www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 159, 2026 | DOI: 10.69849/c5gbtk04

Os impactos da lei nº 15.397/2026 no crime de estelionato: uma análise comparativa entre a legislação anterior e o novo regime jurídico.

The impacts of law nº 15,397/2026 on the crime of embezzlement: a comparative analysis between the previous legislation and the new legal regime.

Jessica Feitosa da Silva Souza[1]
Orientadora: Profa. Esp. Rosana Reis de Melo Silva[2]

RESUMO

O presente artigo analisa os impactos da Lei nº 15.397/2026 no crime de estelionato previsto no artigo 171 do Código Penal Brasileiro, realizando um paralelo comparativo entre a legislação anterior e o novo regime jurídico introduzido pela referida norma. A pesquisa possui como objetivo examinar as principais alterações legislativas relacionadas à persecução penal, às fraudes eletrônicas e à proteção das vítimas diante do crescimento da criminalidade digital no Brasil. A fundamentação teórica baseia-se em doutrinas penais, legislação vigente, artigos científicos e entendimentos jurisprudenciais relacionados ao crime de estelionato e aos crimes cibernéticos. A metodologia utilizada é de natureza qualitativa, mediante pesquisa bibliográfica e documental, utilizando o método dedutivo para análise das modificações legislativas e seus reflexos práticos no sistema penal brasileiro. O estudo demonstra que a Lei nº 15.397/2026 buscou fortalecer os mecanismos de combate às fraudes eletrônicas e ampliar a efetividade da investigação criminal, embora ainda existam desafios relacionados à aplicação prática da norma e à estrutura estatal de repressão aos crimes digitais. Conclui-se que a nova legislação representa importante avanço no enfrentamento do estelionato eletrônico, mas sua eficácia depende da integração entre tecnologia, investigação especializada e políticas públicas de segurança digital.

Palavras-chave: Estelionato. Fraudes eletrônicas. Lei nº 15.397/2026. Crime digital. Código Penal.

[1] Graduando(a) do curso de Bacharelado em Direito, no Centro Universitário FAMETRO, Manaus, Amazonas , Brasil. Orientador(a): Prof(a). Dr(a). Rosana Reis de Melo Silva E-mail: rosanareismello@gmail.com. Orcid nº: 0009-0009-4815-212X.

[2] Prof.ª Orientadora e Coordenadora do TCC II, no Centro Universitário FAMETRO: Prof.ª Esp. Rosana Reis de Melo Silva. Manaus, Amazonas, Brasil. E-mail: rosanareismello@gmail.com

ABSTRACT

This article analyzes the impacts of Law No. 15.397/2026 on the crime of fraud provided for in Article 171 of the Brazilian Penal Code, making a comparative analysis between the previous legislation and the new legal regime introduced by the aforementioned law. The research aims to examine the main legislative changes related to criminal prosecution, electronic fraud and victim protection in view of the growth of digital crime in Brazil. The theoretical foundation is based on criminal law doctrines, current legislation, scientific articles and jurisprudential understandings related to fraud crimes and cybercrime. The methodology used is qualitative in nature, through bibliographic and documentary research, using the deductive method to analyze legislative changes and their practical effects on the Brazilian criminal system. The study demonstrates that Law No. 15.397/2026 sought to strengthen mechanisms to combat electronic fraud and increase the effectiveness of criminal investigations, although challenges related to the practical application of the law and the state structure to combat digital crimes still remain. It is concluded that the new legislation represents an important advance in combating electronic fraud, but its effectiveness depends on the integration between technology, specialized investigation and public digital security policies.

Keywords: Fraud. Electronic fraud. Law No. 15.397/2026. Digital crime. Penal Code.

1 INTRODUÇÃO

O crime de estelionato, previsto no artigo 171 do Código Penal Brasileiro, constitui uma das infrações patrimoniais mais recorrentes no ordenamento jurídico nacional. Nos últimos anos, o avanço tecnológico e a ampliação do acesso aos meios digitais contribuíram significativamente para o crescimento das fraudes eletrônicas, especialmente aquelas praticadas por aplicativos de mensagens, redes sociais e plataformas bancárias virtuais. Segundo Nucci (2025), o estelionato acompanha as transformações sociais e tecnológicas, exigindo constante atualização legislativa para garantir efetividade na repressão penal.

Nesse contexto, a Lei nº 15.397/2026 surgiu como importante instrumento de modernização legislativa voltado ao enfrentamento da criminalidade digital. As alterações promovidas pela nova legislação impactaram diretamente aspectos materiais e processuais relacionados ao crime de estelionato, especialmente no que se refere à persecução penal, à investigação das fraudes eletrônicas e à proteção das vítimas. Para Greco (2024), “a criminalidade cibernética representa um dos maiores desafios contemporâneos do Direito Penal moderno” (GRECO, 2024, p. 112).

O crescimento das fraudes virtuais demonstra a necessidade de fortalecimento dos mecanismos estatais de combate aos crimes patrimoniais digitais. Conforme destaca Capez

(2024), o ambiente virtual ampliou significativamente as possibilidades de prática criminosa, dificultando a identificação dos autores e exigindo novas estratégias de investigação criminal.

