORES. Disponível em: <https://idec.org.br/>. Acesso em: 02 nov. 2025.

ITFORUM. Disponível em: <https://itforum.com.br/noticias/gartner-9-tendencias-impactar-negocios-2025/> Acesso em: 30 mai. 2025.

ITISE. **Os perigos dos links curtos**. Disponível em: <https://itise.com.br/blog/2023/10/09/os-perigos-dos-links-curtos/>. Acesso em: 01 nov. 2025.

JESUS, Damásio de. **Código penal anotado**. 23. ed. Rio de Janeiro: Saraiva Jur, 2015. *E-book*, p. 353. ISBN 9788502634343. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788502634343/>. Acesso em: 18 mai. 2025.

JESUS, Damásio de. **Direito penal: parte especial** (arts. 121 a 183). v. 2. 35. ed. Rio de Janeiro: Saraiva Jur, 2015. *E-book*, p. 166. ISBN 9788502619302. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788502619302/>. Acesso em: 24 abr. 2025.

JESUS, Damásio E. de. **Direito penal**, v. 2, 35ª ed. São Paulo: Saraiva, 2014.

KASPERSKY. **O que é typosquatting? - Definição e Explicação**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-typosquatting>. Acesso em 01 nov. 2025.

KLÜTSCH, Jennifer; SCHWAB, Jasmin; BÖFFEL, Christian; ZIMMERMANN, Verena; SCHLITTMEIER, Sabine. Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media. **Humanities and Social Sciences Communications**. 11. 10.1057/s41599-024-03412-8. 2024.

KOSINSKI, Matthew. O que é phishing? **IBM**. Disponível em: <https://www.ibm.com/br-pt/think/topics/phishing>. Acesso em: 01 nov. 2025.

LACERDA, Emanuel D. Nunes. A evolução dos crimes cibernéticos e a insuficiência das leis no Brasil. **Repositório Institucional do Unifip**, 2022.

LAMEIRAS, André. Tor ou VPN: qual é a melhor opção? **Welivesecurity**. Publicado em: 20 mar. 2023. Disponível em: <https://www.welivesecurity.com/br/2023/03/20/tor-ou-vpn-qual-e-a-melhor-opcao>. Acesso em: 06 jun. 2025

LOUREIRO, Antonio Carlos Tovo. **Perfil do Estelionato Contratual no Ordenamento Jurídico-Penal Brasileiro**. Tese de Doutorado em Direito Penal, Medicina Forense e Criminologia - Faculdade de Direito da Universidade de São Paulo. São Paulo-SP. 2004, p. 50. Disponível em <https://teses.usp.br/teses/disponiveis/2/2136/tde-26082015-113642/publico/tovo.pdf>. Acesso em 18 mai. 2025.

MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova: a investigação criminal em busca da verdade**. 2ª Edição Revista e Atualizada. Ed. Juruá, Curitiba/PR. 2015, p. 75.

MARINHO, Wederson. O futuro da Cibersegurança e Inteligência Artificial: Uma nova era de riscos e oportunidades. **Medium**. Publicado em: 21 abr. 2025. Disponível em: <https://medium.com/@marinhobusiness/o-futuro-da-ciberseguran%C3%A7a-e-intelig%C3%Aancia-artificial-uma-nova-era-de-riscos-e-oportunidades-b9185130c5c2> Acesso em: 30 mai. 2025.

MICROSOFT. **O que é comprometimento de email comercial (BEC)?** Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-business-email-compromise-bec>. Acesso em: 01 nov. 2025.

MICROSOFT. **O que é o phishing?** Disponível em: <https://www.microsoft.com/pt-pt/security/business/security-101/what-is-phishing>. Acesso em: 27 nov. 2025.

MICROSOFT. **O que é o SIEM?** Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-siem>. Acesso em: 25 out. 2025.

MICROSOFT. **O que é:** Autenticação Multifator. Disponível em <https://support.microsoft.com/pt-br/topic/o-que-%C3%A9-autentica%C3%A7%C3%A3o-multifator-e5e39437-121c-be60-d123-eda06bddf661>. Acesso em: 25 out. 2025.

MIRABETE, Júlio Fabrini. **Código Penal Interpretado**. São Paulo. Ed. Atlas, 1999, p. 1094/1095.

MONTEIRO, Washington de Barros. **Curso de direito civil**. 26ª ed. São Paulo: SaraivaJur, 2025.

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.

