



**DANIELE DE SOUSA QUEIROZ
MARIA VITÓRIA FONTES DE SOUSA
SANDRA LUANA COSTA ARAÚJO**

**O CRIME DE ESTELIONATO DIGITAL E A FRAUDE VIRTUAL:
análise jurídica e preventiva à luz da legislação brasileira do código penal,
especialmente após as alterações introduzidas pela Lei nº 15.397/2026**

TERESINA-PI

2026

**DANIELE DE SOUSA QUEIROZ
MARIA VITÓRIA FONTES DE SOUSA
SANDRA LUANA COSTA ARAÚJO**

**O CRIME DE ESTELIONATO DIGITAL E A FRAUDE VIRTUAL:
análise jurídica e preventiva à luz da legislação brasileira do código penal,
especialmente após as alterações introduzidas pela Lei nº 15.397/2026**

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

Orientadora: Prof. Me. Orlando Mauriz Ramos

TERESINA-PI

2026

FICHA CATALOGRÁFICA

Q3c Queiroz, Daniele de Sousa.

O crime de estelionato digital e a fraude virtual: análise jurídica e preventiva à luz da legislação brasileira do código penal, especialmente após as alterações introduzidas pela lei nº 15.397/2026 / Daniele de Sousa Queiroz; Maria Vitória Fontes de Sousa; Sandra Luana Costa Araújo. – Teresina: UNINOVAFAPI, 2026.

Orientador (a): Profº. Me. Orlando Mauriz Ramos – UNINOVAFAPI, 2026.

33.p.; 23cm.

Trabalho de conclusão (Bacharelado em Direito). – UNINOVAFAPI, Teresina, 2026.

1. Estelionato digital. 2. Fraude virtual. 3. Crimes cibernéticos. 4. Lei nº 15.397/2026. 5. Direito penal. I. Título. II. Sousa, Maria Vitória Fontes de. III. Araújo, Sandra Luana Costa.

CDD 341.5572

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

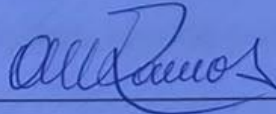
DANIELE DE SOUSA QUEIROZ
MARIA VITÓRIA FONTES DE SOUSA
SANDRA LUANA COSTA ARAÚJO

**O CRIME DE ESTELIONATO DIGITAL E A FRAUDE VIRTUAL:
análise jurídica e preventiva à luz da legislação brasileira do código
penal, especialmente após as alterações introduzidas pela Lei nº
15.397/2026.**

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

Data de Aprovação: 25 / 06 / 2026

BANCA EXAMINADORA



Professor Mestre Orlando Mauriz Ramos
Afya Centro Universitário Uninovafapi
(Orientador)



Professora Mestre Enedina Gizeli Albano Moura
Afya Centro Universitário Uninovafapi
(1º Examinadora)



Professora Mestre Sara Morgana Silva Carvalho Lopes
Afya Centro Universitário Uninovafapi
(2º Examinadora)

RESUMO

O presente estudo analisa o crime de estelionato digital e as fraudes virtuais no ordenamento jurídico brasileiro, com enfoque nas alterações introduzidas pela Lei nº 15.397/2026. A pesquisa aborda a evolução legislativa relacionada aos crimes cibernéticos, destacando os avanços promovidos pelas Leis nº 12.737/2012, nº 12.965/2014, nº 14.155/2021 e nº 14.478/2022, que serviram de base para o aprimoramento do combate às fraudes eletrônicas. Examina-se a conceituação do estelionato virtual, suas principais características, os sujeitos envolvidos e os desafios enfrentados pelas autoridades na persecução penal desses delitos. O estudo demonstra que a Lei nº 15.397/2026 fortaleceu significativamente a repressão criminal ao ampliar penas, tipificar novas condutas relacionadas ao uso de contas bancárias de terceiros e instituir mecanismos processuais mais céleres para o bloqueio de ativos oriundos de fraudes. Contudo, verifica-se que a resposta penal, embora necessária, não é suficiente para erradicar o problema. A prevenção, por meio da educação digital, do investimento em segurança cibernética e da cooperação entre instituições públicas e privadas, revela-se fundamental para reduzir a incidência desses crimes. Conclui-se que o enfrentamento efetivo do estelionato digital exige uma atuação integrada entre legislação atualizada, eficiência investigativa, inovação tecnológica e conscientização social.

Palavras-chave: Estelionato Digital; Fraude Virtual; Crimes Cibernéticos; Lei nº 15.397/2026; Direito Penal.

ABSTRACT

This study analyzes the crime of digital fraud and virtual scams within the Brazilian legal system, focusing on the changes introduced by Law No. 15.397/2026. The research examines the legislative evolution related to cybercrimes, highlighting the advances promoted by Laws No. 12.737/2012, No. 12.965/2014, No. 14.155/2021, and No. 14.478/2022, which served as a foundation for strengthening the fight against electronic fraud. The paper discusses the concept of digital fraud, its main characteristics, the parties involved, and the challenges faced by authorities in the criminal prosecution of such offenses. The study demonstrates that Law No. 15.397/2026 significantly strengthened criminal enforcement by increasing penalties, criminalizing new conducts related to the use of third-party bank accounts, and establishing faster procedural mechanisms for freezing assets derived from fraudulent activities. However, it is observed that criminal punishment alone is insufficient to eliminate the problem. Prevention through digital education, investment in cybersecurity, and cooperation between public and private institutions is essential to reduce the occurrence of these crimes. It is concluded that the effective fight against digital fraud requires integrated action involving updated legislation, efficient investigations, technological innovation, and public awareness.

Keywords: Digital Fraud; Virtual Scams; Cybercrime; Law No. 15.397/2026; Criminal Law.

SUMÁRIO

1 INTRODUÇÃO	7
2 ARTIGO.....	9
3 CONSIDERAÇÕES FINAIS	28
REFERÊNCIAS	30

1 INTRODUÇÃO

Em um mundo cada vez mais conectado, as fraudes eletrônicas e o chamado estelionato digital têm se disseminado de forma preocupante. Como observa Campelo (2023), “com o crescimento da tecnologia e das transações financeiras online, a fraude com a utilização de ativos virtuais... tem se tornado cada vez mais comum”.

Essa realidade é confirmada por pesquisa do DataSenado de 2024, que revela que 24% da população brasileira com mais de 16 anos sofreu algum golpe digital nos 12 meses anteriores. O contexto, portanto, é o de uma dependência crescente das atividades virtuais em transações econômicas, expondo pessoas e empresas a novos riscos patrimoniais (Campelo, 2023; Agência Senado, 2024).

Para enfrentar esse avanço dos crimes patrimoniais virtuais, o ordenamento jurídico brasileiro passou por profundas atualizações nos últimos anos. Um marco importante ocorreu com a edição da Lei nº 14.155/2021, que endureceu as penas para crimes cibernéticos e inseriu o crime de fraude eletrônica no Código Penal.

Como ressalta Aras (2023), a pena prevista no art. 171-A (reclusão de 4 a 8 anos) difere “drasticamente” da escala penal do estelionato comum, que varia de 1 a 5 anos. Mais recentemente, a Lei nº 15.397/2026 reforçou a repressão aos golpes eletrônicos: conforme noticiado pelo Senado Federal, a nova norma “aumenta penas para crimes como ... estelionato e fraudes eletrônicas”, além de tipificar o uso de contas bancárias como “laranja”. Essas mudanças legislativas recentes; com foco no endurecimento de penas e na ampliação das condutas incriminadas; fundamentam o presente estudo (Aras, 2023; Nascimento, 2026).

O presente trabalho delimita-se a analisar, à luz do Código Penal brasileiro atualizado, o crime de estelionato digital e as fraudes virtuais correlatas. Pretende-se compreender como esses delitos são definidos pelo legislador e quais questões jurídicas surgem após as alterações introduzidas em 2026.