A presente pesquisa possui como problemática analisar os impactos jurídicos e processuais decorrentes da Lei nº 15.397/2026 no crime de estelionato em comparação à legislação anterior. Parte-se da hipótese de que a nova legislação representa avanço relevante no enfrentamento das fraudes eletrônicas, embora ainda existam limitações relacionadas à aplicação prática da norma e à estrutura investigativa estatal.

O objetivo geral deste trabalho é analisar os impactos da Lei nº 15.397/2026 no crime de estelionato, realizando um paralelo comparativo entre os dispositivos legais anteriores e o novo regime jurídico introduzido pela legislação. Como objetivos específicos, busca-se demonstrar as principais alterações legislativas, verificar os reflexos processuais da nova norma e explicar os desafios enfrentados pelo sistema penal diante da criminalidade digital contemporânea.

A relevância social da pesquisa decorre do crescimento expressivo dos crimes eletrônicos no Brasil e dos prejuízos causados às vítimas de fraudes virtuais. Além disso, o estudo possui relevância acadêmica e jurídica ao contribuir para o aprofundamento das discussões doutrinárias acerca da evolução legislativa do Direito Penal frente às transformações tecnológicas da sociedade contemporânea.

Segundo Nucci (2025), o crescimento das fraudes eletrônicas exige constante atualização do sistema penal brasileiro:

> O estelionato eletrônico representa uma das modalidades criminosas que mais crescem no Brasil, principalmente em razão da facilidade proporcionada pelos meios digitais e pela dificuldade de identificação dos autores dos delitos. A constante evolução tecnológica exige do legislador permanente adaptação normativa para garantir maior efetividade na repressão penal e proteção adequada das vítimas das fraudes virtuais. (NUCCI, 2025, p. 417).

A presente pesquisa utilizará o método dedutivo, partindo da análise geral das alterações promovidas pela Lei nº 15.397/2026 para a compreensão de seus impactos específicos no crime de estelionato previsto no artigo 171 do Código Penal Brasileiro. Segundo Lakatos e Marconi (2014), o método dedutivo permite extrair conclusões particulares a partir de premissas gerais relacionadas ao objeto de estudo.

Quanto à abordagem, trata-se de pesquisa qualitativa, desenvolvida mediante análise interpretativa da legislação penal, doutrinas jurídicas, artigos científicos, jurisprudências e

documentos oficiais relacionados ao tema. A pesquisa qualitativa possibilita examinar criticamente os reflexos jurídicos e processuais decorrentes das alterações legislativas promovidas pela nova lei.

No que se refere aos procedimentos técnicos, será realizada pesquisa bibliográfica e documental, utilizando livros, revistas jurídicas, artigos científicos, legislação, projetos de lei, decisões judiciais e materiais acadêmicos relacionados ao crime de estelionato e às fraudes eletrônicas.

Além disso, será realizada análise comparativa entre os dispositivos legais vigentes antes da promulgação da Lei nº 15.397/2026 e as alterações introduzidas pela nova legislação, buscando identificar os principais avanços, limitações e impactos práticos relacionados à persecução penal do estelionato eletrônico no Brasil.

2. O CRIME DE ESTELIONATO NO ORDENAMENTO JURÍDICO BRASILEIRO

2.1 Conceito jurídico do estelionato

O crime de estelionato encontra-se tipificado no artigo 171 do Código Penal Brasileiro e consiste na obtenção de vantagem ilícita em prejuízo alheio, mediante artifício, ardil ou qualquer outro meio fraudulento. Trata-se de delito inserido no contexto dos crimes patrimoniais, cuja característica essencial reside na manipulação da vontade da vítima, que é induzida ou mantida em erro.

> O crime de estelionato caracteriza-se pela obtenção de vantagem ilícita mediante fraude capaz de induzir a vítima em erro (BITENCOURT, 2023).
> Segundo Nucci (2025), o estelionato acompanha as transformações sociais e tecnológicas, exigindo constante atualização legislativa diante das novas modalidades criminosas.
> “O estelionato é delito patrimonial cuja essência encontra-se na fraude utilizada pelo agente para obtenção de vantagem ilícita” (BITENCOURT, 2023, p. 417). Segundo Nucci (2025):

A doutrina majoritária reconhece que o estelionato se estrutura sobre quatro elementos fundamentais: a fraude, o erro da vítima, a vantagem ilícita e o prejuízo patrimonial. Sem a presença simultânea desses elementos, não há que se falar em configuração típica do delito.

Segundo Bitencourt (2023), o estelionato exige necessariamente a utilização de fraude apta a enganar a vítima, sendo este o núcleo diferenciador em relação a outros crimes contra o patrimônio, como o furto e o roubo, nos quais não há participação voluntária da vítima.

Nucci (2025) complementa ao afirmar que o estelionato é um crime de elevada complexidade prática, justamente por sua capacidade de adaptação às mudanças sociais e tecnológicas, o que amplia significativamente suas formas de execução. Essa flexibilidade do tipo penal faz com que o delito seja frequentemente praticado por meios sofisticados, especialmente no ambiente digital.

