

A INVESTIGAÇÃO CRIMINAL NO ESTELIONATO DIGITAL: CADEIA DE CUSTÓDIA E OS DESAFIOS DA RECUPERAÇÃO DE ATIVOS EM CRIPTOMOEDAS.

Ludmilla Sousa Gouvêa¹

Jorge Florêncio de Oliveira²

Resumo

Este artigo trata da investigação criminal no contexto do estelionato digital, com enfoque na preservação da cadeia de custódia da prova digital e nos desafios relacionados à recuperação de ativos em criptomoedas. O aumento da utilização de meios tecnológicos para a prática de fraudes patrimoniais evidencia a necessidade de adaptação dos instrumentos investigativos tradicionais diante das novas dinâmicas do crime cibernético. O objetivo principal é analisar as dificuldades enfrentadas pelos órgãos de persecução penal na identificação dos autores, na obtenção e preservação das provas produzidas no meio digital, e no rastreamento e na recuperação de valores desviados através de criptoativos. Dessa forma, adotou-se o método dedutivo, mediante pesquisa bibliográfica, legislativa e análise doutrinária, com fundamento na Constituição Federal, no Código Penal, Processo Penal, no Marco Civil da Internet, na Lei Geral de Proteção de Dados e no Pacote Anticrime. Verificou-se que a volatilidade das provas digitais, a utilização de mecanismos de anonimização, a atuação transnacional dos agentes criminosos e a ausência de estruturas técnicas especializadas constituem obstáculos à efetividade investigativa e à recuperação patrimonial das vítimas. Além disso, observou-se que a insuficiência de cooperação internacional e a rápida evolução tecnológica superam a capacidade de resposta estatal. Por fim, conclui-se que, o enfrentamento do estelionato digital demanda constante atualização legislativa, capacitação técnica dos órgãos investigativos, fortalecimento da cooperação entre instituições públicas e privadas e aprimoramento dos mecanismos de rastreamento de ativos digitais, para assegurar maior eficiência na persecução penal e proteção jurídica às vítimas dos crimes cibernéticos.

Palavras-chave: estelionato digital; prova digital; cadeia de custódia; criptomoedas; investigação criminal.

Abstract

This article aims criminal investigation in the context of digital fraud, focusing on the preservation of the chain of custody of digital evidence and the challenges related to the recovery of assets in cryptocurrencies. The increasing use of technological means for committing property fraud highlights the need to adapt traditional investigative instruments to the new dynamics of cybercrime. The main objective is to analyze the difficulties faced by criminal prosecution agencies in identifying offenders, obtaining and preserving digital evidence, and tracing and recovering assets diverted through cryptoassets. Thus, the deductive method was adopted through bibliographic, legislative, and doctrinal research, based on the

¹ Bacharelada em Direito pela Faculdade de Gestão e Inovação – FGI

E-mail: Ludmilla.gouvea@aluno.faculdadefgi.online

² Professor de Direito na FGI

E-mail: Jorge.oliveira@prof.faculdadefgi.online

Federal Constitution, the Brazilian Penal Code and Criminal Procedure Code, the Internet Civil Rights Framework, the General Data Protection Law, and the Anti-Crime Package. It was found that the volatility of digital evidence, the use of anonymization mechanisms, the transnational operation of criminal agents, and the lack of specialized technical structures constitute obstacles to investigative effectiveness and asset recovery. Furthermore, insufficient international cooperation and rapid technological evolution surpass the State's response capacity. Finally, it is concluded that combating digital fraud requires constant legislative updates, technical training of investigative agencies, the strengthening of cooperation between public and private institutions, and the improvement of digital asset tracing mechanisms in order to ensure greater efficiency in criminal prosecution and legal protection for victims of cybercrimes.

Keywords: digital fraud; digital evidence; chain of custody; cryptocurrencies; criminal investigation.

INTRODUÇÃO

Com o avanço da tecnologia e a crescente digitalização das relações sociais e financeiras, vieram grandes facilidades para a população atual. No entanto, é notório o aumento da criminalidade, principalmente do estelionato, crime tipificado no art. 171 do Código Penal. Esse crime consiste em obter vantagem indevida enganando a vítima, ou seja, induzindo-a ao erro. Segundo Nucci (2025), essa conduta se caracteriza pelo lucro ilícito obtido por meio do engano.

À medida que a tecnologia evolui, o estelionato passou a ser amplamente praticado no ambiente digital, assumindo novas formas e estratégias. Nesse contexto, a Lei nº 14.155/2021 trouxe alterações importantes no Código Penal e no Código de Processo Penal, qualificando o estelionato cometido por meio eletrônico e estabelecendo penas mais severas, como forma de resposta estatal ao aumento dessas práticas delituosas.

Recentemente, foi promulgada a Lei nº 15.397/2026, que modificou o Código Penal, principalmente no que tange ao estelionato digital, aumentando as penalidades e trazendo a tipificação do uso de “contas laranjas”, estabelecendo também o fim da ação penal condicionada à representação.

Diferentemente do estelionato tradicional, que geralmente envolve contato direto entre o criminoso e a vítima, o estelionato digital acontece por meio de ferramentas tecnológicas, como aplicativos de mensagens, redes sociais e plataformas online. Isso permite que o criminoso aja de forma remota, muitas vezes escondendo sua identidade. Além disso, é

comum o uso de estratégias sofisticadas de engenharia social³, nas quais o golpista se apresenta como uma instituição confiável, como bancos ou órgãos públicos, explorando a confiança da vítima para obter vantagem ilícita.

Antes, o estelionato utilizava-se principalmente da manipulação da vítima para que ela recebesse uma recompensa. No entanto, com a modernização atual, os autores passaram a se identificar como um órgão público, utilizando-se de gatilhos de autoridade para induzir a vítima ao erro, modalidade em que o estelionatário se vale da credibilidade institucional para obter vantagem ilícita.

Na prática, o estelionato digital se manifesta por meio de diversas modalidades, sendo algumas das mais recorrentes o chamado “golpe do falso funcionário de banco”, no qual o agente entra em contato com a vítima alegando irregularidades em sua conta, induzindo-a a realizar transferências; o “golpe do Pix”, em que há engenharia social para obtenção de códigos de segurança; e ainda fraudes envolvendo falsas plataformas de investimento em criptomoedas, que simulam ambientes legítimos para atrair vítimas.

Essas práticas demonstram que o crime evoluiu não apenas tecnologicamente, mas também estrategicamente, explorando aspectos comportamentais das vítimas, como medo, urgência e confiança em instituições, o que reforça a complexidade do fenômeno.

A partir desse cenário, o Banco Central do Brasil desenvolveu um mecanismo capaz de rastrear o dinheiro proveniente de um Pix fraudulento e bloquear a conta do receptor e de demais contas envolvidas, proporcionando a possibilidade de a vítima reaver o valor. No entanto, apesar do endurecimento das penas, a investigação do estelionato digital ainda enfrenta desafios significativos. Isso ocorre, sobretudo, em razão da rapidez com que os valores são transferidos entre contas bancárias e convertidos em ativos de difícil rastreamento, como as criptomoedas⁴.

Embora exista o mecanismo de rastreamento desenvolvido pelo Banco Central, a efetividade dessas medidas é frequentemente mitigada pela conversão dos ativos ilícitos em criptomoedas. Conforme apontam Campos e Barros (2021), o uso desses ativos permite a movimentação de quantias para o exterior à margem do sistema bancário tradicional,

³ Tradução Livre da Autora: é uma técnica de manipulação psicológica que explora a confiança e erro humano para obtenção de dados sigilosos.

⁴ Tradução Livre da Autora: são moedas digitais descentralizadas que utilizam de criptografia como segurança e operam sem depender de bancos.

utilizando a fragmentação do rastro financeiro na blockchain⁵ para dificultar a recuperação do patrimônio.

Diante dessa complexidade, a investigação criminal exige que a cadeia de custódia da prova digital seja seguida rigorosamente. Segundo Badaró (2021 apud GAIGHER; AMORIM, 2025), esse procedimento é fundamental para garantir a autenticidade e integridade de dados que, pela sua natureza volátil, são suscetíveis de alteração ou eliminação rápida.

Nesse contexto, a investigação criminal enfrenta obstáculos significativos, sobretudo em razão da volatilidade⁶ das provas digitais, da rapidez com que os valores são transferidos entre diferentes contas e da utilização de mecanismos tecnológicos que dificultam o rastreamento financeiro. Além disso, a utilização de contas de terceiros, conhecidas como “laranjas”, e a conversão de valores em criptoativos ampliam a complexidade da apuração, dificultando a identificação dos autores e a efetiva recuperação do patrimônio subtraído.

Outro aspecto relevante diz respeito à necessidade de preservação adequada das evidências digitais, uma vez que tais elementos probatórios podem ser facilmente alterados, excluídos ou corrompidos. Nesse cenário, a cadeia de custódia da prova digital assume papel fundamental para garantir a integridade, autenticidade e confiabilidade das informações coletadas durante a investigação criminal, assegurando que tais elementos possam ser utilizados de forma válida no processo penal.

Diante do exposto, o presente trabalho tem como problema de pesquisa a seguinte indagação: quais são os principais desafios enfrentados na investigação do estelionato digital, especialmente no que se refere à preservação da prova e à recuperação de ativos em criptomoedas?

O objetivo geral deste estudo é analisar os obstáculos existentes na persecução penal do estelionato digital, com ênfase na cadeia de custódia da prova digital e nas dificuldades relacionadas à recuperação de ativos em criptoativos. Como objetivos específicos, busca-se: examinar as características do estelionato digital e as alterações promovidas pela Lei nº 14.155/2021 e pela nova Lei nº 15.397/2026; compreender a importância da cadeia de custódia na preservação da prova digital; e identificar os principais entraves na recuperação de valores desviados por meio de criptomoedas.

⁵ Tradução Livre da Autora: um banco de dados digital descentralizado que registra transações de forma segura e imutável, sem a necessidade de banco ou governo.

⁶ Tradução Livre da Autora: algo instável, que muda ou desaparece com facilidade.

Por fim, justifica-se a relevância do presente estudo diante do crescimento exponencial dos crimes digitais e da necessidade de aprimoramento dos mecanismos jurídicos e investigativos, a fim de garantir maior efetividade na responsabilização dos agentes e na recuperação dos prejuízos suportados pelas vítimas.