MOURA, Bruno de Freitas. Entenda o golpe do Pix errado e saiba como não ser enganado. **Agência Brasil**. Publicado em: 11 jul. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2024-07/entenda-o-golpe-do-pix-errado-e-saiba-como-nao-ser-enganado>. Acesso em: 02 nov. 2025

NORONHA, Edgard Magalhães. **Direito penal**, v. 2, São Paulo: Saraiva, 2003.

NORONHA, Edgard Magalhães. **Direito Penal**. Vol. 2 - 13ª ed. São Paulo: Saraiva, 1977.

NUCCI, Guilherme de S. **Curso de Direito Penal - Vol.2 - 9ª Edição 2025**. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*, p. 401. ISBN 9788530996666. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 16 mai. 2025.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**, 2ª ed. revista, atualizada e ampliada: parte geral: parte especial. São Paulo. Ed. Revista dos Tribunais, 2006, p. 699/700.

OLHAR DIGITAL. **Ataques Cibernéticos Crescem Quase 70% no Brasil em um Ano**. Disponível em: <https://olhardigital.com.br>. Acesso em: 25 out. 2025

OLIVEIRA, Raphael Rodrigues Valença de; CLEMENTINO, Marco Bruno Miranda. Os Mlats Vigentes no Brasil e as Implicações na Soberania Contemporânea: Internacionalização, Territorialidade e Jurisdição. **Revista FIDES**. 23ª edição. Disponível em: <https://revistafides.ufrn.br/index.php/br/article/view/595>. Acesso em: 25 out. 2025.

PANCINI, Laura. Tecnologia. Inteligência Artificial. **EXAME**. Publicado em: 11 mar. 2022. Disponível em: <https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/> Acesso em: 22 abr. 2025.

PRESCOTT, Roberta. Blockchain, computação quântica, IoT e IA desafiam a proteção de dados. **Convergência Digital 20 anos**. Publicado em: 29 jan. 2025. Disponível em: <https://convergenciadigital.com.br/mercado/blockchain-computacao-quantica-iot-e-ia-desafiam-a-protecao-de-dados/>. Acesso em: 09 jun. 2025.

PRONNUS. **Criptografia AES-256**: O Padrão de Criptografia Inquebrável. Disponível em: <https://pronnus.com.br/blog/criptografia-aes-256-o-padrao-de-criptografia-inquebravel/>. Acesso em: 25 out. 2025

RCZ. **Forense Digital na Resposta a Incidentes (DFIR)**. Disponível em: <https://rcz.com.br/blog/investigacao-forense-digital-dfir/>. Acesso em: 02 nov. 2025.

REALE JÚNIOR, Miguel. **Código Penal Comentado** - 2ª Edição 2023. 2. ed. Rio de Janeiro: Saraiva Jur, 2023. *E-book*, p. 610. ISBN 9786555599510. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555599510/>. Acesso em: 25 abr. 2025.

SALVADOR NETTO, Alamiro Velludo; BRUNI, Aline T.; AMARAL, Cláudio do P.; SAAD-DINIZ, Eduardo; HERME. **Pacote Anticrime** - Comentários à Lei N. 13.964/2019. São Paulo: Almedina Brasil, 2020. *E-book*, p. 30. ISBN 9786556270579. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786556270579/>. Acesso em: 21 mai. 2025.

SARRUBBO, Mário L. **Direito Penal: Parte Especial**. Barueri: Manole, 2012. *E-book*, p. 87. ISBN 9788520444368. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788520444368/>. Acesso em: 18 mai. 2025.

SERASA EXPERIAN. Tentativas de fraudes bancárias cresceram 10,4% em 2024 e poderiam gerar prejuízo de até R\$ 51,6 bilhões, revela Serasa Experian. **Prevenção à Fraude**. Publicado em: 11 mar. 2025. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraudes-bancarias-cresceram-104-em-2024-e-poderiam-gerar-prejuizo-de-ate-r-516-bilhoes-revela-serasa-experian/> Acesso em: 21 abr. 2025.

SSL.COM. **O que é um SSL/TLS Certificado?** Disponível em: <https://www.ssl.com/pt/artigo/what-is-an-ssl-tls-certificado/>. Acesso em: 25 out. 2025.

STF. SUPREMO TRIBUNAL FEDERAL. **Ext 1029 / PT - PORTUGAL. EXTRADIÇÃO**, julgado em 13/09/2006, Relator Ministro Cezar Peluso. Fonte: Site do STF, visto em 06/05/2025.

STF. SUPREMO TRIBUNAL FEDERAL. **HC 116979 AgR**, rel. Min. ROSA WEBER, 1ª Turma, out./2013.