Ademais, trata-se de crime material, o que significa que sua consumação depende da efetiva ocorrência do resultado naturalístico, qual seja, o prejuízo patrimonial da vítima. Assim, a mera tentativa de enganar não é suficiente para a consumação do delito, sendo indispensável a efetiva obtenção da vantagem ilícita.

2.2 Evolução histórica do artigo 171 do Código Penal

O crime de estelionato possui origem histórica ligada às antigas práticas de fraude patrimonial, presentes desde os primeiros códigos penais brasileiros. O artigo 171 do Código Penal de 1940 foi concebido em um contexto social no qual as fraudes eram predominantemente presenciais e baseadas em documentos falsos, promessas enganosas ou simulações de negócios jurídicos.

> O artigo 171 do Código Penal passou por alterações legislativas voltadas à adaptação do sistema penal às novas formas de criminalidade patrimonial (CAPEZ, 2024).
> Segundo Greco (2024), o crescimento das fraudes eletrônicas demonstrou a necessidade de fortalecimento dos mecanismos de persecução penal.
> "A evolução tecnológica ampliou significativamente as modalidades de fraudes patrimoniais praticadas no ambiente virtual" (GRECO, 2024, p. 203).

Com o avanço das relações econômicas e sociais, o tipo penal passou a ser progressivamente interpretado de forma mais ampla, a fim de abranger novas modalidades de fraude. Entretanto, a estrutura original do dispositivo permaneceu relativamente estável por décadas.

A transformação mais significativa ocorreu com o avanço da era digital, especialmente a partir da popularização da internet e dos meios eletrônicos de pagamento. A criminalidade patrimonial passou a se deslocar do ambiente físico para o virtual, exigindo atualização legislativa e interpretativa.

Nesse contexto, a Lei nº 13.964/2019 (Pacote Anticrime) promoveu alteração relevante ao estabelecer, como regra geral, a necessidade de representação da vítima para a persecução penal do estelionato. Tal mudança teve como objetivo reduzir a sobrecarga do sistema penal, mas também gerou críticas quanto à eventual redução da efetividade da repressão penal.

Capez (2024) destaca que tal modificação trouxe intensos debates doutrinários, especialmente diante do aumento exponencial dos crimes patrimoniais eletrônicos, nos quais muitas vítimas sequer conseguem identificar imediatamente o autor do delito.

2.3 O crescimento das fraudes eletrônicas no Brasil

O avanço tecnológico e a digitalização das relações sociais impulsionaram significativamente o aumento das fraudes eletrônicas no Brasil, tornando esse fenômeno um dos maiores desafios da segurança pública contemporânea.

> As fraudes eletrônicas cresceram significativamente em razão da ampliação das relações virtuais e do uso de plataformas digitais (OLIVEIRA, 2025).
> Segundo Greco (2024), a criminalidade digital representa um dos maiores desafios contemporâneos enfrentados pelo Direito Penal.
> "A facilidade proporcionada pela internet ampliou significativamente as modalidades de estelionato eletrônico praticadas no Brasil" (OLIVEIRA, 2025, p. 118).

As modalidades de estelionato digital incluem phishing, clonagem de aplicativos de mensagens, falsas centrais de atendimento bancário, fraudes em compras online e esquemas de investimento fraudulentos, todos com elevado potencial lesivo.

De acordo com Greco (2024), a criminalidade digital possui como característica central a alta adaptabilidade, permitindo que os agentes criminosos alterem rapidamente seus métodos para evitar a atuação estatal. Além disso, a utilização de redes privadas, contas de terceiros e sistemas de anonimização dificulta a identificação dos responsáveis.

Outro fator relevante é a vulnerabilidade das vítimas, que muitas vezes são induzidas ao erro por meio de técnicas de engenharia social altamente sofisticadas, explorando aspectos emocionais, financeiros e psicológicos.

Diante desse cenário, torna-se evidente a necessidade de constante atualização legislativa e de políticas públicas voltadas à prevenção e repressão dessas condutas, culminando na criação da Lei nº 15.397/2026.

3 AS ALTERAÇÕES PROMOVIDAS PELA LEI Nº 15.397/2026

3.1 Modernização legislativa do combate ao estelionato

A Lei nº 15.397/2026 surge como resposta legislativa necessária ao expressivo aumento dos crimes de estelionato praticados, especialmente no ambiente digital, representando um importante marco de modernização do sistema penal brasileiro. A sua edição reflete a preocupação do legislador em adequar o ordenamento jurídico às novas formas de criminalidade patrimonial, cada vez mais sofisticadas, dinâmicas e transnacionais.

> A Lei nº 15.397/2026 buscou fortalecer os mecanismos de investigação e repressão das fraudes eletrônicas no Brasil (BRASIL, 2026).
> Segundo Nucci (2025), a atualização legislativa demonstra preocupação estatal em adaptar o Direito Penal às novas formas de criminalidade tecnológica.
> "A evolução tecnológica exige permanente modernização dos instrumentos jurídicos de combate à criminalidade digital" (GRECO, 2024, p. 215).