METODOLOGIA

A presente pesquisa possui natureza qualitativa e caráter bibliográfico, sendo desenvolvida por meio do método dedutivo, mediante a análise doutrinária, legislativa e jurisprudencial acerca da investigação criminal no contexto do estelionato digital, com enfoque na cadeia de custódia da prova digital e na recuperação de ativos em criptomoedas.

Para a elaboração deste estudo, foram utilizados dispositivos da Constituição Federal, do Código Penal, do Código de Processo Penal, do Marco Civil da Internet, da Lei Geral de Proteção de Dados, da Lei nº 14.155/2021 e da legislação relacionada aos criptoativos, além de obras doutrinárias e artigos científicos pertinentes ao tema.

Ademais, o presente trabalho busca compreender os principais desafios enfrentados pelos órgãos de persecução penal diante da volatilidade das provas digitais, da descentralização dos ativos virtuais e das limitações técnicas e jurídicas existentes na investigação dos crimes cibernéticos.

1. DISCUSSÃO E DESENVOLVIMENTO

1.1 Estelionato Digital: Evolução e Características

O crime de estelionato, previsto no art.171 do Código Penal, está associado à obtenção de vantagens ilícitas mediante a indução ou a manutenção da vítima em erro, por meio de artifícios fraudulentos. Trata-se de um crime que se estrutura na manipulação da confiança da vítima, explorando principalmente a sua boa-fé para que sejam obtidos benefícios econômicos indevidos. Nas palavras de Guilherme de Souza Nucci (2025), o estelionato caracteriza-se pela obtenção de lucro ilícito a partir do engano, sendo a colaboração da vítima um elemento essencial para a consumação do delito.

Com a utilização das tecnologias da informação e a digitalização das relações sociais e econômicas, essa dinâmica clássica de estelionato passou por uma grande transformação. Isso porque, o ambiente digital não apenas ampliou seu alcance, mas também induziu novas

formas de execução, tornando-as mais sofisticadas e de difícil rastreamento. Diante disso, o estelionato deixou de depender exclusivamente do contato direto entre o autor e a vítima e passou a ocorrer por meio de plataformas digitais, como redes sociais e aplicativos de comunicação, possibilitando a atuação remota do autor e a manipulação de vítimas em larga escala.

Essa mudança representa uma verdadeira evolução estrutural da prática delituosa. Observa-se, além da ampliação do alcance, é possível observar também a utilização de técnicas de engenharia social, nas quais o agente se utiliza de elementos psicológicos, como a urgência, o medo e a autoridade, na intenção de induzir a vítima ao erro. Com isso a fraude passa a ser constituída não apenas por narrativas enganosas, mas também pelo uso de tecnologias, como páginas falsas, perfis clonados e sistemas que reproduzem um ambiente institucional verdadeiro.

Diante desse novo estelionato, o legislador brasileiro buscou atualizar o ordenamento jurídico por meio da Lei n.º 14.155/2021, introduzindo modificações extremamente relevantes no tratamento penal do estelionato praticado por meio digital. A norma promoveu um aumento das penas e reconheceu a gravidade das fraudes digitais, além de trazer também alterações processuais voltadas à facilitação da persecução penal, como a definição da competência no domicílio da vítima. Posteriormente, foi sancionada a Lei. nº 15.397/2026, que trouxe penas ainda maiores para o crime de estelionato digital, estabelecendo um marco muito importante, a tipificação de “contas laranjas”. Contudo, a legislação, embora avance na repressão penal, não enfrenta o problema principal, que reside na dificuldade probatória e na demora do Judiciário em atender à constante demanda. Principalmente, com a utilização de criptoativos, o dinheiro proveniente de um estelionato se torna algo irrastrável e de difícil acesso.

Com isso, torna-se imprescindível compreender o estelionato digital não apenas sob a perspectiva da sua tipificação penal, mas também a partir de suas implicações práticas na investigação criminal. Pode-se perceber que a complexidade do ambiente virtual, aliada ao uso de tecnologias que favorecem o anonimato e a dispersão de provas, impõe grandes desafios ao Direito Penal e Processual Penal, exigindo a adoção de mecanismos mais sofisticados de apuração, controle e preservação das provas digitais.

Constata-se também que o uso de criptomoedas traz aos crimes de estelionato uma grande vantagem, como se pode notar em diversos casos reais e bilionários de golpes que utilizam a moeda virtual como uma ferramenta para obter vantagens ilícitas. Devido ao

aumento desses crimes, foi sancionada a Lei nº 14.478/2022, conhecida como Marco Legal dos Criptoativos, responsável por estabelecer diretrizes para a prestação de serviços relacionados a ativos virtuais no Brasil.

1.1.1 Conceito de Estelionato

O crime de estelionato é um crime contra o patrimônio, previsto no art. 171 do Código Penal, e consiste na obtenção de vantagem ilícita, em prejuízo alheio, mediante fraude, por meio da indução ou manutenção da vítima em erro. Trata-se de delito patrimonial em que a colaboração da vítima, ainda que inconsciente, é elemento essencial para a sua consumação.

Para uma melhor compreensão do crime, Miguel Reale Júnior aponta que a configuração típica do delito pode ser dividida em três etapas. A primeira consiste no emprego doloso da fraude pelo agente, com a finalidade de induzir ou manter a vítima em erro, visando à obtenção de vantagem indevida. A segunda etapa refere-se ao ato de disposição patrimonial realizado pela vítima em favor do autor, influenciada pelo erro a que foi conduzida. Por fim, a terceira etapa corresponde à efetiva obtenção da vantagem indevida pelo agente. (REALE JÚNIOR, 2023, p. 610).

Conforme Guilherme de Souza Nucci, a classificação do crime de estelionato se baseia em “Obter vantagem indevida induzindo ou mantendo alguém em erro. Significa conseguir um benefício ou um lucro ilícito em razão do engano provocado na vítima. Esta colabora com o agente sem perceber que está se despojando de seus pertences”. (NUCCI, 2025, p. 864).

Ainda segundo o autor, o estelionato pode ser compreendido como um “crime artístico”, na medida em que o agente constrói uma narrativa persuasiva, utilizando-se de elementos estratégicos para convencer a vítima, de forma semelhante a uma encenação. A diferença, contudo, reside na finalidade da conduta, uma vez que, ao invés de entretenimento, o agente busca a obtenção de vantagem ilícita (NUCCI, 2025, p. 393).

A origem do termo “estelionato” remonta à palavra *stellio* vinda do grego, que designa um lagarto com a capacidade de mudar de cor para enganar as suas presas, analogia que ilustra perfeitamente a conduta fraudulenta praticada pelo agente (OLIVEIRA, 2024). No plano jurídico, o delito consiste na obtenção de vantagens ilícitas mediante a indução da vítima ao erro, conforme previsto no art. 171 do Código Penal. O estelionato difere-se do crime de furto pelo fato de que a vítima entrega seu bem voluntariamente ao autor, acreditando na falsa realidade criada por ele. Também difere-se do roubo, no qual ocorre grave ameaça ou violência.

Com o advento da Lei nº 13.964/2019 (Pacote Anticrime), a ação penal referente ao crime de estelionato passou, como regra, a ser pública condicionada à representação da vítima, exigindo-se manifestação de vontade do ofendido para o início da persecução penal. Nessa hipótese, o prazo para representação era de seis meses, contado do dia em que a vítima tomava conhecimento da autoria do delito, nos termos do art. 38 do Código de Processo Penal. Assim, nos casos em que a identidade do autor permanecesse desconhecida, o prazo decadencial sequer se iniciava. Contudo, esse regime jurídico foi posteriormente alterado pela Lei nº 15.397/2026, que revogou o § 5º do art. 171 do Código Penal, restabelecendo a natureza de ação penal para o crime de estelionato e criminalizando os “laranjas”.

1.1.2 Evolução Para o Meio Digital

A doutrina reconhece que a migração do estelionato para o ambiente digital não altera sua estrutura típica, mas amplia significativamente seus meios de execução e potencial lesivo. Nesse tipo de delito, o agente não utiliza violência ou grave ameaça, mas recorre a artifícios e estratégias fraudulentas para organizar, gerir, ofertar ou intermediar operações que envolvem criptomoedas, valores mobiliários ou outros ativos financeiros digitais, com a finalidade de obter vantagem ilícita em prejuízo da vítima. Nucci explica que o criminoso, ao manipular a percepção da vítima, cria um cenário enganoso que simula segurança e legitimidade, convencendo a vítima a investir, transferir valores ou aderir a operações inexistentes.

No entanto, a transposição desse crime para o ambiente digital operou uma metamorfose na execução do delito. Isso porque, se no estelionato tradicional o cenário era físico, como o "bilhete premiado", ou "falso funcionário de banco" presencial, no estelionato digital, o palco é substituído por interfaces de usuários, algoritmos de persuasão e técnicas de engenharia social. A "fala decorada" de Nucci agora se traduz em roteiros de *phishing*⁷ via WhatsApp ou sites espelho que replicam com perfeição corretoras de criptomoedas legítimas.

Diferentemente do estelionato tradicional, o estelionato digital apresenta características próprias, como a ausência de contato físico entre o autor e a vítima, e a utilização de meios tecnológicos para a prática do delito e a maior dificuldade de rastreamento da autoria, devido ao anonimato, e à utilização de criptomoedas para dificultar o rastreamento. Enquanto no estelionato tradicional o autor precisa estar em contato com a vítima, no estelionato digital o autor, na maioria das vezes, nem chega a ver a vítima.

⁷ Tradução Livre da Autora: é um golpe digital, onde golpistas se passam por instituição bancária, órgão público ou pessoas de confiança para enganar a vítima, através de mensagens falsas

No que se refere especificamente aos criptoativos, estes podem ser compreendidos como representações digitais de valor que operam em redes descentralizadas, baseadas em criptografia e tecnologia *blockchain*. Sua relevância no contexto do estelionato digital decorre não apenas de sua popularização como meio de investimento, mas também, de sua utilização como instrumento de ocultação de valores ilícitos. Isso ocorre porque, ao serem convertidos em criptomoedas, os ativos financeiros passam a circular fora do sistema bancário tradicional, dificultando o rastreamento, a identificação dos beneficiários finais e a recuperação dos valores, o que impacta diretamente a efetividade da persecução penal.

O estelionato digital, portanto, não representa apenas uma transposição do crime para o ambiente virtual, mas uma verdadeira evolução estrutural da conduta criminosa. Enquanto no modelo tradicional o agente dependia de contato direto com a vítima, no ambiente digital há uma ampliação significativa do alcance da fraude, permitindo que um único indivíduo atinja simultaneamente diversas vítimas em diferentes localidades. Além disso, a escalabilidade do crime digital, aliada ao uso de ferramentas automatizadas, como disparos em massa de mensagens fraudulentas, potencializa significativamente os danos causados.