STF. SUPREMO TRIBUNAL FEDERAL. **HC 208.817**, rel. Min. Cármen Lúcia, j. 13-4-2023.

STF. SUPREMO TRIBUNAL FEDERAL. **HC 84735 / PR – Habeas Corpus nº 84735**, julgado em 17/05/2005, Relator: Ministro Eros Grau. Fonte: site do STF, visto em 06/05/2025.

STF. SUPREMO TRIBUNAL FEDERAL. **HC 95.379/RS**, rel. orig. Min. Ellen Gracie, red. p/ o acórdão Min. Cezar Peluso, 2.ª Turma, j. 25.08.2009, noticiado no Informativo 557. E ainda: HC 103.407/RJ, rel. Min. Joaquim Barbosa, 2.ª Turma, j. 10.08.2010, noticiado no Informativo 595; HC 91.716/PR, rel. Min. Joaquim Barbosa, 2.ª Turma, j. 31.08.2010, noticiado no Informativo 598; e HC 82.965/RN, rel. Min. Cezar Peluso, 2.ª Turma, j. 12.02.2008. É também o entendimento do Superior Tribunal de Justiça: HC 48.412/SP, rel. Min. Og Fernandes, 6.ª Turma, j. 23.02.2010, noticiado no Informativo

424; REsp 689.926/PE, rel. Min. Maria Thereza de Assis Moura, 6.^a Turma, j. 29.09.2009, noticiado no Informativo 409; e HC 121.336/SP, rel. Min. Celso Limongi (Desembargador convocado do TJ-SP), 6.^a Turma, j. 10.03.1009, noticiado no Informativo 386.

STF. SUPREMO TRIBUNAL FEDERAL. **HC 99.112**, rel. Min. MARCO AURÉLIO, 1.^a T., 2010.

STF. SUPREMO TRIBUNAL FEDERAL. **RHC 65.186/SP**, rel. Min. Carlos Madeira, 2.^a Turma, j. 19.06.1987.

STF. SUPREMO TRIBUNAL FEDERAL. **RHC: 62912 RS**, Relator.: Min. OCTAVIO GALLOTTI, Data de Julgamento: 12/04/1985, PRIMEIRA TURMA, Data de Publicação: DJ 17-05-1985 PP-07353 EMENT VOL-01378-02 PP-00262.

STF. SUPREMO TRIBUNAL FEDERAL. **Súmula 246**: "Comprovado não ter havido fraude, não se configura o crime de emissão de cheque sem fundos". Disponível em: <https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2123> Acesso em: 06 nov. 2025.

STF. SUPREMO TRIBUNAL FEDERAL. **Súmula 554**. "O pagamento de cheque emitido sem provisão de fundos, após o recebimento da denúncia, não obsta o prosseguimento da ação penal." Súmulas do STF. Aprovação: 15/12/1976. Disponível em: <https://portal.stf.jus.br/>. Acesso em: 18 mai. 2025.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **AgRg no AgRg no AREsp: 2026865 SP 2021/0383539-0**, Data de Julgamento: 09/08/2022, T5 - QUINTA TURMA, Data de Publicação: DJe 15/08/2022.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **AgRg no REsp 1112184/RS**, rel. Min. ROGERIO SCHIETTI CRUZ, 6.^a Turma, 2015.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **CC: 160053 SP 2018/0194677-4**, Relator.: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 22/08/2018, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 27/08/2018.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **CC: 169053 DF 2019/0317771-7**, Relator.: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 11/12/2019, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 19/12/2019.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **EDeclAgRgREsp 1651521**, rel. Min. JORGE MUSSI, 5.^a Turma, 2017

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 247.408/RJ**, rel. Min. GURGEL DE FARIA, 5.^a T., 2015.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 36.760/RJ**, rel. Min. Paulo Medina, 6.^a Turma, j. 1.^o.03.2005.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 573.093/SC**, rel. Min. Reynaldo Soares da Fonseca, 5.^a T., j. 9-6-2020, DJe 18-6-2020