Em outras palavras, formula-se como problema de pesquisa: as recentes alterações legais (art. 171-A e Lei 15.397/2026) oferecem mecanismos penais adequados para inibir golpes digitais? Existem ambiguidades ou lacunas que dificultem a aplicação das normas penais nos casos concretos de fraude online? Essa delimitação busca focar o estudo no exame das inovações legais e de seus impactos práticos (Campelo, 2023).

A partir desse problema, levantam-se hipóteses que nortearão a análise. Hipotetiza-se que o endurecimento das penas e a criação de novos tipos penais reforçam a eficácia repressiva contra o estelionato digital. Por outro lado, admite-se a hipótese de que, isoladamente, as medidas penais ainda sejam insuficientes para coibir completamente as fraudes virtuais, exigindo esforços complementares de prevenção e educação digital.

Além disso, postula-se que a nova redação dos tipos penais possa gerar controvérsias interpretativas, dependendo da dinâmica dos golpes praticados. Em suma, as hipóteses examinadas incluem: (a) o aumento das sanções legais desestimula potenciais criminosos, (b) políticas extrapenais de prevenção são necessárias para eficácia plena, e (c) ainda podem ocorrer debates sobre o enquadramento dos fatos nas inovações legislativas.

O objetivo geral deste trabalho é analisar juridicamente o crime de estelionato digital e as fraudes virtuais no Brasil, especialmente após as alterações trazidas pela Lei nº 15.397/2026.

Como objetivos específicos, propõe-se: descrever os dispositivos penais atualizados (como o art. 171-A e as mudanças no art. 171 do CP); examinar a amplitude e os limites da responsabilização penal em casos de golpes eletrônicos; avaliar a necessidade de medidas preventivas adicionais; e discutir o impacto das mudanças no procedimento criminal e na atuação do Ministério Público.

A relevância deste estudo justifica-se pelo forte impacto social e econômico dos crimes cibernéticos. O elevado número de vítimas de golpes virtuais torna urgente a compreensão crítica da legislação penal sobre o tema.

Sobretudo, o exame aprofundado das normas atualizadas contribui para a segurança jurídica e para a eficácia das ações do Ministério Público e do Judiciário no enfrentamento das fraudes online. Dada a gravidade da questão; que em 2024 afetou mais de 40 milhões de brasileiros; analisar o estelionato digital na legislação penal atual é fundamental para subsidiar políticas públicas de prevenção e reforçar a proteção patrimonial das pessoas (Agência Senado, 2024).

Para o desenvolvimento da presente pesquisa, o trabalho foi estruturado em três seções. Na primeira seção, aborda-se a introdução deste trabalho. Na segunda seção, apresenta-se o artigo completo. Por fim, na terceira seção, elenca-se as considerações finais.

2 ARTIGO

O CRIME DE ESTELIONATO DIGITAL E A FRAUDE VIRTUAL: análise jurídica e preventiva à luz da legislação brasileira do código penal, especialmente após as alterações introduzidas pela Lei nº 15.397/2026

THE CRIME OF DIGITAL EMBEZZLEMENT AND VIRTUAL FRAUD: a legal and preventive analysis in light of Brazilian Criminal Code legislation, especially following the amendments introduced by Law No. 15,397/2026

Daniele de Sousa Queiroz¹
Maria Vitória Fontes de Sousa²
Sandra Luana Costa Araújo³
Orlando Mauriz Ramos⁴

RESUMO

O presente estudo analisa o crime de estelionato digital e as fraudes virtuais no ordenamento jurídico brasileiro, com enfoque nas alterações introduzidas pela Lei nº 15.397/2026. A pesquisa aborda a evolução legislativa relacionada aos crimes cibernéticos, destacando os avanços promovidos pelas Leis nº 12.737/2012, nº 12.965/2014, nº 14.155/2021 e nº 14.478/2022, que serviram de base para o aprimoramento do combate às fraudes eletrônicas. Examina-se a conceituação do estelionato virtual, suas principais características, os sujeitos envolvidos e os desafios enfrentados pelas autoridades na persecução penal desses delitos. O estudo demonstra que a Lei nº 15.397/2026 fortaleceu significativamente a repressão criminal ao ampliar penas, tipificar novas condutas relacionadas ao uso de contas bancárias de terceiros e instituir mecanismos processuais mais céleres para o bloqueio de ativos oriundos de fraudes. Contudo, verifica-se que a resposta penal, embora necessária, não é suficiente para erradicar o problema. A prevenção, por meio da educação digital, do investimento em segurança cibernética e da cooperação entre instituições públicas e privadas, revela-se fundamental para reduzir a incidência desses crimes. Conclui-se que o enfrentamento efetivo do estelionato digital exige uma atuação integrada entre legislação atualizada, eficiência investigativa, inovação tecnológica e conscientização social.

Palavras-chave: Estelionato Digital; Fraude Virtual; Crimes Cibernéticos; Lei nº 15.397/2026; Direito Penal.

ABSTRACT

This study analyzes the crime of digital fraud and virtual scams within the Brazilian legal system, focusing on the changes introduced by Law No. 15.397/2026. The

¹ Discente do Curso de Direito da Afya Centro Universitário Uninovafapi. E-mail: danieliqueiroz123@gmail.com.

² Discente do Curso de Direito da Afya Centro Universitário Uninovafapi. link. E-mail: mavickfontes0208@gmail.com.

³ Discente do Curso de Direito da Afya Centro Universitário Uninovafapi. E-mail: sandraluana21@hotmail.com.

⁴ Bacharel em Direito pela Universidade Estadual do Piauí; Especialista em Ciências Criminais pela Universidade Federal do Piauí; Mestre em Direito pela Universidade Católica de Brasília. Professor do Curso de Direito da Afya Centro Universitário Uninovafapi.

research examines the legislative evolution related to cybercrimes, highlighting the advances promoted by Laws No. 12.737/2012, No. 12.965/2014, No. 14.155/2021, and No. 14.478/2022, which served as a foundation for strengthening the fight against electronic fraud. The paper discusses the concept of digital fraud, its main characteristics, the parties involved, and the challenges faced by authorities in the criminal prosecution of such offenses. The study demonstrates that Law No. 15.397/2026 significantly strengthened criminal enforcement by increasing penalties, criminalizing new conducts related to the use of third-party bank accounts, and establishing faster procedural mechanisms for freezing assets derived from fraudulent activities. However, it is observed that criminal punishment alone is insufficient to eliminate the problem. Prevention through digital education, investment in cybersecurity, and cooperation between public and private institutions is essential to reduce the occurrence of these crimes. It is concluded that the effective fight against digital fraud requires integrated action involving updated legislation, efficient investigations, technological innovation, and public awareness.

Keywords: Digital Fraud; Virtual Scams; Cybercrime; Law No. 15.397/2026; Criminal Law.

1. INTRODUÇÃO

Em um mundo cada vez mais conectado, as fraudes eletrônicas e o chamado estelionato digital têm se disseminado de forma preocupante. Como observa Campelo (2023), “com o crescimento da tecnologia e das transações financeiras online, a fraude com a utilização de ativos virtuais... tem se tornado cada vez mais comum”.

Essa realidade é confirmada por pesquisa do DataSenado de 2024, que revela que 24% da população brasileira com mais de 16 anos sofreu algum golpe digital nos 12 meses anteriores. O contexto, portanto, é o de uma dependência crescente das atividades virtuais em transações econômicas, expondo pessoas e empresas a novos riscos patrimoniais (Campelo, 2023; Agência Senado, 2024).

Para enfrentar esse avanço dos crimes patrimoniais virtuais, o ordenamento jurídico brasileiro passou por profundas atualizações nos últimos anos. Um marco importante ocorreu com a edição da Lei nº 14.155/2021, que endureceu as penas para crimes cibernéticos e inseriu o crime de fraude eletrônica no Código Penal.