Outro aspecto relevante refere-se à assimetria informacional entre autor e vítima. No ambiente digital, o criminoso se vale não apenas da manipulação psicológica, mas também do desconhecimento técnico da vítima, explorando vulnerabilidades relacionadas à segurança da informação, o que torna o delito mais sofisticado e de difícil prevenção.

Vale destacar também que o estelionato digital difere-se do furto mediante fraude eletrônica. Isso porque, no furto digital, o autor utiliza de algum software malicioso sem o consentimento da vítima, ou seja, a vítima não sabe que o dinheiro dela está saindo da conta bancária. Já no estelionato digital, a vítima é enganada e acaba aceitando, ela contribui para que o valor saia de sua conta, ou ela mesma realiza a transferência bancária, ou mesmo em cripto para um site duvidoso que ela acreditava se tratar de um site de criptomoedas confiável.

Diante do exposto, verifica-se que a evolução do estelionato para o ambiente digital não apenas amplia seu alcance, mas também impõe desafios significativos à persecução penal, especialmente no que se refere à identificação dos autores, à produção de provas e à recuperação dos valores subtraídos. Tal cenário evidencia a necessidade de constante atualização dos mecanismos investigativos e do próprio ordenamento jurídico, a fim de garantir uma resposta estatal eficaz diante da complexidade dos crimes digitais.

1.1.3 Lei 14.155/2021

A promulgação da Lei nº 14.155/2021 trouxe impactos significativos, principalmente no que se refere aos crimes cibernéticos, e promoveu alterações no Código Penal brasileiro e no Código de Processo Penal, com a finalidade de adequar a legislação às novas modalidades de crimes praticados em ambientes virtuais, promovendo uma reestruturação na forma como o ordenamento jurídico brasileiro enfrenta os crimes cibernéticos.

Além disso, a legislação passou a reconhecer expressamente a vulnerabilidade do ambiente digital, no qual a confiança do usuário é constantemente explorada por agentes mal-intencionados. Tal reconhecimento demonstra uma tentativa do legislador de adaptar o Direito Penal às novas dinâmicas sociais, embora ainda existam lacunas no que se refere à efetividade da persecução penal.

Essa lei surgiu como uma forma de endurecer as penas dos crimes que são praticados de forma online e preencher as lacunas existentes na legislação anterior. Com isso, o estelionato comum ganhou uma nova modalidade denominada estelionato digital, com penas superiores à sua modalidade comum. Essa alteração resultou na inclusão dos §2º-A e §2º-B, ao artigo 171 do Código Penal, tipificando uma nova modalidade de fraude em seu conteúdo.

Além disso, a Lei nº 14.155/2021 alterou no Código de Processo Penal, especificamente em seu art. 70, §4º, uma inovação de grande importância para as vítimas de estelionato digital. O local para processar e julgar os crimes de estelionato digital passou a ser o local de residência da vítima, e não mais onde o crime foi consumado (CAVALCANTE, 2025).

Um dos maiores entraves para a persecução penal do estelionato digital era a definição da competência. Antes da reforma de 2021, a regra geral determinava que o processo ocorresse no local da consumação do crime, geralmente onde o réu recebia o proveito do crime. Em um golpe envolvendo criptoativos, em que o destino é uma carteira digital fria ou uma *wallet*⁸ no exterior, a vítima ficava processualmente desamparada. A Lei 14.155/2021 corrigiu essa distorção ao alterar o Código de Processo Penal:

Art. 70, § 4º: Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

⁸ Tradução Livre da autora: refere-se a fraudes eletrônicas em que criminosos aplicam golpes na internet para obter vantagens financeiras ilícitas acessando, clonando ou vinculando cartões de vítimas a aplicativos de pagamento e carteiras de criptomoedas.

Essa mudança desloca o eixo da justiça para o lado mais fraco da relação. E, ao permitir que a vítima acompanhe o processo em sua própria comarca, o Estado facilita a colheita de provas e desencoraja a impunidade que o anonimato digital garantia.

Importante destacar que o aumento de pena, por si só, não se mostra suficiente para conter o avanço dessas práticas delituosas, uma vez que o principal desafio não reside apenas na punição, mas na identificação dos autores e na recuperação dos valores subtraídos. Dessa forma, a Lei nº 14.155/2021 apresenta caráter mais simbólico do que efetivamente resolutivo, ao passo que endurece a resposta penal sem necessariamente oferecer mecanismos eficazes de investigação.

Embora a Lei nº 14.155/2021 represente um avanço legislativo relevante, ao agravar as penas e reconhecer a gravidade do estelionato digital, sua eficácia prática é limitada, uma vez que não resolve os principais entraves da persecução penal, especialmente no que se refere à identificação dos autores e à recuperação dos valores subtraídos.

No entanto, mesmo com o endurecimento das penas, a utilização de criptoativos na prática de golpes tem se tornado uma estratégia para se esquivar dos meios de segurança, e assim dificultar a recuperação dos valores provenientes do crime, conforme explicam Campos e Barros:

A natureza descentralizada e anônima do Bitcoin e outras criptomoedas tornam-nas um facilitador de atividades ilícitas, como a “lavagem” de dinheiro, ocultação de bens, financiamentos ao terrorismo e a compra de produtos ilegais. Isso ocorre porque as transações em criptomoedas não estão sujeitas às mesmas regulamentações que as transações em moedas fiduciárias, o que permite que indivíduos e organizações realizem transações sem deixar rastros. (2023, p.71).

Nesse sentido, torna-se imprescindível a atuação conjunta de instrumentos tecnológicos, cooperação internacional e aprimoramento dos mecanismos de investigação, sob pena de perpetuação da impunidade e aumento dos prejuízos suportados pelas vítimas.

A complexidade da persecução penal em crimes dessa natureza também é evidenciada pela jurisprudência recente do Superior Tribunal de Justiça. Em julgamento envolvendo investigação de suposta pirâmide financeira com indícios de estelionato e crimes contra a economia popular, a Corte reconheceu a necessidade de manutenção de competências distintas, considerando a multiplicidade de vítimas, a diversidade de condutas e a existência de investigações paralelas em diferentes localidades. O Tribunal destacou que a definição da competência, nesses casos, deve observar critérios como a prevenção, a gravidade dos delitos e a conexão entre os fatos (STJ, AgRg nos EDcl no CC n. 211.201/SP, 2025). Esse

entendimento demonstra que, em crimes econômicos complexos, especialmente aqueles praticados em ambiente digital, a fragmentação das condutas e a dispersão territorial dificultam a atuação estatal e reforçam os desafios da investigação criminal.

1.1.4 A Lei nº 15.397/2026 e as Novas Diretrizes de Persecução Penal do Crime de Estelionato

O crescimento dos casos de estelionato digital levou os legisladores a realizarem novas alterações no Código Penal e no Código de Processo Penal, sendo realizada a promulgação da Lei nº 15.397, de 2026, que promoveu modificações significativas, especialmente no artigo 171, buscando conferir maior efetividade à repressão penal e adequar a legislação às novas formas de criminalidade.

Uma das principais inovações introduzidas pela referida norma é a revogação do § 5º do artigo 171 do Código Penal, dispositivo incluído pela Lei nº 13.964/2019 (Pacote Anticrime). Com a alteração promovida em 2019, a ação penal relativa ao crime de estelionato passou a ser pública condicionada à representação da vítima, exigindo a manifestação expressa do ofendido para o início da persecução penal. Essa medida foi justificada, pela natureza patrimonial do delito e pela necessidade de prestigiar a autonomia da vontade da vítima.

Porém, a experiência prática demonstrou que a exigência de representação, em muitos casos, dificultava a atuação estatal no combate às fraudes, especialmente aquelas praticadas em ambiente virtual, caracterizadas pela elevada quantidade de vítimas, pela complexidade investigativa e pela atuação organizada dos agentes criminosos. Diante desse cenário, a Lei nº 15.397/2026 restabeleceu a natureza de ação penal pública incondicionada para o crime de estelionato, dispensando a representação da vítima como condição para o oferecimento da denúncia pelo Ministério Público.

Essa alteração legislativa possui um relevante impacto na persecução penal, uma vez que permite o prosseguimento das investigações e da ação penal independentemente da manifestação de vontade do ofendido. Dessa forma, o Estado retoma integralmente a titularidade da persecução penal nos casos de estelionato, ampliando os instrumentos de enfrentamento às fraudes patrimoniais e reduzindo obstáculos procedimentais que, em determinadas situações, favoreciam a impunidade.

Além da modificação referente à ação penal, a Lei nº 15.397/2026 também reforçou o combate às fraudes eletrônicas ao prever mecanismos voltados à responsabilização daqueles

que colaboram com a prática criminosa por meio da cessão de contas bancárias destinadas à movimentação de valores obtidos ilicitamente, conhecidas popularmente como "contas laranja". Essas estruturas são frequentemente utilizadas para ocultar a origem dos recursos provenientes de golpes e dificultar a identificação dos verdadeiros autores do delito.

A nova legislação representa, portanto, uma resposta estatal ao aumento dos crimes patrimoniais praticados por intermédio de tecnologias digitais, refletindo a necessidade de constante atualização do ordenamento jurídico diante das transformações sociais e tecnológicas. Ao tornar a ação penal do estelionato pública incondicionada e ampliar os mecanismos de responsabilização dos envolvidos nas fraudes, o legislador buscou fortalecer a proteção do patrimônio das vítimas e aumentar a eficiência da atuação dos órgãos de persecução criminal.

Observa-se que as alterações promovidas pela Lei nº 15.397/2026 evidenciam uma mudança de política criminal em relação ao tratamento do estelionato. Se a reforma introduzida pelo Pacote Anticrime privilegiava a participação da vítima na deflagração da ação penal, a nova legislação prioriza a tutela do interesse público na repressão das fraudes patrimoniais, especialmente diante do crescimento exponencial dos golpes eletrônicos e dos prejuízos econômicos e sociais deles decorrentes.

1.2 A Prova Digital e a Cadeia de Custódia

Com a crescente incidência do estelionato digital, novos desafios são impostos à persecução penal, principalmente no que tange à produção e preservação de provas, pois, diferentemente dos crimes tradicionais nos quais os elementos probatórios são predominantemente físicos, os delitos praticados em ambiente virtual dependem, em grande medida, de evidências digitais, como registros eletrônicos, logs de acesso e comunicações realizadas por meio de aplicativos.