Nesse contexto, a norma promove uma reestruturação significativa no tratamento jurídico do estelionato eletrônico, ampliando o alcance das medidas investigativas e reforçando os mecanismos de repressão penal. A legislação passa a reconhecer, de forma mais clara, a complexidade das fraudes digitais, que envolvem múltiplos agentes, plataformas tecnológicas e fluxos financeiros fragmentados.

Entre os principais avanços, destaca-se o fortalecimento da cooperação interinstitucional, especialmente entre órgãos de persecução penal, instituições financeiras, empresas de tecnologia e provedores de serviços digitais. Essa integração permite maior agilidade na identificação de transações suspeitas, rastreamento de valores e bloqueio de ativos provenientes de ilícitos.

Segundo Nucci (2025), esse movimento legislativo representa uma tendência contemporânea do Direito Penal, que busca não apenas punir condutas já praticadas, mas também se adaptar preventivamente às novas modalidades de criminalidade econômica, sobretudo aquelas impulsionadas pelo avanço tecnológico.

Além disso, a legislação reforça a importância da prova digital como elemento central da investigação criminal moderna, reconhecendo sua relevância na reconstrução dos fatos e na identificação da autoria delitiva em crimes de natureza cibernética.

3.2 Comparação entre a legislação anterior e a nova lei

Antes da promulgação da Lei nº 15.397/2026, o ordenamento jurídico brasileiro enfrentava dificuldades relevantes no enfrentamento das fraudes eletrônicas, principalmente em razão da ausência de instrumentos normativos suficientemente eficazes para lidar com a complexidade da criminalidade digital.

A legislação anterior, embora já contemplasse o crime de estelionato no artigo 171 do Código Penal, não possuía mecanismos específicos voltados à realidade tecnológica contemporânea, o que gerava limitações significativas na investigação e responsabilização dos agentes.

> A legislação anterior apresentava limitações relacionadas à obtenção de provas digitais e à identificação dos autores dos crimes virtuais (CAPEZ, 2024).
> Segundo Mesquita, Ferreira e Reis (2025), a nova legislação ampliou os mecanismos de cooperação investigativa relacionados ao estelionato eletrônico.
> "A modernização legislativa representa importante instrumento de fortalecimento da persecução penal digital" (MESQUITA; FERREIRA; REIS, 2025, p. 193).

Entre os principais entraves do regime anterior, destacavam-se a dificuldade de identificação dos autores, a morosidade na obtenção de dados junto a provedores de serviços digitais e a insuficiência de instrumentos de rastreamento financeiro em tempo real. Esses fatores contribuíam para a baixa efetividade na recuperação de valores e para a sensação de impunidade em relação aos crimes virtuais.

Com a nova legislação, observa-se uma mudança de paradigma, com a ampliação dos mecanismos de investigação, fortalecimento da cooperação institucional e maior integração entre sistemas públicos e privados de informação. Essa evolução normativa permite uma atuação mais célere e eficiente do Estado na repressão às fraudes digitais.

Greco (2024) enfatiza que a efetividade da persecução penal nos crimes cibernéticos depende diretamente de três pilares fundamentais: atualização legislativa constante, capacitação técnica dos agentes públicos e integração tecnológica entre os órgãos de investigação. Tais elementos passam a ser reforçados com a nova legislação, que busca superar as deficiências do modelo anterior.

Dessa forma, a comparação entre os dois regimes evidencia uma transição do modelo tradicional de repressão penal para um modelo mais tecnológico, integrado e responsivo às dinâmicas da criminalidade contemporânea.

3.3 Impactos processuais da Lei nº 15.397/2026

A Lei nº 15.397/2026 produziu impactos relevantes não apenas no direito material, mas também no âmbito processual penal, especialmente no que se refere à investigação, instrução probatória e medidas cautelares aplicáveis aos crimes de estelionato eletrônico.

Um dos principais avanços consiste na ampliação dos mecanismos de bloqueio e indisponibilidade de valores obtidos por meio de fraudes digitais. Essa medida possui relevância prática significativa, uma vez que a dinâmica dos crimes cibernéticos envolve a rápida movimentação de ativos entre diversas contas bancárias e ocultação patrimonial.

> A nova legislação ampliou mecanismos voltados à coleta de provas digitais e ao bloqueio de ativos financeiros provenientes de fraudes eletrônicas (BRASIL, 2026).
> Segundo Greco (2024), a efetividade das investigações criminais depende da integração entre tecnologia, legislação e capacitação profissional.
> "O combate ao estelionato eletrônico exige rapidez investigativa e integração institucional" (NUCCI, 2025, p. 422).

Outro impacto importante refere-se ao fortalecimento da produção de prova digital, que passa a ocupar posição central na persecução penal desses delitos. Registros eletrônicos, logs de acesso, dados bancários e informações de plataformas digitais tornam-se elementos essenciais para a reconstrução da cadeia delitiva e identificação dos responsáveis.