Como ressalta Aras (2023), a pena prevista no art. 171-A (reclusão de 4 a 8 anos) difere “drasticamente” da escala penal do estelionato comum, que varia de 1 a 5 anos. Mais recentemente, a Lei nº 15.397/2026 reforçou a repressão aos golpes eletrônicos: conforme noticiado pelo Senado Federal, a nova norma “aumenta penas para crimes como estelionato e fraudes eletrônicas”, além de

tipificar o uso de contas bancárias como “laranja”. Essas mudanças legislativas recentes; com foco no endurecimento de penas e na ampliação das condutas incriminadas; fundamentam o presente estudo (Aras, 2023; Nascimento, 2026).

O presente trabalho delimita-se a analisar, à luz do Código Penal brasileiro atualizado, o crime de estelionato digital e as fraudes virtuais correlatas. Pretende-se compreender como esses delitos são definidos pelo legislador e quais questões jurídicas surgem após as alterações introduzidas em 2026.

Em outras palavras, formula-se como problema de pesquisa: as recentes alterações legais (art. 171-A e Lei 15.397/2026) oferecem mecanismos penais adequados para inibir golpes digitais? Existem ambiguidades ou lacunas que dificultem a aplicação das normas penais nos casos concretos de fraude online? Essa delimitação busca focar o estudo no exame das inovações legais e de seus impactos práticos (Campelo, 2023).

A partir desse problema, levantam-se hipóteses que nortearão a análise. Hipotetiza-se que o endurecimento das penas e a criação de novos tipos penais reforçam a eficácia repressiva contra o estelionato digital. Por outro lado, admite-se a hipótese de que, isoladamente, as medidas penais ainda sejam insuficientes para coibir completamente as fraudes virtuais, exigindo esforços complementares de prevenção e educação digital.

Além disso, postula-se que a nova redação dos tipos penais possa gerar controvérsias interpretativas, dependendo da dinâmica dos golpes praticados. Em suma, as hipóteses examinadas incluem: (a) o aumento das sanções legais desestimula potenciais criminosos, (b) políticas extrapenais de prevenção são necessárias para eficácia plena, e (c) ainda podem ocorrer debates sobre o enquadramento dos fatos nas inovações legislativas.

O objetivo geral deste trabalho é analisar juridicamente o crime de estelionato digital e as fraudes virtuais no Brasil, especialmente após as alterações trazidas pela Lei nº 15.397/2026.

Como objetivos específicos, propõe-se: descrever os dispositivos penais atualizados (como o art. 171-A e as mudanças no art. 171 do CP); examinar a amplitude e os limites da responsabilização penal em casos de golpes eletrônicos; avaliar a necessidade de medidas preventivas adicionais; e discutir o impacto das mudanças no procedimento criminal e na atuação do Ministério Público.

A relevância deste estudo justifica-se pelo forte impacto social e econômico

dos crimes cibernéticos. O elevado número de vítimas de golpes virtuais torna urgente a compreensão crítica da legislação penal sobre o tema.

Sobretudo, o exame aprofundado das normas atualizadas contribui para a segurança jurídica e para a eficácia das ações do Ministério Público e do Judiciário no enfrentamento das fraudes online. Dada a gravidade da questão; que em 2024 afetou mais de 40 milhões de brasileiros; analisar o estelionato digital na legislação penal atual é fundamental para subsidiar políticas públicas de prevenção e reforçar a proteção patrimonial das pessoas (Agência Senado, 2024).

1.0 ESTELIONATO VIRTUAL E O DIREITO PENAL

1.1 Estelionato Virtual: Conceitos e Características

O estelionato praticado pela internet é uma das modalidades recorrentes no contexto atual, utilizado por muitos perpetradores para chegar facilmente às suas vítimas; muitas pessoas mentem e criam perfis falsos nas redes sociais, além de invadir contas e dados de outras pessoas com o único propósito de chantagem e lucros ilegais.

De acordo com Oliveira (2020), é verdade que o avanço da tecnologia tornou as coisas melhores e mais conectadas entre as pessoas, mas ao mesmo tempo que os criminosos usaram essas oportunidades para seu próprio benefício ou para outros, às custas de outros, eles foram ousados o suficiente para classificá-las como crimes cibernéticos.

Nesse contexto, ainda de acordo com o autor,

(...) pode se entender preliminarmente que o estelionato virtual é aquele em que o indivíduo servindo-se de equipamentos tecnológicos e acesso à rede, pratica em benefício próprio ou de outrem e em prejuízo alheio, o ato de induzir ou manter a vítima em erro, utilizando-se quaisquer meios fraudulentos e almejando vantagem ilícita (Oliveira, 2020, p. 32).

De acordo com o entendimento do Tribunal de Justiça do Distrito Federal e dos Territórios – TJDF (2021), o Estelionato Virtual ocorre quando o criminoso consegue enganar alguém, por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento, a fornecer dados confidenciais, tais como, senhas de acesso, bancos ou número de cartão de crédito ou débito.

Ocorre crime de estelionato virtual em muitas ocasiões quando criminosos criam links, e-mails falsos, etc. pretendem não ser identificados e, portanto,

prometem fazer algo que sabem que não pode ser cumprido, mas cumprem essa promessa em troca de um benefício que na maioria das vezes é uma quantia em dinheiro. Em suma, a fraude virtual comete-se incitando a vítima, através de meios digitais, aproveitando as lacunas que estes permitem para obter vantagem (Ataide, 2017).

Em consonância, a advogada criminalista e professora, Cristiane Dupret, em um texto escrito ao portal Instituto Direito Penal Brasileiro - IDPB, descreve que:

(...) os estelionatários digitais utilizam diferentes técnicas, como phishing, engenharia social, fraudes online, e-mails falsos e outros métodos para ludibriar vítimas e obter informações pessoais ou financeiras, realizar transações fraudulentas ou enganar pessoas de várias maneiras (Dupret, 2023, p. 4).

Com relação ao sujeito ativo no contexto do estelionato virtual, Carvalho (2023 *Apud* CUNHA, 2021) esclarece que este sujeito é aquele que pratica fraudes pela internet, visando obter vantagens financeiras ou patrimoniais de forma ilícita.

Além disso, esse indivíduo pode ser qualquer pessoa com as habilidades técnicas necessárias para cometer fraudes on-line, incluindo conhecimentos de informática, de programação e de segurança cibernética. Normalmente, esses golpistas atuam em gangues especializadas em crimes cibernéticos, utilizando técnicas avançadas para enganar suas vítimas (Carvalho, 2023 *Apud* Cunha, 2021).

1.2 Estelionato Virtual previsões legais anteriores à Lei nº 15.397/2026

No Brasil, o crime de estelionato virtual pode ser enquadrado principalmente no artigo 171 do Código Penal Brasileiro, que trata do estelionato em geral:

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

§ 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

§ 2º - Nas mesmas penas incorre quem:

§ 3º - 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 (BRASIL, 1940)

Além disso, há outras leis que podem ser aplicadas dependendo do contexto específico do crime cibernético, como é o caso da Lei 12.737 de 2012,

popularmente conhecida com Lei Carolina Dieckmann, que “dispõe a tipificação criminal de delitos informáticos e dá outras providências, ou seja, aqueles voltados contra dispositivos ou sistemas de informação e não os crimes comuns praticados por meio do computador” (Cardoso, 2023, p. 3390).

De acordo com Cardoso (2023), a “Lei Carolina Dieckmann” (Lei nº 12.737/2012) inseriu o delito de crime de invasão de dispositivo informático no Código Penal, tendo em vista que a atriz havia sido vítima dessa conduta poucos meses antes, em maio de 2012, quando ainda não havia uma figura típica específica, possibilitou quatro alterações no crime, modificou a redação do caput, ampliando a incidência do tipo penal, majorou a pena do crime na sua forma básica (caput do art. 154-A), majorou os limites da causa de aumento de pena do § 2º; majorou a pena da qualificadora do § 3º.