Conforme apresentado, verifica-se que a simples existência da prova digital não se torna suficiente para garantir a validade do processo penal, sendo imprescindível a utilização de procedimentos técnicos e jurídicos que assegurem a sua integridade e autenticidade. Diante desse contexto, destaca-se a importância da cadeia de custódia, prevista no artigo 158-A do Código de Processo Penal, como um mecanismo destinado a documentar e preservar o histórico do vestígio desde a sua coleta até a apresentação em juízo. A cadeia de custódia assume papel ainda mais relevante no âmbito dos crimes digitais, em que os elementos probatórios são altamente voláteis e suscetíveis a alterações. Além disso, a correta

preservação das provas digitais não apenas assegura a admissibilidade processual, mas também viabiliza a adoção de medidas investigativas eficazes, especialmente no que se refere ao rastreamento e à eventual recuperação de ativos decorrentes de práticas ilícitas.

1.2.1 Conceito de prova digital

O avanço da tecnologia da informação trouxe diversas transformações na persecução penal, especialmente no que se refere à produção probatória. Nesse contexto, surge a chamada prova digital, que pode ser compreendida como dados em forma digital constantes de um suporte eletrônico ou transmitidos em rede de comunicações, os quais contêm a representação de fatos ou ideias relevantes para o processo (VAZ, 2012).

A autora, em sua tese, define que não é o aparelho eletrônico que constitui uma prova, mas sim os dados contidos nele ou que foram transmitidos por ele. Portanto, o que caracteriza a prova digital é justamente o fato de ser uma informação produzida ou registrada por meios tecnológicos, capaz de ajudar a esclarecer o que ocorreu em determinada situação.

Conforme apresenta a autora, a prova digital possui algumas características, sendo elas a imaterialidade e desprendimento do suporte físico originário, a volatilidade, suscetibilidade de clonagem e a necessidade de intermediação de equipamento para ser acessada (VAZ, 2012, p.67). A imaterialidade diz que a prova digital não é um celular ou HD, mas o dado contido neles, não é um objeto tocável, o que traz outras características, a volatilidade e a fragilidade, visto que, por serem dados eletrônicos, eles podem facilmente ser alterados, apagados ou comprimidos, o que exige uma coleta imediata e segura. Diferentemente de um documento em papel, a prova digital precisa de um dispositivo ou software para se tornar inteligível.

A jurisprudência do Superior Tribunal de Justiça reforça a necessidade de rigor na análise da prova digital, especialmente quanto à observância da cadeia de custódia. A Corte destacou que a prova digital possui características de volatilidade e modificabilidade, exigindo a adoção de procedimentos técnicos capazes de assegurar sua integridade e autenticidade. No caso, discutia-se a validade de elementos como capturas de tela de conversas de WhatsApp, obtidas sem a devida perícia técnica, o que levantou dúvidas quanto à fidedignidade dos dados. O Tribunal entendeu que, havendo incerteza sobre a preservação dos vestígios digitais, impõe-se a realização de exame pericial para garantir a confiabilidade da prova e o efetivo exercício do contraditório (STJ, AgRg no HC 1.014.212/ES, Rel. Min. Carlos Pires Brandão, j. 10 fev. 2026).

O entendimento evidencia que, no contexto das provas digitais, a simples existência do dado não é suficiente para sua utilização no processo penal, sendo imprescindível a demonstração de sua integridade e rastreabilidade. Tal posicionamento reforça a importância da cadeia de custódia como instrumento essencial para a validação da prova no ambiente digital.

1.2.2 Cadeia de Custódia no CPP

No processo penal, a prova constitui o alicerce da decisão judicial, tornando indispensável a adoção de mecanismos que assegurem sua integridade desde a coleta até sua apresentação em juízo. Nesse cenário, a cadeia de custódia, prevista nos arts. 158-A a 158-F do Código de Processo Penal, surge como instrumento essencial para garantir a confiabilidade da prova (MENEZES; BORRI; SOARES, 2018). Portanto, é essencial entender como funciona a cadeia de custódia e quais são seus requisitos para que não ocorra a anulação da prova colhida, tendo em vista que, ao se tratar de provas digitais, a cadeia de custódia toma um papel muito importante. Como apresentado anteriormente, a prova digital possui grande volatilidade, podendo ser facilmente alterada.

Nesse sentido, a cadeia de custódia pode ser compreendida como o conjunto de procedimentos destinados a preservar a integridade da prova, sendo definida como “uma sucessão de eventos concatenados, em que cada um proporciona a viabilidade ao desenvolvimento do seguinte, de forma a proteger a integridade de um vestígio do local de crime ao seu reconhecimento como prova” (MENEZES; BORRI; SOARES, 2018, p. 281). A finalidade da cadeia de custódia é assegurar a autenticidade, integridade e rastreabilidade da prova, garantindo sua idoneidade para utilização no processo penal.

A cadeia de custódia foi adicionada ao Código de Processo Penal, através da Lei nº 13.964/2019, o chamado “Pacote Anticrime” que inseriu os referidos artigos supracitados, tornando crucial o registro documental de todo o manuseio da prova, evitando a sua nulidade. Ademais, o Art. 158-A, §3º, estabelece as fases da cadeia de custódia, que compreendem o reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e, por fim, o descarte. Cada uma dessas etapas desempenha papel fundamental na preservação da confiabilidade do vestígio.

Entre essas etapas, destaca-se a coleta, que é o momento em que o vestígio é efetivamente retirado do local do crime. Nessa fase, é exigido o uso de técnicas adequadas

para evitar contaminações. Também merece atenção o acondicionamento, pois é ele que garante a preservação do material até a realização da análise pericial.

A observância rigorosa da cadeia de custódia não se limita apenas a um formalismo procedimental, mas constitui garantia essencial à validade da prova, especialmente em um cenário em que elementos digitais podem facilmente ser manipulados e comprometer a efetividade da persecução penal.

1.2.3 A Aplicação da Cadeia de Custódia nos Crimes Digitais

Conforme destacam Barros e Oliveira (2025), os vestígios digitais, por serem imateriais, são mais suscetíveis a interferências, o que impõe a adoção de procedimentos mais rigorosos para garantir a integridade. Diante disso, a aplicação da cadeia de custódia nos crimes digitais apresenta desafios específicos decorrentes da própria natureza imaterial das provas. Diferentemente das evidências em crimes físicos, realizados fora dos meios digitais, as provas digitais são marcadas pela volatilidade e pela facilidade de alteração, o que compromete diretamente a confiabilidade do elemento probatório e dificulta sua utilização no processo penal, especialmente quando não há mecanismos adequados de preservação.

A preservação da integridade da prova digital demanda a utilização de mecanismos técnicos que assegurem a autenticidade, como, por exemplo, a geração de códigos *hash*⁹, que funcionam como identificadores únicos dos arquivos digitais. Os códigos *hash* consistem em um processo matemático que transforma dados de qualquer tamanho em sequências alfanuméricas, geralmente utilizadas para verificar a integridade, arquivar, armazenar senhas ou assinar documentos digitais. A utilização do *hash* na cadeia de custódia, permite assegurar que o conteúdo da prova permaneceu inalterado ao longo do tempo, o que confere maior confiabilidade ao elemento probatório.

Registros de *logs*¹⁰ de acesso, metadados e dados armazenados em ambientes virtuais exigem técnicas mais apropriadas de coleta e de armazenamento, uma vez que a manipulação indevida pode comprometer significativamente a confiabilidade da prova. Barros e Oliveira (2025), ressaltam que a ausência de regulamentação específica para a cadeia de custódia digital no ordenamento jurídico brasileiro contribui para a insegurança na utilização desses elementos no processo penal. Apesar de o Código de Processo Penal disciplinar a cadeia de

⁹ Tradução Livre da autora: é uma sequência única de letras e números gerada por um algoritmo matemático. Funciona como uma impressão digital para arquivos, senhas ou textos.

¹⁰ Tradução Livre da Autora: registros eletrônicos automáticos que armazenam informações sobre atividades realizadas em sistemas digitais, como acessos, horários, endereços IP e ações executadas pelos usuários.

custódia nos artigos 158-A e 158-F, esses dispositivos foram estruturados, com foco em vestígios físicos, não contemplando de forma específica as particularidades das provas digitais, o que evidencia uma lacuna normativa.

Vale pontuar, que a coleta de provas digitais necessita de extrema cautela, e portanto, quando um agente se depara com um vestígio digital, é essencial que ele o colete de imediato, sendo necessário coletar diversos dados para apresentar ao judiciário e assegurar o contraditório e a ampla defesa, devendo principalmente afastar qualquer possibilidade de contaminação da prova. A doutrina destaca que a atividade pericial em ambientes digitais deve observar alguns métodos próprios da forense computacional, garantindo a preservação do conteúdo digital, por meio de técnicas como o espelhamento de dados (LIMA, 2020).

A forense computacional trata-se de um conjunto de técnicas criadas com o objetivo de combater os crimes digitais, adotando análises e métodos para detectar, coletar, preservar e analisar evidências e identificar cybercriminosos¹¹. Ela desempenha um papel fundamental na produção de prova, tendo em vista que busca reconstruir os fatos ocorridos no ambiente digital e garantir que as evidências obtidas não sejam comprometidas ou mesmo perdidas durante o processo investigativo (FRANCK; FERREIRA, 2023). Durante todo esse processo, deve ser rigorosamente observada a cadeia de custódia para garantir a autenticidade da prova e evitar questionamentos quanto à sua validade no processo penal.

1.2.4 Consequências da Quebra da Cadeia de Custódia

Como já citado acima, a cadeia de custódia, quando se trata de ativos digitais, deve ser seguida com extrema cautela para a manutenção da idoneidade da prova que percorre o caminho desde a coleta até a análise pelo magistrado, e qualquer interferência indevida ou falha no registro cronológico desde o trâmite pode, em tese, comprometer a efetividade do elemento probatório, podendo resultar na imprestabilidade para fins de convicção judicial.

A jurisprudência tem mitigado a rigidez formal em prol da busca pela verdade real e do princípio da instrumentalidade das formas. Conforme o entendimento do STJ, o reconhecimento de nulidade decorrente da alegada quebra da cadeia de custódia exige a demonstração do prejuízo efetivo à defesa, em observância ao princípio *pas de nullité sans grief*, disposto no art. 563 do Código de Processo Penal.

¹¹ Tradução Livre da Autora: indivíduos ou grupos que praticam crimes por meio de tecnologias digitais, redes de computadores ou sistemas informatizados.