A legislação também intensifica a cooperação entre órgãos públicos e entidades privadas, especialmente instituições financeiras, empresas de tecnologia e provedores de internet. Essa cooperação permite maior celeridade na obtenção de dados e contribui para a eficiência das investigações, reduzindo o tempo de resposta estatal diante das fraudes.

Entretanto, apesar dos avanços normativos, ainda persistem desafios relevantes relacionados à implementação prática dessas medidas. A insuficiência de estrutura tecnológica em alguns órgãos de investigação, a ausência de sistemas integrados e a necessidade de maior capacitação técnica dos agentes públicos continuam sendo obstáculos que limitam a plena efetividade da norma.

Nesse sentido, a aplicação da Lei nº 15.397/2026 exige não apenas adequação normativa, mas também investimento contínuo em tecnologia, inteligência investigativa e qualificação profissional, sob pena de a legislação não atingir plenamente seus objetivos de combate ao estelionato eletrônico.

4 OS DESAFIOS DO COMBATE AO ESTELIONATO ELETRÔNICO

4.1 Dificuldades investigativas nos crimes virtuais

O combate ao estelionato eletrônico apresenta desafios significativos no âmbito da investigação criminal, sobretudo em razão da complexidade tecnológica envolvida na prática dessas condutas. Diferentemente dos crimes patrimoniais tradicionais, os delitos cibernéticos são caracterizados por alta sofisticação, anonimato e rápida mutação dos meios executórios.

> Os crimes eletrônicos apresentam elevado grau de complexidade investigativa em razão dos mecanismos tecnológicos utilizados pelos criminosos (CAPEZ, 2024).
> Segundo Aragão (2015), a ocultação da identidade virtual representa um dos principais obstáculos enfrentados pelas autoridades policiais.
> "A criminalidade cibernética exige conhecimento técnico especializado e constante atualização investigativa" (ARAGÃO, 2015, p. 87).

Nesse cenário, os agentes criminosos utilizam ferramentas tecnológicas avançadas para dificultar sua identificação, como redes privadas virtuais (VPNs), servidores estrangeiros, criptografia de dados e perfis falsos em plataformas digitais. Essas estratégias tornam o rastreamento da autoria extremamente complexo, exigindo das autoridades policiais conhecimentos técnicos específicos.

Capez (2024) destaca que a investigação dos crimes cibernéticos demanda não apenas conhecimento jurídico, mas também domínio de ferramentas tecnológicas e técnicas de investigação digital, como análise forense de dados, rastreamento de IPs e recuperação de informações apagadas.

Outro fator que agrava a investigação é a atuação de organizações criminosas estruturadas, que operam de forma descentralizada e utilizam "contas de passagem" ou "contas laranja" para ocultar a origem dos valores ilícitos. Essa estrutura dificulta a identificação do verdadeiro beneficiário do crime e compromete a efetividade da persecução penal.

Além disso, a velocidade com que as fraudes são executadas e os valores são transferidos entre diferentes contas bancárias reduz significativamente o tempo hábil para bloqueio e recuperação dos ativos, o que gera prejuízos irreversíveis às vítimas.

.

4.2 A vulnerabilidade das vítimas no ambiente digital

A vulnerabilidade das vítimas constitui um dos principais fatores que contribuem para a elevada incidência do estelionato eletrônico no Brasil. Isso ocorre porque grande parte da população ainda não possui plena conscientização acerca dos riscos existentes no ambiente virtual, o que facilita a atuação de criminosos.

> O crescimento das fraudes eletrônicas demonstra a vulnerabilidade da população diante da criminalidade digital (BITENCOURT, 2023). Segundo Oliveira (2025), muitos golpes virtuais utilizam técnicas de manipulação psicológica para induzir as vítimas ao erro.
> "A prevenção das fraudes eletrônicas depende também da educação digital da população" (OLIVEIRA, 2025, p. 126).

As fraudes digitais são frequentemente estruturadas com base em técnicas de engenharia social, que consistem na manipulação psicológica das vítimas para induzi-las a realizar ações prejudiciais, como fornecimento de senhas, transferências bancárias ou compartilhamento de dados pessoais.

Essas práticas exploram aspectos emocionais como medo, urgência e confiança, simulando situações legítimas, como supostas comunicações de bancos, empresas ou até familiares.

Bitencourt (2023) observa que a evolução tecnológica não apenas ampliou as possibilidades de criminalidade, mas também aumentou a exposição dos indivíduos a riscos virtuais, exigindo uma resposta estatal que vá além da repressão penal, incluindo políticas públicas de educação digital.

Nesse sentido, a ausência de conhecimento técnico por parte das vítimas cria um ambiente propício para a ocorrência de fraudes, evidenciando que o estelionato eletrônico não depende apenas da habilidade do agente, mas também da vulnerabilidade informacional do sujeito passivo.

4.3 O papel do Estado no enfrentamento da criminalidade digital

O enfrentamento eficaz do estelionato eletrônico exige uma atuação coordenada e integrada do Estado, envolvendo diferentes instituições e níveis de poder. A criminalidade digital, por sua natureza complexa e transnacional, ultrapassa os limites tradicionais da investigação criminal, exigindo cooperação interinstitucional e internacional.