No mesmo sentido da Lei Carolina Dieckmann, mas ampliando todo o contexto jurídico brasileiro no tocante dos crimes praticados através dos meios digitais, no ano de 2014, foi promulgada a Lei 12.965/2014, conhecida popularmente como o Marco Civil da Internet.

O Marco Civil da Internet estabelece princípios que regem o uso da Internet no Brasil, como princípios de privacidade e proteção de dados pessoais. Embora seja considerado de natureza “civil”, tem impacto na investigação e ação contra o crime cibernético (Machado; Grott, 2022 *APUD* Nucci, 2017).

Sobre as contribuições da Lei 12.965/2014 para o combate de crimes virtuais, tais como o Estelionato Virtual, os autores Silva e Neto (2017) esclarecem que:

Com a aprovação do Marco Civil, os blogs devem ser guardados por um ano e esse prazo pode ser estendido, ou seja, só será obtido o blog por medida judicial assim como outra ordem judicial autoriza a associação entre número do IP e do número. Nesse caso, é preciso comprovar que haja um crime naquele horário e que o usuário seja suspeito de ter cometido esse crime. Os usuários respondem pelo conteúdo que publicarem e os provedores de acesso não podem ser responsabilizados por danos decorrentes de conteúdos gerados por usuários. Os provedores de conteúdo serão responsabilizados caso não acatem no prazo determinado decisões judiciais que mandem tirar conteúdos gerados pelos usuários (Silva; Neto, 2017, p. 13 *APUD* Peasani, 2014).

Contudo, Silva (2023) ressalta que, o Marco Civil da internet, não tipifica condutas penais, tendo em vista que as condutas que possam resultar da prática de qualquer modalidade de crime virtual serão observadas o Código Penal, bem como no âmbito da compensação por dano civil ou mesmo no âmbito da

responsabilidade civil objetiva, de acordo com o Código Civil vigente.

Em se tratando de leis mais específicas, no que tange diretamente crimes como o estelionato virtual, promulgou-se no ano de 2021, a Lei nº 14.155/2021, popularmente conhecida como "Lei do Superendividamento", que trouxe importantes alterações ao Código Penal Brasileiro e introduziu dispositivos específicos para tratar do crime de estelionato virtual.

Desta forma, a Lei nº 14.155/2021, ou "Lei do Superendividamento", modificou o Código Penal acrescentando o artigo 171-A, que trata do estelionato cometido de forma eletrônica, digital ou similar e trazendo alterações referentes aos crimes de invasão de dispositivos informáticos, furto mediante fraude eletrônica, estelionato mediante fraude eletrônica, dentre outras (Pinheiro, 2022).

Além disso, de acordo com o Juiz Fernando Brandini Barbagalo (2022, p. 2), com essa Lei do Superendividamento, “finalmente, foram criados os crimes específicos de furto mediante fraude eletrônica (art. 155, § 4º-B do CP) e de fraude eletrônica (art. 171, § 2º-A do CP)”.

A mesma lei também determina o foro das fraudes cometidas por meio de cheques sem fundos, pagamentos indevidos ou transferências de valores, nesses casos, o local da residência da vítima (art. 70, § 4º, CP) (Barbagalo, 2022).

Além das relatadas leis citadas anteriormente, há dois outros projetos de leis em andamento, que preveem pressionar contra os crimes de estelionato virtual; um destes é o Projeto de Lei nº 2254 de 2022, que visa alterar o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para recrudescer o tratamento penal dispensado aos crimes de extorsão, de estelionato e de fraude no comércio, e a Lei nº 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), para incluir o crime de estelionato contra idoso ou vulnerável no rol dos crimes hediondos (Federal, 2022).

O outro projeto em curso de aprovação é o Projeto de Lei nº 2339 de 2023, que prevê a figura do estelionato em programa de renda extra (Estelionato Digital), alterando o art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) (Deputados, 2023).

2. A FRAUDE VIRTUAL E O DIREITO PENAL: ANTES E DEPOIS DA LEI Nº 15.397/2026

2.1 O Cenário Normativo Anterior: As Leis 14.155/2021 e 14.478/2022 como Marcos Transitórios

Até o início da década de 2020, o Direito Penal brasileiro enfrentava imensas dificuldades para lidar com a criminalidade cibernética patrimonial. Antes de alterações legislativas mais robustas, promotores e juízes precisavam adaptar a redação clássica do artigo 171 do Código Penal, datada de 1940, para enquadrar golpes sofisticados praticados via internet.

Essa analogia forçada frequentemente esbarrava no princípio da taxatividade penal, gerando insegurança jurídica e penas brandas (de 1 a 5 anos), que permitiam a suspensão condicional do processo e a rápida substituição por penas restritivas de direitos, gerando um sentimento de impunidade social (Capez, 2023).

O primeiro grande ponto de inflexão nesse cenário de defasagem ocorreu com a promulgação da Lei nº 14.155/2021. Este diploma legal foi responsável por criar, no § 2º-A do artigo 171 do Código Penal, a figura qualificada da fraude eletrônica.

A partir desse momento, o legislador passou a punir com reclusão de 4 a 8 anos o estelionato cometido com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento.

Essa mudança demonstrou o reconhecimento estatal de que o engodo virtual possui um potencial lesivo difuso e muito superior ao estelionato presencial (Masson, 2024, p. 512).

Além do aumento da pena, a legislação de 2021 tentou resolver um dos maiores gargalos processuais da época: a fixação da competência territorial. Historicamente, os tribunais superiores divergiam se a competência para julgar o estelionato virtual era do local de onde o dinheiro partiu ou de onde foi sacado.

Com a inserção do § 4º no art. 70 do Código de Processo Penal, consolidou-se que, nos casos de fraude eletrônica, a competência será definida pelo local do domicílio da vítima, facilitando o acesso do ofendido à Justiça e a comunicação

com as autoridades investigativas locais (Távora; Alencar, 2024).

Em sequência a essa modernização, o legislador precisou lidar com o avanço de uma nova tecnologia que facilitou a lavagem de dinheiro e a ocultação de patrimônio: as criptomoedas. Assim, adveio a Lei nº 14.478/2022 (que incluiu no Código Penal o art. 171-A, tipificando especificamente a fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros).

Essa tipificação mirou diretamente as falsas corretoras e as pirâmides financeiras digitais, estabelecendo penas rigorosas para quem organizasse esquemas de captação de recursos disfarçados de investimentos em blockchain (Sanches Cunha, 2023).

Contudo, apesar desses avanços entre 2021 e 2022, a dogmática penal logo percebeu que essas leis focavam essencialmente na conduta do cabeça da fraude (o estelionatário direto) e na ferramenta utilizada (Greco, 2025).

Ficaram lacunas perigosas referentes à estrutura de apoio dessas quadrilhas, especialmente no que tange ao recrutamento de contas bancárias de terceiros e à velocidade de bloqueio de ativos. A lentidão processual para atingir o patrimônio desviado e a falta de punição específica para as bases logísticas do crime digital tornaram o sistema ainda vulnerável, pavimentando o caminho para a reforma de 2026.

2.2 O Novo Paradigma Punitivo e Processual: Impactos da Lei nº 15.397/2026

A promulgação da Lei nº 15.397/2026 inaugurou uma nova era na repressão aos crimes patrimoniais cibernéticos no Brasil, alterando não apenas as balizas punitivas do Código Penal, mas também o regime de recuperação de ativos.

A principal mudança conceitual promovida por essa lei foi o tratamento da fraude digital não mais como um crime isolado, mas como uma atividade inerente ao crime organizado de alta tecnologia.

O aumento generalizado das penas para fraudes envolvendo o sistema financeiro aberto (Open Finance) e inteligência artificial afastou de vez a incidência dos institutos despenalizadores da Lei nº 9.099/95, garantindo que o fraudador virtual responda ao processo preso ou sob severas medidas cautelares (Prado, 2026, p. 304).