O autor aponta que, apesar da minuciosidade do legislador em todas as etapas da cadeia de custódia, houve certa destreza nas consequências da violação da cadeia de custódia, acarretando o surgimento de algumas vertentes doutrinárias (BONFIM, 2025). De fato, existe uma ausência de normatividade quanto às consequências da quebra da cadeia de custódia, portanto, doutrinas e jurisprudências preenchem de certa forma o vácuo legislativo.

Uma das consequências da quebra da cadeia de custódia é a inadmissibilidade da prova, essa consequência é abordada pelo doutrinador Aury Lopes Junior:

“Preferimos pensar a quebra da cadeia de custódia como temática diretamente vinculada às regras do devido processo penal, na medida em que significa o descumprimento de uma forma-garantia. Portanto, como regra, deve conduzir ao campo da ilicitude probatória, devendo esbarrar no filtro da admissibilidade/inadmissibilidade. Utilizando o mesmo raciocínio desenvolvido ao tratar das invalidades processuais, onde explicamos que a violação da forma traz a lesão atrelada a um direito fundamental, é preciso compreender que a disciplina da cadeia de custódia é um meio para o cumprimento de regras probatórias diretamente vinculadas à concepção de devido processo penal. Dessarte, quebrar a cadeia de custódia é violar as regras que a definem e, portanto, é violar o devido processo”.

(Aury Lopes Jr, 2025, p.495).

Diante disso, podemos definir a inadmissibilidade da prova como a proibição de utilizar, em um processo judicial, elementos de convicção que são obtidos em violação à norma jurídica e aos direitos fundamentais. Uma prova que seja considerada inadmissível é juridicamente inexistente, não podendo servir como fundamento para a decisão do juiz. Por exemplo, provas digitais que foram extraídas sem os procedimentos adequados, poderão ser inadmitidas.

Em outro ponto, é abordado também pela doutrina, a admissibilidade, sendo o segundo momento da prova, é onde o juiz decide se uma prova pode ou não entrar no processo para ser avaliada. Ao contrário da inadmissibilidade, que se trata da exclusão da prova, a admissibilidade é a autorização para que a prova produzida possa ser considerada na decisão final, e para que a prova seja admitida, ela deve seguir os requisitos fundamentais analisados no juízo de admissibilidade.

O Superior Tribunal de Justiça reconheceu algumas consequências severas decorrentes da quebra da cadeia de custódia, em especial no que diz respeito às provas digitais. No julgamento do AgRg no HC 738418/SP (2025), a Sexta Turma entendeu que a ausência de preservação dos elementos necessários à verificação da confiabilidade da prova, como a auditabilidade, a repetibilidade e reprodutibilidade, comprometeu a sua validade, tornando ineficaz para os fins processuais. No caso, a falha na cadeia de custódia das mensagens de Whatsapp ensejou o desentranhamento da prova dos autos e a determinação de novo

juízo, evidenciando o impacto direto da irregularidade na formação do convencimento judicial.

Além disso, vale destacar que a violação da cadeia de custódia pode ocasionar a nulidade da prova, de acordo com o art. 157 do Código de Processo Penal e do art. 5º, inciso LVI, da Constituição Federal. Contudo, a doutrina e a jurisprudência majoritárias não adotam posição absoluta quanto à nulidade automática, exigindo a demonstração de prejuízo à parte, em conjunto com o princípio do *pas de nullité sans grief*. Sendo assim, nem toda irregularidade formal será suficiente para invalidar a prova, sendo necessária a análise do caso concreto.

Outra consequência bastante relevante quando se trata da quebra da cadeia de custódia é a possibilidade de contaminação das provas, conforme a teoria dos frutos da árvore envenenada disposta no art. 157, §1º, do Código de Processo Penal. Dessa forma, a invalidade da prova originária pode irradiar efeitos sobre outros elementos probatórios dela decorrentes, comprometendo todo o conjunto probatório dela decorrentes, comprometendo todo o conjunto probatório.

Por fim, podemos destacar que a quebra da cadeia de custódia pode acabar influenciando diretamente a decisão do magistrado, reduzindo o valor probatório dos elementos apresentados, e em casos ainda mais graves, levar à absolvição por insuficiência de provas. Além disso, eventuais irregularidades na preservação de vestígios digitais podem acarretar na responsabilização dos agentes públicos envolvidos, principalmente quando constatada conduta negligente ou dolosa na manipulação da prova.

Diante do exposto, podemos observar que a adequada observância da cadeia de custódia constitui elemento indispensável na validade e na confiabilidade da prova no processo penal, especialmente quando falamos de provas digitais. Portanto, a crescente utilização de tecnologias complexas e descentralizadas, como os criptoativos, intensifica os desafios relacionados à preservação e análise da prova, impondo dificuldades à atuação da persecução penal, tornando-se necessário desenvolver a compreensão das particularidades dos ativos digitais e dos obstáculos que apresentam à investigação criminal, tema que será abordado no capítulo seguinte.

1.3 Criptoativos e os Desafios da Investigação

As criptomonedas se tornaram uma ferramenta para a lavagem de dinheiro e, de certa forma, dificultam as investigações. Isso porque, valores ilícitos provenientes de crimes são

convertidos em cripto, uma espécie de moeda digital descentralizada, que não depende de bancos centrais ou intermediários financeiros que identificam os usuários. Mas é importante diferenciarmos o anonimato de segredo, tendo em vista que a maioria das criptomoedas utiliza uma *blockchain* pública, onde todas as transações são visíveis, mas os participantes não são identificados por nomes, mas sim por codificação.

Neste capítulo, veremos a dificuldade nas investigações criminais, principalmente se tratando de ativos digitais e as dificuldades na recuperação deles, e reforçaremos a importância da cadeia de custódia na investigação de crimes que se utilizam dos meios digitais para se esconderem da lei, e como a lei precisa de certa forma se adaptar a essas novas práticas que se encontram sempre em constante evolução.

1.3.1 Criptomoedas como Instrumento de Ocultação

A utilização de criptomoedas como um instrumento de ocultação de valores ilícitos tem se tornado uma das principais preocupações no âmbito da persecução penal, especialmente em crimes de natureza econômica e financeira, isso devido à maneira como os criptoativos operam, sendo de forma descentralizada, e sem qualquer intermediação de instituições financeiras, dificultando de forma significativa a identificação dos autores.

Uma das maiores controvérsias relacionadas às moedas digitais reside no anonimato que permeia suas operações. Conforme aponta Neves:

“a maior polêmica em torno das moedas digitais está relacionada ao anonimato das transações, visto que esse caráter anônimo acaba retirando do Estado o controle do fluxo de capitais em seus territórios, e, conseqüentemente, dificulta o combate aos crimes financeiros”

(NEVES, 2023, p.16).

Essa característica decorre da própria estrutura da tecnologia blockchain, onde não há a identificação correta dos usuários.

Contudo, conforme já destacado anteriormente, o anonimato não é absoluto, mas sim relativo, uma vez que as transações permanecem registradas em blockchain, possibilitando o rastreamento dos fluxos financeiros, mediante técnicas especializadas.

A ocultação de bens utilizando-se de criptomoedas configura crime de lavagem de dinheiro e ocultação de bens, crime esse tipificado na Lei nº 9.613/1998. Essa lei cria mecanismos de prevenção e estabelece penalidades buscando, principalmente impedir a utilização do sistema financeiro para atos ilícitos. A conversão desses ativos ilícitos em

criptoativos pode dificultar a recuperação dos valores pelas vítimas, sobretudo em razão da ausência de mecanismos centralizados de controle e bloqueio imediato, como ocorre no sistema financeiro tradicional.

As moedas digitais se tornam a escolha perfeita para que ocorra a lavagem de dinheiro e a ocultação, sendo cada vez mais utilizadas para esse fim, dificultando de certa forma que a vítima reaveja aquele valor subtraído. Isso porque, quando o valor é subtraído em forma de pix e transferido para a conta do autor, o Banco Central, através do seu novo modelo de recuperação (o MED, que é acionado no aplicativo do banco), no mesmo instante faz com que o banco do pagador notifique o banco do recebedor, que bloqueia o valor na conta do golpista. No entanto, isso não ocorre com moedas digitais, pelo fato de a mesma ser descentralizada.

1.3.2 Técnicas de Rastreamento e Atuação Estatal

Apesar das dificuldades relacionadas à utilização de criptoativos para a prática de crimes digitais, especialmente quando nos referimos ao pseudoanonimato das transações, verifica-se que tais operações não são completamente imunes à atuação do Estado. Tendo em vista que a própria estrutura da tecnologia blockchain possibilita o registro permanente e transparente das transações realizadas, permitindo o rastreamento dos fluxos financeiros mediante o uso de ferramentas especializadas.

A tecnologia *blockchain*, ou cadeia de blocos, consiste em um sistema de registro distribuído que permite o armazenamento seguro e transparente de transações digitais, sem a necessidade de uma autoridade central. Sua estrutura é formada por blocos interligados de informações, os quais são validados por mecanismos criptográficos, garantindo a integridade e a imutabilidade dos dados registrados. Nesse sentido, destaca-se que “a *blockchain* permite o registro descentralizado de transações, formando um banco de dados compartilhado e seguro, cuja alteração se torna extremamente difícil em razão dos mecanismos criptográficos empregados” (NEVES, 2023, p. 18).

Para melhor compreensão, podemos também verificar o que diz Bruno Mohammed Zohar Jaffal, onde ele explica de forma concreta como funciona o registro de criptoativos através da blockchain:

“Cada usuário de criptoativos possui uma chave privada que serve para autenticar sua identidade e possibilitar a realização de transações. Essas chaves podem ser geradas manualmente pelo próprio usuário, por meio de números inteiros que variam de 1 até 78 dígitos, ou por meio de geradores automáticos baseados em algoritmos de números aleatórios. A partir do momento em que o usuário detém a chave, torna-se possível movimentar ou utilizar os criptoativos. Contudo, na ausência dessa

chave, não é possível acessar, gastar ou converter os ativos, o que os torna inutilizáveis até que a chave seja recuperada”. (JAFFAL, 2025, p. 07).