> O combate eficiente aos crimes eletrônicos depende da integração entre órgãos públicos e instituições financeiras (GRECO, 2024).
> Segundo Henriques e Gonçalves (2024), a criação de delegacias especializadas representa importante avanço no enfrentamento das fraudes digitais.
> "O Estado deve investir continuamente em inteligência cibernética e cooperação institucional" (GRECO, 2024, p. 228).

O Poder Judiciário, o Ministério Público, as Polícias Civis e Federal, bem como as instituições financeiras e empresas de tecnologia, desempenham papel fundamental na identificação, prevenção e repressão dessas condutas.

A criação de delegacias especializadas em crimes cibernéticos representa um avanço importante, pois permite maior especialização técnica na investigação dessas modalidades criminosas. Contudo, ainda há grande desigualdade estrutural entre os estados brasileiros, o que compromete a uniformidade da resposta estatal.

Greco (2024) destaca que o Estado deve investir continuamente em inteligência cibernética, sistemas integrados de investigação e cooperação internacional, uma vez que a criminalidade digital frequentemente envolve servidores e autores localizados fora do território nacional.

Outro aspecto relevante é a necessidade de regulamentação e fiscalização mais eficiente das instituições financeiras e plataformas digitais, que desempenham papel central na circulação dos valores obtidos ilicitamente.

Além da repressão, o Estado também deve atuar de forma preventiva, por meio de campanhas educativas, programas de conscientização digital e incentivo à segurança da informação, buscando reduzir a vulnerabilidade social frente aos golpes virtuais.

5 ANÁLISE CRÍTICA DOS IMPACTOS DA LEI Nº 15.397/2026

5.1 Avanços promovidos pela nova legislação

A Lei nº 15.397/2026 representa um marco relevante na evolução do Direito Penal contemporâneo brasileiro, especialmente no que se refere ao enfrentamento do estelionato eletrônico e das fraudes patrimoniais praticadas em ambiente digital. Sua promulgação evidencia a tentativa do legislador de adequar o sistema penal às transformações tecnológicas que impactaram diretamente as relações sociais, econômicas e financeiras.

Entre os principais avanços promovidos pela nova legislação, destaca-se o fortalecimento dos mecanismos de investigação criminal, com maior ênfase na coleta de provas digitais e na

rastreabilidade de ativos financeiros. Esse aspecto é fundamental, uma vez que a criminalidade moderna se vale de tecnologias avançadas para ocultar sua autoria e dificultar a recuperação do patrimônio subtraído.

> A Lei nº 15.397/2026 representa importante avanço legislativo no enfrentamento do estelionato eletrônico (NUCCI, 2025).
> Segundo Mesquita, Ferreira e Reis (2025), a nova legislação fortaleceu os mecanismos de repressão às fraudes digitais.
> "A atualização normativa demonstra preocupação estatal com a evolução da criminalidade tecnológica" (NUCCI, 2025, p. 430).

Além disso, a lei promoveu significativa ampliação da cooperação institucional entre órgãos públicos e privados, especialmente instituições financeiras, provedores de internet e plataformas digitais. Essa integração possibilita maior agilidade na identificação de transações suspeitas, contribuindo para a interrupção mais rápida da dinâmica criminosa.

Outro ponto relevante refere-se à proteção jurídica conferida às vítimas, que passam a contar com maior suporte institucional para bloqueio e recuperação de valores obtidos ilicitamente. Tal medida reforça a função reparadora do Direito Penal, aproximando-o de uma perspectiva mais eficiente e menos meramente punitiva.

Segundo Nucci (2025), a atualização legislativa nesse contexto demonstra a necessidade de constante adaptação do Direito Penal às novas formas de criminalidade, especialmente aquelas praticadas em ambientes digitais, onde a velocidade das transformações supera frequentemente a capacidade de resposta normativa.

5.2 Limitações práticas da aplicação da norma

Apesar dos avanços normativos introduzidos pela Lei nº 15.397/2026, sua efetividade prática ainda encontra diversas limitações estruturais, institucionais e operacionais que impactam diretamente os resultados esperados pela política criminal adotada.

Em primeiro lugar, destaca-se a insuficiência de recursos tecnológicos em muitos órgãos de investigação criminal. A ausência de sistemas integrados e de ferramentas avançadas de análise de dados dificulta a identificação de padrões criminosos e o rastreamento de transações financeiras complexas, o que reduz a eficácia da persecução penal.

> Muitos órgãos públicos ainda enfrentam insuficiência estrutural para combate eficiente aos crimes digitais (CAPEZ, 2024).

> Segundo Aragão (2015), a deficiência tecnológica estatal limita a efetividade da persecução penal cibernética.
> "A simples alteração legislativa não é suficiente para solucionar integralmente os problemas da criminalidade digital" (ARAGÃO, 2015, p. 103).

Outro ponto crítico refere-se à defasagem na capacitação dos agentes públicos responsáveis pela investigação de crimes cibernéticos. A criminalidade digital exige conhecimentos altamente especializados, envolvendo informática forense, análise de dados, criptografia e engenharia reversa, o que nem sempre está presente na formação tradicional dos operadores do Direito.