O maior destaque legislativo do novo diploma, contudo, foi o enfrentamento direto ao fenômeno dos "laranjas". Antes da Lei 15.397/2026, indivíduos que emprestavam ou vendiam suas contas bancárias, chaves PIX ou identidades para que estelionatários recebessem o dinheiro das vítimas costumavam ser absolvidos sob a alegação de "erro de tipo" ou ausência de dolo (Bitencourt, 2026).

O novo regramento criou um tipo penal autônomo (ou qualificadora específica, dependendo do enquadramento do caso concreto) para a conduta de "ceder, alugar ou comercializar dados bancários ou credenciais de acesso para fins de ocultação de capital ilícito", impondo o dever de cuidado ao titular da conta (Bitencourt, 2026).

Outra transformação profunda trazida pelo regramento de 2026 ocorreu na esfera processual penal e investigativa. O legislador instituiu o congelamento cautelar de urgência, um mecanismo que permite à autoridade policial, mediante representação imediata ao juiz plantonista e com comunicação simultânea ao Banco Central, efetuar o bloqueio de contas receptoras em tempo real (Lima, 2026).

Antes, o tempo entre o registro do boletim de ocorrência, a representação policial, a oitiva do Ministério Público e a decisão judicial permitia que os valores fossem pulverizados em dezenas de contas em questão de minutos.

Sob o prisma dogmático, a Lei 15.397/2026 também pacificou o entendimento sobre o momento consumativo dos delitos envolvendo engenharia social avançada (como falsas centrais de atendimento) (Pacelli, 2026).

Consagrou-se a tese de que a obtenção da vantagem ilícita se perfectibiliza no exato instante em que os valores saem da esfera de disponibilidade da vítima e ingressam na rede de lavagem dos criminosos, independentemente de quem efetue o saque final (Pacelli, 2026). Isso eliminou antigas teses defensivas que tentavam desclassificar o crime para a modalidade tentada quando os bancos conseguiam estornar parte do valor dias depois.

Em suma, a transição entre o arcabouço normativo de 2021/2022 e as inovações de 2026 evidencia a adaptação forçada do Estado brasileiro diante do avanço da criminalidade hiperconectada.

Se antes o Direito Penal enxergava o estelionato como a lábia de rua transposta para o computador, hoje, após a Lei 15.397/2026, ele compreende a fraude virtual como uma engrenagem complexa, que exige punição severa não

apenas para quem programa o golpe, mas para toda a cadeia de auxílio material, aliada a mecanismos estatais de bloqueio financeiro em velocidade cibernética.

3. NOVOS CONCEITOS E CARACTERÍSTICAS À LUZ DA LEI Nº 15.397/2026

A dogmática penal brasileira tem passado por um processo de ressignificação de seus institutos clássicos para dar conta da complexidade das interações em ambiente cibernético. Com o advento da Lei nº 15.397/2026, o conceito de estelionato digital deixou de ser uma mera extensão do artigo 171 tradicional, consolidando-se como um fenômeno delitivo com características próprias, dotado de hipercomplexidade e transnacionalidade.

A nova legislação reconhece que o "ardil" e o "artifício" no meio digital não se limitam à persuasão verbal, mas envolvem a manipulação de algoritmos, engenharia social automatizada e o uso de inteligência artificial para clonagem de voz e imagem, redefinindo o conceito de fraude no século XXI (Nucci, 2026).

Essas inovações legislativas alteraram substancialmente as características do crime, especialmente no que tange à figura do dolo e à consumação do delito. Diferente do estelionato físico, onde o engodo ocorre muitas vezes de forma interpessoal e direta, a fraude virtual moderna caracteriza-se pela assimetria técnica entre a vítima e o criminoso.

A Lei nº 15.397/2026 passou a prever qualificadoras específicas para quando a fraude envolve a simulação de canais oficiais de instituições financeiras ou o uso de *deepfakes*, entendendo que o poder de lesividade dessas condutas afeta não apenas o patrimônio individual, mas a própria confiabilidade do sistema financeiro digital (Cunha, 2026).

Outra característica fundamental introduzida no arcabouço conceitual do Direito Penal pela norma de 2026 foi a tipificação autônoma e o endurecimento das penas para os chamados "laranjas" (pessoas que cedem ou vendem contas bancárias para o trânsito de valores ilícitos).

Até então, havia grande dificuldade hermenêutica em enquadrar essas figuras, que muitas vezes alegavam desconhecimento da fraude. O novo texto legal estabelece que a cessão, a título oneroso ou gratuito, de credenciais bancárias para ocultação de valores oriundos de fraude eletrônica constitui conduta autônoma

e de alta reprovabilidade, mitigando a impunidade das bases logísticas das quadrilhas virtuais (Estefam, 2026).

Ademais, no que diz respeito ao sujeito passivo (a vítima), a nova legislação ampliou o conceito de vulnerabilidade no ambiente digital. Se antes a vulnerabilidade era atrelada quase exclusivamente à idade (idosos) ou a deficiências cognitivas, a Lei nº 15.397/2026 reconhece a "vulnerabilidade técnica momentânea", que ocorre quando cidadãos comuns são submetidos a ataques de engenharia social de altíssima sofisticação.

Essa mudança de paradigma conceitual é crucial, pois desloca a culpa; muitas vezes atribuída à "desatenção" da vítima pela jurisprudência mais conservadora; para a sofisticação da conduta do agente criminoso, exigindo do aplicador do direito uma visão mais protetiva e menos estigmatizante (Bitencourt, 2026).

Diante disso, entende-se que as características do estelionato digital, sob a égide da referida lei, não demandam apenas a análise da transferência patrimonial indevida, mas a compreensão de todo o iter criminis tecnológico (Senado Federal, 2026).

A consumação, que no passado gerava intensos debates sobre a competência territorial, passa a ser irrefragavelmente vinculada ao domicílio da vítima no momento da fraude, conforme já sinalizava a legislação anterior, mas agora com mecanismos processuais que obrigam as plataformas e provedores de internet a fornecerem os dados de conexão em prazos sumarássimos sob pena de responsabilização solidária (Senado Federal, 2026).

Portanto, em termos conceituais, o estelionato virtual pós-2026 é definido como um crime pluriofensivo. Ele não fere apenas o patrimônio da vítima (bem jurídico tradicional do art. 171), mas atinge diretamente a segurança da informação e a paz social nas relações de consumo e serviços bancários (Nucci, 2026, p. 412). É uma infração penal que exige do Estado-investigador conhecimentos multidisciplinares, unindo o Direito Penal material à Tecnologia da Informação, consolidando a fraude eletrônica como a principal ameaça patrimonial da atualidade.

3.1 Análise Preventiva e Desafios da Persecução Penal nos Crimes Cibernéticos

Apesar dos significativos avanços trazidos pelo recrudescimento penal da Lei nº 15.397/2026, a repressão punitiva, por si só, tem se mostrado insuficiente para frear a escalada criminosa no ambiente virtual. O

Direito Penal atua como a *ultima ratio*, sendo imperativa a adoção de uma análise preventiva multifocal. A prevenção do estelionato digital envolve o que a doutrina moderna chama de "compliance digital anticrime", que obriga instituições financeiras e plataformas de comércio eletrônico a adotarem mecanismos proativos de segurança, como biometria comportamental e bloqueios cautelares baseados em inteligência artificial, antes mesmo que a fraude se consuma (FEBRABAN, 2026).

Nesse aspecto preventivo, a legislação recente passou a exigir que as instituições bancárias não apenas alertem seus clientes, mas comprovem a eficácia de seus sistemas antifraude. Caso haja falha na prestação desse serviço de segurança, a responsabilidade civil objetiva das instituições fortalece a chamada prevenção geral secundária (Silva, 2026).

Ao obrigar os grandes *players* do mercado a investirem massivamente em cibersegurança, o legislador cria um ecossistema digital mais hostil para o criminoso, dificultando a engenharia social que outrora encontrava terreno fértil em aplicativos bancários vulneráveis (Silva, 2026).