É importante destacar que, mesmo com o uso da *blockchain*, ainda há dificuldades na identificação do autor. Isso porque a *blockchain* registra, principalmente, de qual endereço saiu o valor e para qual endereço ele foi direcionado, mas não identifica, de forma direta, quem está por trás daquele endereço. Trata-se, portanto, de um sistema baseado no pseudoanonimato¹², no qual os registros são públicos e transparentes, porém desvinculados da identidade civil dos usuários. Outro obstáculo relevante diz respeito à dependência de dados externos, uma vez que, para que o Estado consiga identificar o autor, torna-se necessário o acesso a informações provenientes de *exchanges*¹³, endereços de IP e cadastros de usuários, os quais, muitas vezes, encontram-se sob a guarda de plataformas situadas no exterior.

Nesses casos apresentados, a investigação depende de mecanismos de cooperação internacional, frequentemente marcados pela ausência de regulamentação uniforme e pela morosidade no atendimento de requisições, o que pode comprometer a efetividade da persecução penal. Soma-se a isso a utilização de mecanismos voltados à ocultação de transações, como *mixers*¹⁴ e carteiras não custodiadas, que dificultam o rastreamento dos ativos. Nesse contexto, embora a tecnologia *blockchain* proporcione maior transparência às transações com criptoativos, verifica-se que persistem entraves significativos tanto na identificação dos agentes quanto na recuperação de ativos ilícitos.

Além da *blockchain*, a investigação de crimes envolvendo criptoativos também utiliza mecanismos complementares de identificação, conforme já mostrado, a *blockchain*, por si só, não permite a identificação direta dos usuários, exigindo a utilização de dados externos e estratégias investigativas adicionais. Diante disso, existe a obtenção de informações junto às *exchanges* (plataformas responsáveis pela intermediação de operações com criptoativos), que exigem o fornecimento de dados pessoais, documentos e, em alguns casos, a comprovação de endereço. Essas informações podem ser requisitadas pelas autoridades competentes, mediante ordem judicial, possibilitando a identificação dos autores.

¹² Tradução Livre da Autora: característica das transações em criptomoedas nas quais os usuários não são identificados diretamente por seus nomes civis, mas por códigos ou endereços digitais, permitindo eventual rastreamento mediante investigação técnica.

¹³ Tradução Livre da Autora: plataformas digitais destinadas à compra, venda, negociação e conversão de criptomoedas e outros criptoativos.

¹⁴ Tradução Livre da Autora: ferramenta que mistura criptomoedas de diversos usuários para dificultar o rastreamento das transações e a identificação da origem dos recursos.

Outro instrumento bastante relevante consiste na análise de endereços IP e metadados associados às transações e o acesso a plataformas digitais, sendo possível rastrear a origem das operações e estabelecer vínculos com dispositivos e localizações específicas.

Porém, mesmo com esses mecanismos citados, ainda persistem limitações no que diz respeito à plena individualização dos autores de crime com o uso de criptoativos como meio de ocultação de valores ilícitos. Devido à possibilidade da utilização de plataformas estrangeiras, que não possuem regulamentação equivalente, à adoção de ferramentas de anonimização e à fragmentação em múltiplos endereços, que dificultam de certa forma o rastreamento de ativos.

Sob essa perspectiva, tais dificuldades não se limitam à fase investigativa, mas também repercutem na produção de prova, especialmente no que se refere à cadeia de custódia, principalmente porque a coleta, o armazenamento e a análise de dados digitais, muitas vezes obtidos de diferentes fontes, inclusive internacionais, exigem, rigorosos procedimentos de documentação e preservação, com o intuito de garantir a integridade, autenticidade e a confiabilidade das evidências.

1.3.3 Casos Práticos de Estelionato com Criptoativos

A crescente utilização de criptoativos em esquemas de estelionato digital pode ser observada de forma concreta em operações policiais recentes, destacando-se a Operação Mirage, deflagrada pela Polícia Civil do Estado do Rio Grande do Sul, que investigou uma organização criminosa especializada em golpes de falsos investimentos, com utilização de plataformas digitais e posterior conversão de valores em criptomoedas, evidenciando as dificuldades investigativas e de recuperação de ativos no ambiente virtual.

No referido caso, os investigados utilizavam redes sociais e aplicativos de mensagens com o intuito de captar vítimas, simulando operações financeiras com promessas falsas de alto valor. Com a criação de um ambiente de confiança, a maior parte dos valores era transferida via *pix*, para contas vinculadas a empresas de fachada e posteriormente convertida em criptoativos, com o objetivo de dificultar o rastreamento e a recuperação patrimonial.

O caso apresenta que a eficácia da persecução penal em crimes de estelionato digital depende não apenas da adequada preservação da cadeia de custódia da prova, mas também do desenvolvimento de mecanismos jurídicos e técnicos aptos a viabilizar a rastreabilidade e a recuperação de ativos em ambientes que operam de forma descentralizada.

No caso apresentado, a investigação envolveu a apreensão de dispositivos eletrônicos, análise de dados e bloqueio de dezenas de contas bancárias, exigindo rigor na observância da cadeia de custódia da prova digital, nos termos dos arts. 158-A ao 158-F do Código de Processo Penal, a fim de garantir a integridade e a autenticidade dos elementos informativos coletados.

Sob a perspectiva jurídica, o caso evidencia a incidência do crime de estelionato, previsto no art. 171 do Código Penal, praticado mediante fraude eletrônica, com utilização de engenharia social e manipulação de informações no ambiente digital. Observa-se também a utilização de mecanismos típicos de ocultação patrimonial, especialmente por meio da conversão dos valores em criptoativos, o que se aproxima das práticas descritas na Lei nº 9.613/98 (Lei de Lavagem de Dinheiro), sobretudo no que tange à dissimulação da origem ilícita dos recursos.

Outro golpe bastante comum atualmente, é o “golpe do falso advogado” que ganhou bastante destaque por utilizar dados pessoais das partes e de seus advogados, onde criminosos se passam pelo advogado da vítima, informando que obteve êxito no processo e que receberia uma quantia equivalente mediante pagamento de um valor.

1.4 Desafios Investigativos e Jurisdicionais

É notável que o isolamento social ocasionado pela pandemia da Covid-19 teve uma grande influência no aumento da criminalidade praticada através de meios digitais. Com a ampliação do uso de serviços digitais durante o período de distanciamento social, transações financeiras, compras e comunicações passaram a ocorrer predominantemente no ambiente virtual, criando novas oportunidades para a atuação de agentes criminosos. (FERNANDES, 2026).

No entanto, mais relevante que o aumento quantitativo da prática do crime de estelionato digital é a constatação de que o ordenamento jurídico e os mecanismos de persecução penal não evoluíram na mesma proporção. Evidenciam-se limitações estruturais, normativas e operacionais que comprometem a efetividade da investigação e da responsabilização penal, bem como a recuperação dos vestígios digitais.

Nesse cenário, a morosidade na condução das investigações surge como uma das manifestações mais evidentes dessas deficiências. Conforme destaca Aury Lopes Junior (2026), a manutenção de inquéritos policiais por longos períodos sem qualquer definição, seja

oferecimento de denúncia ou arquivamento, evidencia a ineficiência estatal e pode configurar violação ao direito fundamental à duração razoável do processo.

Verifica-se que os desafios enfrentados na persecução penal dos crimes digitais não se limitam ao aumento de sua incidência, mas envolvem entraves de natureza normativa, probatória, temporal e operacional, que comprometem a efetividade da resposta estatal. Nesse sentido, passa-se à análise das principais limitações normativas relacionadas à persecução penal de crimes digitais.

1.4.1 Limitações Normativas na Persecução Penal de Crimes Digitais

O presente cenário nos faz observar que a evolução normativa brasileira se deu por eventos que trouxeram grandes repercussões, sem uma ideia normativa que se mostrasse voltada ao ambiente digital. Temos como exemplo a Lei 12.737/12, mais conhecida como “Lei Carolina Dieckmann”, a qual alterou o Código Penal Brasileiro tipificando crimes informáticos e que apresentou grandes lacunas posteriormente sanadas pela Lei 14.155/21 (SILVA, 2026, p.06).

A Lei Carolina Dieckmann apresentou o primeiro esforço legislativo tipificando os crimes informáticos no ordenamento jurídico, isso porque inseriu o art. 154-A no Código Penal e criminalizou a invasão de dispositivos informáticos. Porém, com a constante evolução, houve dificuldades interpretativas e lacunas normativas de significativo impacto prático. Esse vácuo normativo foi parcialmente suprido pela Lei nº 14.155/2021, que trouxe uma alteração ao art. 171 do Código Penal para a inclusão do § 2º-A, que trata especificamente da fraude eletrônica e fixou penas de 4 (quatro) a 8 (oito) anos e multa para crimes cometidos mediante o uso de dispositivos eletrônicos.

Diante desse cenário, surgiram duas leis extremamente importantes no que diz respeito a crimes cibernéticos, a Lei nº 12.965/2014, mais conhecida como o Marco Civil da Internet e a Lei Geral de Proteção de dados, que se incorporaram ao sistema como normas complementares muito relevantes, mas de natureza predominantemente regulatória, e não penal. Isso decorre pelo fato de que, enquanto o Marco Civil estabelece obrigações de guarda de registros e acessos e de conexão pelos provedores, criando fundamento normativo para eventual obtenção de elementos probatórios em investigação criminal, a Lei Geral de Proteção de Dados regula o tratamento de dados pessoais, focando principalmente na proteção dos titulares e na responsabilidade civil e administrativa de organizações.

Recentemente, foi sancionada, em maio de 2026, a Lei nº 15.397/2026, que promoveu o endurecimento das penas para crimes patrimoniais, focada principalmente em crimes cometidos no meio digital, como o estelionato. Dentre as inovações, podemos ressaltar a criminalização do uso de “contas laranjas” como instrumento para fraudes eletrônicas, prática recorrente em esquemas de estelionato digital. Essa legislação evidencia tentativa do legislador de acompanhar as novas dinâmicas criminosas, ampliando os mecanismos de repressão penal. No entanto, apesar dos avanços, essas medidas ainda se mostram insuficientes para superar as limitações estruturais do sistema penal, especialmente na complexidade das fraudes envolvendo ativos digitais.

As limitações normativas não decorrem apenas da ausência de tipos penais específicos, mas da inadequada estrutura do próprio Código Penal frente à realidade digital. Diante do cenário atual, Silva (2025) afirma que “a principal limitação estrutural da legislação penal brasileira em matéria digital reside na defasagem conceitual do Código Penal de 1940, elaborado em um contexto histórico de total ausência de tecnologia informática”. Segundo o autor, ainda que os tipos penais tradicionais tenham sido criados com base em elementos de materialidade física, como bens corpóreos e documentos em papel, fato que dificulta e inviabiliza a adequada integração de condutas praticadas no ambiente virtual. Esse cenário revela um descompasso entre a evolução tecnológica e a resposta legislativa, comprometendo a efetividade da persecução penal, especialmente em delitos que envolvem ativos digitais.