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 583.837**, rel. Min. Sebastião Reis Júnior, j. 4-8-2020.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC 610.201/SP**, rel. Min. Ribeiro Dantas, j. 24-3-2021.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **HC: 121460 DF 2008/0258029-0**, Relator.: Ministro JORGE MUSSI, Data de Julgamento: 06/04/2010, T5 - QUINTA TURMA, Data de Publicação: DJe 03/05/2010.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp 1.055.960**, rel. Min. Laurita Vaz, j. 31.10.2008.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp 142.451/DF**, rel. Min. Gilson Dipp, 5.^a Turma, j. 13.02.2002.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **REsp 683.075/DF**, rel. Min. Arnaldo Esteves Lima, 5.^a Turma, j. 18.04.2006.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **RHC: 132655 RS 2020/0206191-0**, Relator.: Ministro ROGERIO SCHIETTI CRUZ, Data de Julgamento: 28/09/2021, T6 - SEXTA TURMA, Data de Publicação: DJe 30/09/2021.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **RHC: 161635 DF 2022/0065612-3**, Data de Julgamento: 23/08/2022, T5 - QUINTA TURMA, Data de Publicação: DJe 30/08/2022.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula 107**. Disponível em: https://www.stj.jus.br/docs_internet/revista/electronica/stj-revista-sumulas-2010_7_capSumula107.pdf Acesso em: 6 out. 2025.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **Sumula 73**. "A utilização de papel-moeda grosseiramente falsificado configura, em tese, o crime de estelionato, de competência da Justiça Estadual". Disponível em: <https://www.stj.jus.br/publicacaoainstitucional/index.php/sumstj/article/viewFile/5276/5401> Acesso em: 06 nov. 2025.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. **Súmula nº 24**. "Aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da previdência social, a qualificadora do § 3º, do art. 171 do Código Penal." Súmulas do STJ. Disponível em: www.stj.jus.br. Acesso em: 13 maio 2025.

TECH NEWS. **Tokenização de Dados Sensíveis: Estratégias e Melhores Práticas**. Disponível em: <https://tech-news.neostream.com.br/2025-06-24-tokenizacao-de-dados-sensiveis-estrategias-e-melhores-praticas>. Acesso em: 25 out. 2025.

TECHTUDO. **Golpe da falsa central: entenda como funciona e saiba se proteger**. Disponível em: <https://www.techtudo.com.br/noticias/2023/03/golpe-da-falsa-central-entenda-como-funciona-e-saiba-se-proteger.ghml>. Acesso em: 02 nov. 2025.

TISAFE. **Ciberataques em alta no Brasil: empresas registam mais de 350 bilhões de tentativas de invasão em 2024**. Publicado em: 28 mar. 2025. Disponível em: <https://tisafe.com/pt/ciberataques-em-alta-no-brasil-empresas-registam-mais-de-350-bilhoes-de-tentativas-de-invasao-em-2024/>. Acesso em: 30 mai. 2025.

TRANSUNION. **Relatório de Tendências de Fraude Omnichannel 2025**. Disponível em: <https://www.transunion.com.br/report/fraude-report-h1-2025>. Acesso em: 27 out. 2025.

TRANSUNION. **Relatório de Tendências de Fraude Omnichannel 2025**. Disponível em: <https://www.transunion.com.br/report/fraude-report-h1-2025>. Acesso em: 27 out. 2025.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 5000772-72.2010.404.7114**, Des. Federal LEANDRO PAULSEN, 8ª Turma, jun./2014.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 5011701-17.2012.404.7205**, Des. Federal LEANDRO PAULSEN, 8ª Turma, set/2015.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 005658-39.2004.404.7009**, 8ª Turma, Juíza Federal SIMONE BARBISAN FORTES, por unanimidade, fev./2015.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 012145-58.2009.404.7200**, 8ª Turma, Juíza Federal SIMONE BARBISAN FORTES, fev./2015.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 5000196-96.2012.404.7118**, Des. Federal LEANDRO PAULSEN, 8ª Turma, out./2015.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **ACR 5000839-31.2010.404.7213**, 8ª TURMA, Des. Federal LEANDRO PAULSEN, jun./2014.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **ACR 5056950-87.2013.4.04.7000/PR**, 8ª Turma, Des. Federal LEANDRO PAULSEN, jun./2016.

TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **ENUL 5000855-24.2010.4.04.7103**, 4ª Seção, rel. Des. Fed. JOÃO PEDRO GEBRAN NETO, dez./2015. 51 TRF4. TRIBUNAL REGIONAL FEDERAL DA QUARTA REGIÃO. **AC 012145-58.2009.404.7200**, 8ª T., Juíza Federal SIMONE BARBISAN FORTES, fev./2015.

WHATELY, Marussia. Acesso a água e saneamento reflete desigualdades do Brasil. **PODER 360**. Publicado em: 11 mar. 2024. Disponível em: <https://www.poder360.com.br/poder-economia/golpes-causaram-prejuizo-de-r-101-bi-em-2024-diz-febraban/> Acesso em: 22 abr. 2025.