Contudo, quando a barreira preventiva falha, a persecução penal enfrenta desafios monumentais. O principal deles é o anonimato e o uso de redes criptografadas e VPNs (Redes Privadas Virtuais) pelos estelionatários, que mascaram seus endereços de IP e dificultam a individualização da autoria (Lima, 2025).

A investigação cibernética no Brasil esbarra na morosidade na quebra de sigilos telemáticos e na cooperação internacional, visto que muitas das estruturas utilizadas para hospedar páginas falsas (phishing) estão localizadas em servidores no exterior, em jurisdições que não possuem acordos de cooperação mútua com o Brasil (Lima, 2025).

A Lei nº 15.397/2026 tentou mitigar esses entraves ao conferir poderes cautelares mais ágeis à autoridade policial para o bloqueio de contas e suspensão de domínios na internet, independentemente de prévia autorização judicial em casos de urgência manifesta e flagrante delito contínuo.

Essa medida, embora elogiada por conferir celeridade à cessação do dano patrimonial, levanta intensos debates sobre os limites do poder de polícia e o direito fundamental ao sigilo de dados, desafiando a jurisprudência a encontrar o ponto de equilíbrio entre a eficiência investigativa e as garantias constitucionais (Távora; Alencar, 2026).

Outro desafio da persecução penal reside na capacitação dos órgãos de segurança pública. O estelionato virtual é um crime de rastros efêmeros; provas digitais podem ser deletadas em frações de segundo.

Para que a materialidade e a autoria sejam comprovadas em juízo, é necessária a adoção da chamada "cadeia de custódia da prova digital" de forma rigorosa, utilizando técnicas forenses de *hash*. A ausência de peritos especializados em delegacias de pequenas e médias cidades brasileiras ainda é um gargalo significativo, que frequentemente resulta na absolvição de fraudadores por falta de provas robustas (Vianna, 2026, p. 188).

Por fim, a análise jurídica e preventiva deságua na necessidade de uma educação digital ostensiva e contínua. O fator humano continua sendo o elo mais fraco da corrente de segurança cibernética (STJ, 2026).

Mesmo com o rigor da Lei 15.397/2026 e das penalidades elevadas, enquanto houver desinformação e ingenuidade digital por parte da população, os criminosos encontrarão atalhos para suas práticas ilícitas. Portanto, a resposta estatal adequada exige a integração entre a inteligência investigativa, o rigor penal equilibrado e a formação de uma cultura de desconfiança e segurança cibernética na sociedade civil.

4. CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo permitiu compreender que o estelionato digital representa uma das principais modalidades criminosas da contemporaneidade, impulsionada pela crescente digitalização das relações sociais, financeiras e comerciais.

A expansão do uso da internet e das plataformas digitais trouxe inúmeros benefícios à sociedade, mas também ampliou as oportunidades para a prática de fraudes cada vez mais sofisticadas, exigindo respostas legislativas e institucionais

compatíveis com essa nova realidade.

Verificou-se que a evolução normativa brasileira foi fundamental para o aprimoramento do combate aos crimes cibernéticos. Nesse contexto, as Leis nº 12.737/2012, nº 12.965/2014, nº 14.155/2021 e nº 14.478/2022 contribuíram significativamente para a construção de um sistema jurídico mais adequado às demandas do ambiente digital.

Todavia, foi a Lei nº 15.397/2026 que promoveu avanços mais expressivos ao endurecer as sanções penais, ampliar o alcance das condutas tipificadas e criar mecanismos processuais voltados à rápida recuperação de ativos provenientes de fraudes eletrônicas.

A pesquisa também evidenciou que as inovações legislativas introduzidas em 2026 fortaleceram a capacidade repressiva do Estado, especialmente ao responsabilizar indivíduos que participam indiretamente das fraudes, como os chamados “laranjas”, e ao possibilitar medidas cautelares mais céleres para o bloqueio de valores desviados.

Tais medidas representam importantes instrumentos para reduzir a sensação de impunidade e aumentar a efetividade da persecução penal nos crimes praticados em ambiente virtual.

Entretanto, constatou-se que o recrudescimento penal, isoladamente, não é suficiente para conter o crescimento das fraudes digitais. Os desafios relacionados ao anonimato dos agentes, à utilização de tecnologias avançadas de ocultação de identidade, à cooperação internacional e à preservação das provas digitais demonstram que o enfrentamento desses delitos exige investimentos permanentes em tecnologia, capacitação profissional e estrutura investigativa especializada.

Por fim, conclui-se que a prevenção continua sendo o mecanismo mais eficaz para a redução dos índices de estelionato digital. A promoção da educação digital, o fortalecimento das políticas de cibersegurança, a conscientização da população sobre os riscos das fraudes eletrônicas e a cooperação entre Estado, instituições financeiras e sociedade civil constituem medidas indispensáveis para a construção de um ambiente virtual mais seguro.

Dessa forma, a efetividade da Lei nº 15.397/2026 dependerá não apenas de sua aplicação rigorosa, mas também da implementação de estratégias preventivas capazes de acompanhar a constante evolução da criminalidade cibernética.

REFERÊNCIAS

AGÊNCIA SENADO. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Senado Notícias, 01 out. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado>. Acesso em: 03 jun. 2026.

ARAS, Vladimir. Os aspectos penais da Lei Brasileira dos Criptoativos. In: **Revista do Ministério Público do Estado do Rio de Janeiro**, n. 88, p. 268–285, abr./jun. 2023. Disponível em: https://www.mprj.mp.br/documents/20184/3978934/Vladimir+Aras_RMP-8810.pdf. Acesso em: 03 jun. 2026.

ATAÍDE, Amanda Albuquerque. **Crimes Virtuais: uma análise da impunidade e dos danos causados às vítimas**. Maceió, 2017. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf Acesso em: 20 Mai 2026

BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade**. Tribunal de Justiça do Distrito Federal e dos Territórios – TJDF. 2022. Disponível em: [https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade#:~:text=A%20lei%2014.155%2F21%20alterou,e%20de%20fraude%20eletr%C3%B4nica%20\(art](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade#:~:text=A%20lei%2014.155%2F21%20alterou,e%20de%20fraude%20eletr%C3%B4nica%20(art). Acesso em: 20 Mai 2026

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial**. 26. ed. São Paulo: Saraiva, 2026.

BRASIL. **Decreto-lei no 2.848, de 7 de dezembro de 1940**. Código Penal. 1940. CARDOSO, Marcos Antônio Frota. O estelionato virtual praticado contra o idoso e os reflexos jurídico-penais. In: **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 5, p. 3385-3398, 2023.

BRASIL. **Lei nº 15.397, de 30 de abril de 2026**. Diário Oficial da União, Brasília, DF, 05 maio 2026. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2026/lei-15397-30-abril-2026-799020-publicacaooriginal-179083-pl.html>. Acesso em: 03 jun. 2026. CAMPELO, Marcelo. **Crimes cibernéticos – Fraude com criptoativos – Bitcoins – Art. 171-A**. Migalhas de Peso, 17 abr. 2023. Disponível em: <https://www.migalhas.com.br/depeso/384922/crimes-ciberneticos--fraude-com-criptoativos--bitcoins--art-171-a>. Acesso em: 03 jun. 2026.

CAPEZ, Fernando. **Curso de direito penal, volume 2: parte especial**. 23. ed. São Paulo: Saraiva, 2023.

CARVALHO, Mariane Moreira. **Histórico do crime de estelionato**. 2023.

Disponível em: <https://www.jusbrasil.com.br/artigos/historico-do-crime-de-estelionato/2332397665> Acesso em: 14 Mai 2026

CARVALHO, Mariane Moreira. **Do crime de estelionato virtual**. 2023:1. Disponível em: <https://www.jusbrasil.com.br/artigos/do-crime-de-estelionato-virtual/2332421047> Acesso em: 14 Mai 2026

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial**. 18. ed. Salvador: Juspodivm, 2026.