Além disso, a lentidão na cooperação entre instituições públicas e privadas ainda representa um obstáculo relevante. Em muitos casos, a obtenção de informações bancárias ou dados de usuários depende de procedimentos burocráticos que comprometem a rapidez necessária para o bloqueio de valores ilícitos, favorecendo a dissipação do patrimônio obtido por meio da fraude.

Outro aspecto relevante é a própria dinâmica evolutiva da criminalidade digital. Os criminosos frequentemente desenvolvem novas técnicas de fraude, como o uso de inteligência artificial, deepfakes, perfis falsos automatizados e redes descentralizadas, o que torna o sistema penal constantemente reativo, e não preventivo.

Nesse sentido, Greco (2024) ressalta que a mera alteração legislativa não é suficiente para enfrentar a complexidade da criminalidade moderna, sendo indispensável a articulação entre legislação eficiente, estrutura investigativa robusta e políticas públicas preventivas.

5.3 Perspectivas futuras do combate aos crimes eletrônicos

O futuro do enfrentamento ao estelionato eletrônico exige uma mudança estrutural na forma como o Estado lida com a criminalidade digital, indo além da simples repressão penal e incorporando estratégias integradas de prevenção, tecnologia e cooperação internacional.

Uma das principais perspectivas está relacionada ao uso crescente de tecnologias avançadas de investigação, como inteligência artificial, machine learning e análise preditiva de dados. Essas ferramentas permitem identificar padrões suspeitos de comportamento financeiro e antecipar possíveis fraudes antes mesmo da sua consumação, conferindo maior caráter preventivo à atuação estatal.

> O enfrentamento da criminalidade virtual exige constante atualização legislativa e tecnológica (GRECO, 2024).
> Segundo Souza (2024), a inteligência artificial poderá representar importante instrumento de combate às fraudes eletrônicas.
> "A prevenção e repressão dos crimes digitais dependem da integração entre tecnologia, investigação e educação digital" (SOUZA, 2024, p. 51).

Outro ponto relevante diz respeito à necessidade de fortalecimento da cooperação internacional, uma vez que grande parte dos crimes digitais possui natureza transnacional. Os autores frequentemente operam a partir de diferentes países, utilizando servidores estrangeiros e sistemas de pagamento globais, o que exige integração entre autoridades de diferentes jurisdições.

Além disso, a capacitação contínua de agentes públicos torna-se indispensável. A evolução constante das tecnologias utilizadas pelos criminosos exige que policiais, promotores e magistrados estejam em permanente atualização técnica, sob pena de o sistema de justiça penal se tornar obsoleto frente às novas práticas delitivas.

No campo social, destaca-se a importância da educação digital da população como medida preventiva essencial. A conscientização sobre riscos virtuais, segurança de dados pessoais e identificação de golpes eletrônicos pode reduzir significativamente a vulnerabilidade das potenciais vítimas.

Por fim, é possível afirmar que a Lei nº 15.397/2026 representa um importante avanço normativo, mas seu verdadeiro impacto dependerá da capacidade do Estado de integrar tecnologia, estrutura institucional e políticas públicas de prevenção. Assim, o combate ao estelionato eletrônico deve ser compreendido como um desafio multidimensional, que ultrapassa os limites do Direito Penal tradicional.

6 CONSIDERAÇÕES FINAIS

A presente pesquisa permitiu analisar os impactos da Lei nº 15.397/2026 no tratamento jurídico do crime de estelionato, com ênfase nas fraudes eletrônicas e na modernização dos mecanismos de persecução penal no ambiente digital.

Verificou-se que a nova legislação representa um importante avanço no ordenamento jurídico brasileiro, ao buscar adequar o Direito Penal às transformações sociais e tecnológicas decorrentes da expansão da criminalidade cibernética. Nesse sentido, a norma promoveu significativa reestruturação dos instrumentos de investigação criminal, fortalecendo a atuação

conjunta entre órgãos de persecução penal, instituições financeiras e demais agentes envolvidos na identificação de práticas fraudulentas.

Observou-se, ainda, que a Lei nº 15.397/2026 contribui para o aprimoramento da proteção das vítimas, especialmente no que se refere à possibilidade de rastreamento e bloqueio de valores obtidos ilicitamente, o que reforça a dimensão patrimonial e reparatória do Direito Penal contemporâneo.

Entretanto, conclui-se que a efetividade prática da referida legislação não depende exclusivamente de sua previsão normativa, mas está diretamente condicionada à capacidade estrutural e tecnológica dos órgãos responsáveis pela investigação e repressão dos delitos. A ausência de integração entre sistemas, a limitação de recursos tecnológicos e a necessidade de capacitação contínua dos profissionais da segurança pública ainda representam obstáculos relevantes à plena eficácia da norma.