Diante do apresentado, verifica-se que a insuficiência normativa não apenas dificulta a tipificação adequada das condutas praticadas em ambientes digitais, como também compromete a eficácia da persecução penal em crimes de estelionato eletrônico. Isso se torna ainda mais evidente quando tratamos de crimes envolvendo criptoativos, cuja natureza descentralizada e intangível desafia os modelos tradicionais de repressão penal, evidenciando-se a necessidade de constante atualização legislativa e de adaptação dos instrumentos jurídicos, a fim de garantir uma resposta estatal mais eficiente frente às novas modalidades de crimes.

1.4.2 Prova Digital: Obtenção, Preservação e Validade

Como já apresentado anteriormente, a obtenção e preservação da prova digital, representa um dos principais desafios investigativos contemporâneos, especialmente quando tratamos da volatilidade dos dados eletrônicos e da facilidade de alteração ou exclusão das informações armazenadas em ambientes virtuais. Muito diferente das provas tradicionais, os

vestígios digitais exigem procedimentos técnicos específicos destinados à preservação da integridade e autenticidade da evidência.

Conforme Aury Lopes Junior (2026, p. 463), a cadeia de custódia da prova digital possui “morfologia específica e completamente distinta” das provas tradicionais, exigindo procedimentos técnicos rigorosos destinados à preservação da integridade e confiabilidade da evidência eletrônica.

Esse tipo de característica apresentada pelos vestígios digitais dificulta a preservação da prova, exigindo dos agentes mais cautela na obtenção e na preservação da prova, trazendo à persecução penal uma dificuldade a mais para manter a prova digital algo válido no processo.

1.4.3 Morosidade Investigativa E Duração Razoável Do Processo

Além das dificuldades técnicas da obtenção da prova digital, a persecução penal nos crimes virtuais também enfrenta entraves relacionados à morosidade investigativa, especialmente diante da dependência de provedores, da necessidade de cooperação internacional e da complexidade das diligências tecnológicas.

A Constituição Federal assegura o direito fundamental à razoável duração do processo e os meios que garantam a celeridade de sua transmissão, em seu art. 5º, inciso LXXVIII. Essa garantia possui aplicação no âmbito judicial e também na fase pré-processual investigativa, uma vez que o inquérito policial não se pode perpetuar indefinidamente sob pena de violar a segurança jurídica e as garantias fundamentais do indivíduo.

Conforme Aury Lopes Jr., o inquérito policial constitui modelo de investigação preliminar que é conduzido pela polícia judiciária, porém são dependentes de investigação judicial para a adoção de medidas restritivas de direitos fundamentais. Essa característica nos apresenta uma importante limitação estrutural da persecução penal, especialmente nos crimes digitais, nos quais a obtenção de registros telemáticos, dados bancários ou informações vinculadas a criptoativos frequentemente exigem prévia autorização judicial, contribuindo para a morosidade investigativa.

Essa dependência de autorização judicial para a adoção de medidas invasivas, embora essencial à proteção das garantias fundamentais, contribui para a lentidão investigativa em crimes cometidos por meio virtual, diante da rapidez na circulação e ocultação de ativos.

É importante destacar também que a morosidade é intensificada pela dependência de provedores de aplicação e plataformas digitais, que são muitas das vezes estabelecidos no

exterior. E a obtenção de dados relevantes como registros telemáticos, endereços de IP e informações bancárias digitais dependem do cumprimento de procedimentos burocráticos e de cooperação jurídica internacional.

A lentidão investigativa nos crimes de estelionato digital também decorre da insuficiência estrutural das forças de segurança pública brasileira. A escassez de delegacias especializadas em crimes cibernéticos compromete a capacidade estatal de resposta imediata, especialmente diante da volatilidade das evidências digitais, que podem ser rapidamente apagadas ou modificadas. Ademais, a migração das práticas fraudulentas para ambientes de anonimização, como a *Deep Web*¹⁵, associada ao uso de mecanismos de criptografia, intensifica a complexidade investigativa e frequentemente conduz à ineficácia das diligências estatais. (MIRANDA JUNIOR; RODRIGUES; ALVES, 2026).

O Marco Civil da Internet (Lei nº 12.965/2014) estabelece parâmetros importantes para a preservação e fornecimento de registros digitais, prevendo, inclusive, hipóteses de guarda obrigatória de dados por provedores de conexão e aplicação. Contudo, a efetividade dessas disposições ainda encontra limitações práticas, especialmente diante da atuação de empresas estrangeiras e da ausência de mecanismos céleres de cooperação internacional. Tal cenário evidencia o descompasso entre a velocidade das práticas criminosas digitais e a capacidade de resposta do sistema estatal de persecução penal.

Dessa forma, verifica-se que a morosidade investigativa constitui um dos principais entraves à efetividade da persecução penal nos crimes de estelionato digital envolvendo criptomoedas. A insuficiência estrutural do Estado, aliada à dependência tecnológica e à burocracia internacional, compromete tanto a produção probatória quanto a recuperação patrimonial dos ativos ilícitos, revelando a necessidade de modernização dos mecanismos investigativos e de fortalecimento da cooperação jurídica internacional no combate à criminalidade digital.

1.4.4 Dificuldades Práticas Na Identificação, Responsabilização E Recuperação De Ativos

Um dos maiores entraves nos crimes de estelionato digital está ligado à responsabilização dos sujeitos ativos do crime de estelionato praticados por meio do ambiente virtual, em consequência da forma com que a execução ocorre, onde o golpista, utilizando-se de várias contas nas redes sociais, ou mesmo de vários endereços de e-mail, consegue atingir um

¹⁵ Tradução Livre da Autora: parte da internet não acessada por mecanismos de busca convencionais, composta por conteúdos e sistemas acessíveis apenas mediante autorização, autenticação ou ferramentas específicas.

número ainda maior de vítimas, que ao buscarem a responsabilização do autor, acabam enfrentando óbices relacionados à identificação. (RIBEIRO, 2023).

Em alguns casos, salienta-se que a impunidade ocorre na medida em que transações bancárias, mesmo que registradas e rastreadas, nem sempre podem indicar a verdadeira autoria do delito, tendo em vista que atualmente é possível criar contas em que carteiras digitais com quase nenhuma documentação, possibilitando que golpistas se utilizem de contas laranjas, adquiridas por meio de informações vazadas em banco de dados, a fim de afastar a autoria do crime (RIBEIRO, 2023).

Os crimes cometidos sob o anonimato digital se tornaram um dos maiores desafios enfrentados pelas autoridades policiais. Conforme Oliveira e Cunha, a legislação brasileira, embora avançada em termos de garantias individuais, se mostrou deficiente quanto à articulação de normas penais e ferramentas digitais de investigação.

Essa dificuldade pode ser observada em golpes praticados mediante a utilização indevida do nome de instituições públicas e profissionais do Direito, como ocorre nos casos envolvendo falsas comunicações em nome da Receita Federal ou indivíduos que se passam por advogados para obtenção de vantagem ilícita. Nessas situações, os criminosos utilizam elementos visuais, linguagem técnica e informações pessoais das vítimas para conferir aparência de legitimidade às fraudes, dificultando a identificação imediata do golpe e ampliando o potencial lesivo da conduta criminosa.

Outro ponto a ser destacado é o uso de várias “contas laranja”, embora a quebra do sigilo bancário seja um importante instrumento investigativo, sua efetivação depende de autorização judicial, o que, na prática, pode demandar um tempo incompatível com a velocidade das transações financeiras eletrônicas. Durante esse intervalo, os valores são rapidamente transferidos para diversas outras contas, pulverizados por meio de sucessivas movimentações financeiras ou convertidos em criptoativos, reduzindo significativamente as chances de bloqueio, rastreamento e recuperação dos ativos.

Ademais, podemos citar que os crimes digitais cometidos no exterior dependem de cooperação jurídica internacional para possibilitar a identificação dos autores, a obtenção de provas e o bloqueio de valores decorrentes das fraudes. Isso ocorre principalmente porque muitos aplicativos, plataformas e provedores digitais utilizados pelos criminosos possuem servidores localizados fora do território nacional, circunstância em que limitam a atuação imediata das autoridades brasileiras. Diante disso, a obtenção de registros telemáticos, dados cadastrais e informações bancárias frequentemente exige a utilização de mecanismos de

cooperação internacional, como cartas rogatórias, acordos bilaterais e pedidos de auxílio direto entre Estados.

As criptomoedas também ampliaram a complexidade das investigações patrimoniais. Embora os registros em *blockchain* permitam a visualização das movimentações realizadas, a identificação do titular das carteiras digitais ainda é um obstáculo significativo, especialmente em operações realizadas por meio de plataformas financeiras descentralizadas ou corretoras estrangeiras, favorecendo a ocultação patrimonial. Conforme Barros (2026), a utilização de criptomoedas e mecanismos de criptografia dificulta significativamente a recuperação de ativos provenientes de crimes digitais, especialmente em razão da descentralização das operações e da limitação de acesso das autoridades públicas às carteiras virtuais.

Embora existam mecanismos de constrição patrimonial, como o SISBAJUD, sua efetividade ainda encontra limitações diante da velocidade das operações financeiras digitais e da utilização de plataformas descentralizadas.

Diante do apresentado, a recuperação de ativos obtidos ilicitamente se mostra uma das etapas mais difíceis da persecução penal, diante da rapidez das transferências eletrônicas que possibilitam a dispersão imediata dos valores em diferentes contas, reduzindo consideravelmente a efetividade do bloqueio patrimonial. Em muitos casos, quando as autoridades conseguem identificar o caminho percorrido pelos recursos, os valores já foram convertidos, transferidos ou sacados, inviabilizando a restituição integral à vítima.

Assim, constata-se que a recuperação de ativos digitais se configura como um dos maiores obstáculos no combate ao estelionato eletrônico, sobretudo em razão da rapidez das operações, da descentralização das criptomoedas e das restrições quanto à cooperação internacional e à identificação patrimonial. Esse quadro ressalta a urgência de aperfeiçoamento legislativo, o reforço dos instrumentos de investigação financeira digital e a formulação de estratégias mais eficientes direcionadas à restituição de valores oriundos da criminalidade cibernética.