DEPUTADOS, Câmara dos. **Projeto de Lei nº 2339 de 2023**. 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2359843> Acesso em: 03 Mai 2026

DUPRET, Cristiane. **O que é crime de estelionato digital e como advogar?** Instituto Direito Penal Brasileiro - IDPB, 2023.

ESTEFAM, André. **Direito penal: parte especial**. 15. ed. São Paulo: Saraiva, 2026.

FEBRABAN – Federação Brasileira de Bancos. **Relatório de Cibersegurança e Prevenção a Fraudes no Sistema Financeiro**. São Paulo: Febraban, 2026. Disponível em: <https://www.febraban.org.br>. Acesso em: 05 jun. 2026.

FEDERAL, Senado. **Projeto de Lei nº 2254 de 2022**. 2022. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/154453> Acesso em: 03 Mai 2026

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume II**. 22. ed. Rio de Janeiro: Impetus, 2025.

LEGALCLOUD. **Lei 15.397/2026: O que mudou no Código Penal e quais os impactos práticos para advogados?** Legalcloud (blog), 05 maio 2026. Disponível em: <https://legalcloud.com.br/lei-15397-codigo-penal-impactos-para-advogados>. Acesso em: 03 jun. 2026.

LIMA, Renato Brasileiro de. **Manual de processo penal: volume único**. 15. ed. Salvador: Juspodivm, 2026.

MASSON, Cleber. **Direito penal: parte especial: arts. 121 a 212**. 17. ed. Rio de Janeiro: Método, 2024.

NASCIMENTO, Henrique. **Sancionada lei que aumenta penas para furto, roubo e golpes virtuais**. Rádio Senado, 05 maio 2026. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2026/05/05/sancionada-lei-que-aumenta-penas-para-furto-roubo-e-golpes-virtuais>. Acesso em: 03 jun. 2026.

OLIVEIRA, Maxwell. **Metodologia científica: um manual para a realização de pesquisas em Administração**. 2011.

OLIVEIRA, Hesrom César. **Cybercrimes**: do estelionato virtual. Faculdade Evangélica de Rubiataba - GO, 2020.

MACHADO, Daniela Regina Gabriel; GROTT, Sérgio. Estelionato virtual. In: **Revista Científica Multidisciplinar do CEAP**, v. 4, n. 1, p. 10-10, 2022.

NUCCI, Guilherme de Souza. **Código penal comentado**. 26. ed. Rio de Janeiro: Forense, 2026.

PACELLI, Eugênio. **Curso de processo penal**. 30. ed. São Paulo: Atlas, 2026.

PINHEIRO, Bruno Victor de Arruda. **As Novas Disposições sobre os Crimes Cibernéticos**: Uma análise acerca da Lei 14.132 de 2021 e Lei 14.155 de 2021. JusBrasil, 2022. Disponível em: <https://www.jusbrasil.com.br/artigos/as-novas-disposicoes-sobre-os-crimes-ciberneticos/1518500029#:~:text=A%20Lei%2014.155%20de%202021,mediante%20fraude%20e%20letr%C3%B4nica%20C%20dentre%20outras> Acesso em: 30 Mai 2026

PRADO, Luiz Regis. **Tratado de direito penal brasileiro**: parte especial. 5. ed. Rio de Janeiro: Forense, 2026.

SANCHES CUNHA, Rogério. **Manual de direito penal: parte especial**. 15. ed. Salvador: Juspodivm, 2023.

SENADO FEDERAL. Agência Senado. **Congresso aprova nova lei que endurece penas para estelionato digital e laranjas**. Brasília, DF, 2026. Disponível em: <https://www12.senado.leg.br/noticias>. Acesso em: 05 jun. 2026.

SILVA, Beatriz Mussalem De Sousa. **Direito penal**: estelionato sob a ótica do dolo específico. Trabalho de Conclusão de Curso - Universidade São Judas Tadeu - São Paulo, 2022.

SILVA, Dion Clésio Pereira; NETO, Geraldo Miranda Pinto. **Crimes Cibernéticos**: ordenamento jurídico frente ao estelionato virtual. 2017.

SILVA, João Pedro; MARINHO, Luiz Eduardo. **O Aumento dos Crimes Virtuais na Pandemia e os Limites da Liberdade de Expressão**. 2022.

SILVA, Natália dos Santos. **O estelionato virtual e a sua estrutura jurídica**. Dissertação de Mestrado. Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP; Brasília, 2023.

SILVA, João Carlos da. A Responsabilidade Civil e Preventiva das Instituições Financeiras na Nova Lei de Fraudes. **Revista Brasileira de Direito Digital**, São Paulo, v. 12, n. 2, p. 45-67, mar. 2026.

STJ – Superior Tribunal de Justiça. **Jurisprudência em Teses: Crimes Cibernéticos e Fraudes Eletrônicas**. Brasília: STJ, 2026. Disponível em: <https://www.stj.jus.br>. Acesso em: 05 jun. 2026.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 21. ed. Salvador: Juspodivm, 2026.

VIANNA, Túlio. **Crimes Informáticos e Cadeia de Custódia Digital**. 4. ed. Belo Horizonte: Del Rey, 2026.

3 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo permitiu compreender que o estelionato digital representa uma das principais modalidades criminosas da contemporaneidade, impulsionada pela crescente digitalização das relações sociais, financeiras e comerciais.

A expansão do uso da internet e das plataformas digitais trouxe inúmeros benefícios à sociedade, mas também ampliou as oportunidades para a prática de fraudes cada vez mais sofisticadas, exigindo respostas legislativas e institucionais compatíveis com essa nova realidade.

Verificou-se que a evolução normativa brasileira foi fundamental para o aprimoramento do combate aos crimes cibernéticos. Nesse contexto, as Leis nº 12.737/2012, nº 12.965/2014, nº 14.155/2021 e nº 14.478/2022 contribuíram significativamente para a construção de um sistema jurídico mais adequado às demandas do ambiente digital.

Todavia, foi a Lei nº 15.397/2026 que promoveu avanços mais expressivos ao endurecer as sanções penais, ampliar o alcance das condutas tipificadas e criar mecanismos processuais voltados à rápida recuperação de ativos provenientes de fraudes eletrônicas.

A pesquisa também evidenciou que as inovações legislativas introduzidas em 2026 fortaleceram a capacidade repressiva do Estado, especialmente ao responsabilizar indivíduos que participam indiretamente das fraudes, como os chamados “laranjas”, e ao possibilitar medidas cautelares mais céleres para o bloqueio de valores desviados.

Tais medidas representam importantes instrumentos para reduzir a sensação de impunidade e aumentar a efetividade da persecução penal nos crimes praticados em ambiente virtual.

Entretanto, constatou-se que o recrudescimento penal, isoladamente, não é suficiente para conter o crescimento das fraudes digitais. Os desafios relacionados ao anonimato dos agentes, à utilização de tecnologias avançadas de ocultação de identidade, à cooperação internacional e à preservação das provas digitais demonstram que o enfrentamento desses delitos exige investimentos permanentes em tecnologia, capacitação profissional e estrutura investigativa especializada.

Por fim, conclui-se que a prevenção continua sendo o mecanismo mais eficaz para a redução dos índices de estelionato digital. A promoção da educação digital, o fortalecimento das políticas de cibersegurança, a conscientização da população sobre os riscos das fraudes eletrônicas e a cooperação entre Estado, instituições financeiras e sociedade civil constituem medidas indispensáveis para a construção de um ambiente virtual mais seguro.

Dessa forma, a efetividade da Lei nº 15.397/2026 dependerá não apenas de sua aplicação rigorosa, mas também da implementação de estratégias preventivas capazes de acompanhar a constante evolução da criminalidade cibernética.