Ademais, destaca-se que o enfrentamento do estelionato eletrônico exige não apenas respostas repressivas, mas também estratégias preventivas, voltadas à educação digital da população e à conscientização sobre os riscos inerentes ao ambiente virtual. A vulnerabilidade das vítimas permanece como um dos principais fatores de sucesso das fraudes eletrônicas, o que evidencia a necessidade de políticas públicas permanentes de orientação e proteção.

Dessa forma, conclui-se que, embora a Lei nº 15.397/2026 represente um avanço significativo na modernização do sistema penal brasileiro, o combate eficaz à criminalidade digital demanda uma atuação integrada e multidimensional, envolvendo legislação atualizada, desenvolvimento tecnológico, cooperação institucional e conscientização social contínua.

Assim, o enfrentamento do estelionato eletrônico não se esgota na esfera normativa, mas exige um esforço permanente do Estado e da sociedade para acompanhar a constante evolução das formas de criminalidade no ambiente digital.

REFERÊNCIAS

ARAGÃO, David Farias de. *Crimes cibernéticos na pós-modernidade: direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil*. Dissertação (Mestrado em Direito) – Universidade Federal do Maranhão, São Luís, 2015. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/667. Acesso em: 29 maio 2026.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*. São Paulo: Saraiva, 2023.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. *Código Penal*. Brasília, DF: Presidência da República, 1940. Disponível em:

https://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Acesso em: 29 maio 2026.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. *Diário Oficial da União*, Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 29 maio 2026.

BRASIL. Superior Tribunal de Justiça. *Jurisprudência sobre estelionato eletrônico*. Brasília, DF. Disponível em: https://www.stj.jus.br. Acesso em: 29 maio 2026.

BRASIL. Supremo Tribunal Federal. *Legislação e jurisprudência penal*. Brasília, DF. Disponível em: https://www.stf.jus.br. Acesso em: 29 maio 2026.

CAPEZ, Fernando. *Curso de Direito Penal*. São Paulo: Saraiva, 2024.

COMBATE ao estelionato eletrônico no Brasil: análise das condições de investigação ocorridas no Pará, Piauí, Distrito Federal, São Paulo e Paraná. *Revista Brasileira de Criminalística*, v. 15, n. 1, p. 13-23, 2026. Disponível em: https://revista.rbc.org.br/index.php/rbc/article/view/955. Acesso em: 29 maio 2026.

COSTA, Fabrício Reis. *O crime de estelionato: contornos típicos e questões contemporâneas*. Dissertação (Mestrado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024. Disponível em: https://repositorio.usp.br/item/003263320. Acesso em: 29 maio 2026.

GRECO, Rogério. *Curso de Direito Penal: Parte Especial*. Rio de Janeiro: Impetus, 2024.

HENRIQUES, Thiago Alves; GONÇALVES, Samuel Martins. Crimes digitais: análise sobre o estelionato virtual. *Revista Eletrônica de Ciências Jurídicas*, v. 14, n. 1, 2024. Disponível em: https://revista.fadipa.br/index.php/cjuridicas/article/view/576. Acesso em: 29 maio 2026.

HENRIQUES, Thiago Alves; GONÇALVES, Samuel Martins. Crimes digitais: análise sobre o estelionato virtual. *Revista Eletrônica de Ciências Jurídicas*, v. 14, n. 1, 2024. Disponível em: https://revista.fadipa.br/index.php/cjuridicas/article/view/576. Acesso em: 29 maio 2026.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Metodologia do Trabalho Científico*. São Paulo: Atlas, 2014.

MESQUITA, Milson Rodrigues; FERREIRA, Rony de Oliveira; REIS, Gabriel de Castro Borges. Estelionato digital: a natureza jurídica da ação penal para o crime de estelionato digital praticado em ambientes virtuais. *Revista Raízes no Direito*, v. 14, n. 1, p. 187-202, 2025. Disponível em: https://revistas.unievangelica.edu.br/index.php/raizesnodireito/article/view/8047. Acesso em: 29 maio 2026.

NUCCI, Guilherme de Souza. *Código Penal Comentado*. São Paulo: Forense, 2025.

SALLES, Gabriel Felipe Ribeiro Henderson. *O direito digital e a punibilidade dos crimes cibernéticos no ordenamento jurídico brasileiro*. Trabalho de Conclusão de Curso (Graduação

em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: https://pantheon.ufrj.br/handle/11422/22833. Acesso em: 29 maio 2026.

SOUZA, Elias Emanuel Bemerguy de; SOARES, Luiz Felipe Pinheiro; GONÇALVES, Dimas Melo. A criminalização da prática de phishing e seus impactos no ordenamento jurídico na cidade de Manaus. *Periódicos Brasil – Pesquisa Científica*, v. 5, n. 1, p. 2018-2037, 2026. Disponível em: https://periodicosbrasil.emnuvens.com.br/revista/article/view/531. Acesso em: 29 maio 2026.

SOUZA, Vinícius Cunha de. *Estelionato digital: uma análise sobre o delito de fraude eletrônica na região Norte do Brasil*. Monografia (Graduação em Direito) – Universidade Federal do Tocantins, Arraias, 2025. Disponível em: https://repositorio.uft.edu.br/handle/11612/8166. Acesso em: 29 maio 2026.