CONSIDERAÇÕES FINAIS

O rápido avanço tecnológico e a constante digitalização das relações sociais transformaram significativamente a forma como os crimes ocorrem atualmente, especialmente quando nos referimos ao estelionato digital. A crescente utilização de plataformas virtuais, aplicativos de mensagens e ativos digitais ampliou não apenas o alcance das fraudes eletrônicas, mas também a complexidade da atuação estatal voltada à investigação criminal e,

principalmente, à responsabilização dos autores. Diante disso, o presente trabalho buscou analisar os principais desafios enfrentados pela persecução penal no estelionato digital, com enfoque na cadeia de custódia da prova digital e nas dificuldades jurídicas relacionadas à recuperação de ativos em criptomoedas no ordenamento jurídico brasileiro.

Durante a pesquisa, constatou-se que a produção da prova digital exige cuidados técnicos específicos para garantir sua autenticidade, integridade e confiabilidade, principalmente diante da volatilidade dos dados eletrônicos, aliada à fácil alteração, exclusão ou até mesmo de manipulação. Portanto, evidencia-se, a importância da observância da cadeia de custódia prevista nos arts. 158-A a 158-F do Código de Processo Penal. Verificou-se que a preservação adequada dos vestígios digitais é requisito essencial para assegurar a validade probatória no processo penal e evitar questionamentos quanto à licitude ou confiabilidade das provas produzidas.

Foi observado que os crimes de estelionato digital apresentam maiores obstáculos relacionados à identificação da autoria. Isso porque, o anonimato, a utilização de perfis falsos, contas de terceiros, mecanismos de criptografia e plataformas estrangeiras acabam dificultando o rastreamento dos autores. Isso ainda, somada à natureza transnacional dos crimes cibernéticos, que frequentemente exigem mecanismos de cooperação jurídica internacional para a obtenção de dados e bloqueio de ativos financeiros.

No que diz respeito à recuperação patrimonial, verificou-se que a utilização de criptomoedas e ativos digitais ampliou significativamente a complexidade das investigações financeiras. Embora, possamos contar com a tecnologia *blockchain*, que permite o registro das transações realizadas, a descentralização das operações e a utilização de carteiras protegidas por mecanismos de criptografia dificultam a identificação dos titulares e a efetiva recuperação dos valores obtidos ilicitamente. Foi constatado, ainda, que a rapidez das transferências eletrônicas e a possibilidade de movimentação internacional instantânea dos ativos comprometem a efetividade das medidas cautelares patrimoniais adotadas pelo Estado.

A pesquisa aborda que, apesar dos crescentes avanços legislativos promovidos, o ordenamento jurídico ainda se encontra defasado, apresentando limitações normativas e operacionais diante da constante inovação tecnológica, que se desenvolve também no crime. A ausência de regulamentação no cenário internacional, aliada à dificuldade de fiscalização de plataformas estrangeiras e das finanças descentralizadas, contribui de forma significativa para a ampliação dos desafios investigativos enfrentados e para a baixa efetividade da recuperação de ativos digitais.

Portanto, conclui-se que o enfrentamento do crime de estelionato digital não exige apenas a atualização legislativa contínua, mas também investimentos em tecnologias investigativas, capacitação técnica dos órgãos de persecução penal e fortalecimento da cooperação internacional. É imprescindível a adoção de mecanismos mais eficientes de rastreamento patrimonial digital, de preservação da cadeia de custódia digital e de fiscalização de operações que envolvam ativos virtuais, com o objetivo de proporcionar maior efetividade à tutela penal e reduzir a sensação de impunidade nos crimes praticados no ambiente virtual.

Por fim, a evolução tecnológica impõe ao Direito o desafio permanente de adaptação às novas formas de criminalidade, tornando-se fundamental a construção de instrumentos jurídicos e investigativos compatíveis com a realidade atual, principalmente no que tange à proteção patrimonial das vítimas e à preservação da segurança jurídica no contexto das relações virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

BARROS, Ana Carolina de Souza; OLIVEIRA, Tarsis Barreto. A preservação das provas na investigação de crimes cibernéticos: desafios da cadeia de custódia digital. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 11, n. 11, p. 2537–2554, 2025. Disponível em: <https://periodicorease.pro.br/rease/article/view/22103>. Acesso em: 28 abr. 2026.

BONFIM, Edilson M. **Curso de Processo Penal**. 15. ed. Rio de Janeiro: SRV, 2025. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625833/>. Acesso em: 30 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Conflito de Competência n. 188.955/SC**. Relator: Ministro Ribeiro Dantas. Julgado em 2022. Disponível em: <https://www.stj.jus.br>. Acesso em: 20 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental nos Embargos de Declaração no Conflito de Competência n. 211.201/SP**. Relator: Ministro Joel Ilan Paciornik. Julgado em 14 maio 2025. Diário de Justiça Eletrônico Nacional: 2 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **AgRg no HC 1.014.212/ES**. Relator: Ministro Carlos Pires Brandão. Sexta Turma. Julgado em 10 fev. 2026. DJe: 20 fev. 2026.

BRASIL. Superior Tribunal de Justiça. **AgRg no HC 738418/SP**. Relator: Ministro Otávio de Almeida Toledo (Desembargador convocado do TJSP). Sexta Turma. Julgado em: 11 mar. 2025. DJe: 21 mar. 2025.

FERNANDES, Pablo Henrique Vieira; PINTO, Diego Santos Almeida. Fraudes eletrônicas e estelionatos no Brasil: entre a expansão criminosa e os limites da legislação vigente. **Aposta: Revista de Ciências Sociais**, [S. l.], v. 110, p. e700, 2026. Disponível em: <https://revistaaposta.com/index.php/ra/article/view/700>. Acesso em: 5 maio 2026.

FERREIRA VAZ, Millena. A preservação da cadeia de custódia como pressuposto de admissibilidade da prova digital. **Revista da ESMESC**, [S. l.], v. 30, n. 36, p. 323–350, 2023. Disponível em: <https://esmesec.emnuvens.com.br/re/article/view/406>. Acesso em: 17 mar. 2026.

FRANCK, Kewry Mariobo; FERREIRA, Romario Vitorino. Instruções preventivas contra crimes cibernéticos e orientações da perícia forense computacional. **Revista Nativa Americana de Ciências, Tecnologia & Inovação**, v. 4, n. 1, p. 116–132, 2023. Disponível em: <https://jiparana.emnuvens.com.br/riacti/article/view/689>. Acesso em: 29 abr. 2026.

GALINDO, Guilherme Delgado. **Evolução do estelionato pelo meio digital**. 2022. 30 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Presbiteriana Mackenzie, São Paulo, 2022. Disponível em: <https://dspace.mackenzie.br/handle/10899/32604>. Acesso em: 15 maio 2026.

JAFFAL, Bruno Mohammed Zoher. A lavagem de dinheiro por meio de criptoativos no Brasil: desafios regulatórios e repercussões jurídicas. **Revista Jurídica da OAB/SC**, Florianópolis, v. 5, p. 1-23, out. 2025. Disponível em: <https://iabnacional.org.br>. Acesso em: 3 maio 2026.

JUNIOR, Aury L. **Direito Processual Penal**. 23. ed. Rio de Janeiro: SRV, 2026. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786551771675/>. Acesso em: 1 maio 2026.

JÚNIOR, Miguel R. **Código Penal Comentado**. 2. ed. Rio de Janeiro: Saraiva Jur, 2023. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555599510/>. Acesso em: 17 abr. 2026.

MIRANDA JUNIOR, A. N. S.; RODRIGUES, E. S.; ALVES, M. D. A. O locus delicti na era digital: competência jurisdicional e os desafios investigativos do estelionato eletrônico. **Revista Ilustração**, [S. l.], v. 7, n. 3, p. 187–198, 2026. Disponível em: <https://journal.editorailustracao.com.br/index.php/ilustracao/article/view/560>. Acesso em: 11 maio 2026.

NEVES, Janaine Alcântara. **Criptomoedas: os desafios da investigação policial no combate aos crimes contra a ordem econômico-financeira**. 2023. Monografia (Bacharelado em Relações Internacionais) – Centro Universitário de Brasília (UniCEUB), Brasília, 2023.

NUCCI, Guilherme de S. **Código Penal Comentado**. 25. ed. Rio de Janeiro: Forense, 2025. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530995973/>. Acesso em: 14 nov. 2025.

NUCCI, Guilherme de S. Curso de Direito Penal: Vol. 2. 9. ed. Rio de Janeiro: Forense, 2025. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996666/>. Acesso em: 3 mar. 2026.

NUCCI, Guilherme de S. **Curso de Direito Processual Penal**. 22. ed. Rio de Janeiro: Forense, 2025. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530996642/>. Acesso em: 12 mar. 2026.

OLIVEIRA, Carlos Henrique Bassani de. **Discussões jurídicas acerca do estelionato virtual: evolução, características e combate**. 2024. 21 f. Artigo de conclusão de curso (Bacharel em Ciências Jurídicas e Sociais) – Curso de Direito, Universidade de Passo Fundo, Soledade, 2024.

PINHEIRO, Patrícia P. **Direito Digital**. 7. ed. Rio de Janeiro: Saraiva Jur, 2021. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/>. Acesso em: 19 nov. 2025.

POLÍCIA CIVIL DO ESTADO DO RIO GRANDE DO SUL. **Operação Mirage mira organização criminosa especializada em golpes de falsos investimentos**. 2026. Disponível em: <https://www.pc.rs.gov.br>. Acesso em: 4 maio 2026.

RIBEIRO, Gabriel Santos. O estelionato por meios digitais: a problemática da responsabilização. In: SIMPÓSIO INTERNACIONAL DE ANÁLISE CRÍTICA DO

DIREITO, 12., 2023, Jacarezinho. **Anais [...]**. Jacarezinho, PR: UENP, 2023. p. 111-125. Disponível em: <https://siacrid.com.br>. Acesso em: 13 maio 2026.

RIGHI IVAHY BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, p. 7–9, 2024. Disponível em: <https://publicacoes.ibccrim.org.br>. Acesso em: 22 abr. 2026.

SILVA, Gustavo Almeida; FRANCO, Arisson Carneiro. A eficácia da legislação penal brasileira no combate aos crimes cibernéticos. **Revista de Geopolítica**, [S. l.], v. 17, n. 4, p. e2261, 2026. Disponível em: <https://mail.revistageo.com.br/revgeo/article/view/2261>. Acesso em: 6 maio 2026.

VAZ, Denise Provasi. **Prova digital no processo penal**. 2012. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: <https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/>. Acesso em: 20 abr. 2026.