REFERÊNCIAS

AGÊNCIA SENADO. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Senado Notícias, 01 out. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado>. Acesso em: 03 jun. 2026.

ARAS, Vladimir. Os aspectos penais da Lei Brasileira dos Criptoativos. In: **Revista do Ministério Público do Estado do Rio de Janeiro**, n. 88, p. 268–285, abr./jun. 2023. Disponível em: https://www.mprj.mp.br/documents/20184/3978934/Vladimir+Aras_RMP-8810.pdf. Acesso em: 03 jun. 2026.

ATAÍDE, Amanda Albuquerque. **Crimes Virtuais: uma análise da impunidade e dos danos causados às vítimas**. Maceió, 2017. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf Acesso em: 20 Mai 2026

BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade**. Tribunal de Justiça do Distrito Federal e dos Territórios – TJDF. 2022. Disponível em: [https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade#:~:text=A%20lei%2014.155%2F21%20alterou,e%20de%20fraude%20eletr%C3%B4nica%20\(art](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade#:~:text=A%20lei%2014.155%2F21%20alterou,e%20de%20fraude%20eletr%C3%B4nica%20(art). Acesso em: 20 Mai 2026

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial**. 26. ed. São Paulo: Saraiva, 2026.

BRASIL. **Decreto-lei no 2.848, de 7 de dezembro de 1940**. Código Penal. 1940. CARDOSO, Marcos Antônio Frota. O estelionato virtual praticado contra o idoso e os reflexos jurídico-penais. In: **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 5, p. 3385-3398, 2023.

BRASIL. **Lei nº 15.397, de 30 de abril de 2026**. Diário Oficial da União, Brasília, DF, 05 maio 2026. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2026/lei-15397-30-abril-2026-799020-publicacaooriginal-179083-pl.html>. Acesso em: 03 jun. 2026.

CAMPELO, Marcelo. **Crimes cibernéticos – Fraude com criptoativos – Bitcoins – Art. 171-A**. Migalhas de Peso, 17 abr. 2023. Disponível em: <https://www.migalhas.com.br/depeso/384922/crimes-ciberneticos--fraude-com-criptoativos--bitcoins--art-171-a>. Acesso em: 03 jun. 2026.

CAPEZ, Fernando. **Curso de direito penal, volume 2: parte especial**. 23. ed. São Paulo: Saraiva, 2023.

CARVALHO, Mariane Moreira. **Histórico do crime de estelionato**. 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/historico-do-crime-de-estelionato/2332397665> Acesso em: 14 Mai 2026

CARVALHO, Mariane Moreira. **Do crime de estelionato virtual**. 2023:1. Disponível em: <https://www.jusbrasil.com.br/artigos/do-crime-de-estelionato-virtual/2332421047> Acesso em: 14 Mai 2026

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial**. 18. ed. Salvador: Juspodivm, 2026.

DEPUTADOS, Câmara dos. **Projeto de Lei nº 2339 de 2023**. 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2359843> Acesso em: 03 Mai 2026

DUPRET, Cristiane. **O que é crime de estelionato digital e como advogar?** Instituto Direito Penal Brasileiro - IDPB, 2023.

ESTEFAM, André. **Direito penal: parte especial**. 15. ed. São Paulo: Saraiva, 2026.

FEBRABAN – Federação Brasileira de Bancos. **Relatório de Cibersegurança e Prevenção a Fraudes no Sistema Financeiro**. São Paulo: Febraban, 2026. Disponível em: <https://www.febraban.org.br>. Acesso em: 05 jun. 2026.

FEDERAL, Senado. **Projeto de Lei nº 2254 de 2022**. 2022. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/154453> Acesso em: 03 Mai 202

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume II**. 22. ed. Rio de Janeiro: Impetus, 2025.

LEGALCLOUD. **Lei 15.397/2026: O que mudou no Código Penal e quais os impactos práticos para advogados?** Legalcloud (blog), 05 maio 2026. Disponível em: <https://legalcloud.com.br/lei-15397-codigo-penal-impactos-para-advogados>. Acesso em: 03 jun. 2026.

LIMA, Renato Brasileiro de. **Manual de processo penal: volume único**. 15. ed. Salvador: Juspodivm, 2026.

MASSON, Cleber. **Direito penal: parte especial: arts. 121 a 212**. 17. ed. Rio de Janeiro: Método, 2024.

NASCIMENTO, Henrique. **Sancionada lei que aumenta penas para furto, roubo e golpes virtuais**. Rádio Senado, 05 maio 2026. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2026/05/05/sancionada-lei-que-aumenta-penas-para-furto-roubo-e-golpes-virtuais>. Acesso em: 03 jun. 2026.

OLIVEIRA, Maxwell. **Metodologia científica**: um manual para a realização de pesquisas em Administração. 2011.

OLIVEIRA, Hesrom César. **Cybercrimes**: do estelionato virtual. Faculdade Evangélica de Rubiataba - GO, 2020.

MACHADO, Daniela Regina Gabriel; GROTT, Sérgio. Estelionato virtual. In: **Revista Científica Multidisciplinar do CEAP**, v. 4, n. 1, p. 10-10, 2022.

NUCCI, Guilherme de Souza. **Código penal comentado**. 26. ed. Rio de Janeiro: Forense, 2026.

PACELLI, Eugênio. **Curso de processo penal**. 30. ed. São Paulo: Atlas, 2026.

PINHEIRO, Bruno Victor de Arruda. **As Novas Disposições sobre os Crimes Cibernéticos**: Uma análise acerca da Lei 14.132 de 2021 e Lei 14.155 de 2021. JusBrasil, 2022. Disponível em: <https://www.jusbrasil.com.br/artigos/as-novas-disposicoes-sobre-os-crimes-ciberneticos/1518500029#:~:text=A%20Lei%2014.155%20de%202021,mediante%20fraude%20e%20eletr%C3%B4nica%2C%20dentre%20outras> Acesso em: 30 Mai 2026

PRADO, Luiz Regis. **Tratado de direito penal brasileiro**: parte especial. 5. ed. Rio de Janeiro: Forense, 2026.

SANCHES CUNHA, Rogério. **Manual de direito penal: parte especial**. 15. ed. Salvador: Juspodivm, 2023.

SENADO FEDERAL. Agência Senado. **Congresso aprova nova lei que endurece penas para estelionato digital e laranjas**. Brasília, DF, 2026. Disponível em: <https://www12.senado.leg.br/noticias>. Acesso em: 05 jun. 2026.

SILVA, Beatriz Mussalem De Sousa. **Direito penal**: estelionato sob a ótica do dolo específico. Trabalho de Conclusão de Curso - Universidade São Judas Tadeu - São Paulo, 2022.

SILVA, Dion Clésio Pereira; NETO, Geraldo Miranda Pinto. **Crimes Cibernéticos**: ordenamento jurídico frente ao estelionato virtual. 2017.

SILVA, João Pedro; MARINHO, Luiz Eduardo. **O Aumento dos Crimes Virtuais na Pandemia e os Limites da Liberdade de Expressão**. 2022.

SILVA, Natália dos Santos. **O estelionato virtual e a sua estrutura jurídica**. Dissertação de Mestrado. Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP; Brasília, 2023.

SILVA, João Carlos da. A Responsabilidade Civil e Preventiva das Instituições Financeiras na Nova Lei de Fraudes. **Revista Brasileira de Direito Digital**, São Paulo, v. 12, n. 2, p. 45-67, mar. 2026.

STJ – Superior Tribunal de Justiça. **Jurisprudência em Teses: Crimes Cibernéticos e Fraudes Eletrônicas**. Brasília: STJ, 2026. Disponível em: <https://www.stj.jus.br>. Acesso em: 05 jun. 2026.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 21. ed. Salvador: Juspodivm, 2026.

VIANNA, Túlio. **Crimes Informáticos e Cadeia de Custódia Digital**. 4. ed. Belo Horizonte: Del Rey, 2026.