

DIREITO PENAL: DO CRIME DE ESTELIONATO E OUTRAS FRAUDES ELETRÔNICAS NO BRASIL

CRIMINAL LAW: THE CRIME OF FRAUD AND OTHER FORMS OF ELECTRONIC FRAUD IN BRAZIL

Artigo submetido em 19 de outubro de 2026

Artigo aprovado em 21 de outubro de 2026

Artigo publicado em 21 de outubro de 2026

Cognitio Juris

Volume 16 – Número 59 – 2026

ISSN 2236-3009

Autor:

Geane Romeu Gadelha Lima de Moraes

Rita de Cássia Fadoul Cacho

Franklin Vieira dos Santos

Resumo: O desenvolvimento das tecnologias digitais proporcionou importantes avanços nas relações sociais, comerciais e financeiras, mas também favoreceu o surgimento e o aperfeiçoamento de práticas criminosas realizadas por meios eletrônicos. Nesse cenário, destaca-se o estelionato eletrônico, caracterizado pela utilização de mecanismos fraudulentos destinados a induzir ou manter a vítima em erro para obtenção de vantagem ilícita. O presente artigo tem como objetivo analisar o crime de estelionato e as principais

fraudes eletrônicas praticadas no Brasil, abordando seus elementos jurídicos, as alterações promovidas pela Lei nº 14.155/2021 e os desafios enfrentados pelo Direito Penal diante da constante evolução tecnológica. A pesquisa utiliza método dedutivo, com abordagem qualitativa e procedimento bibliográfico e documental, fundamentando-se na legislação brasileira e na doutrina penal. Verifica-se que a expansão das redes sociais, aplicativos de mensagens, serviços bancários digitais e sistemas de pagamento instantâneo ampliou as possibilidades de atuação dos criminosos, exigindo maior proteção jurídica das vítimas. Conclui-se que o fortalecimento da legislação penal representa importante mecanismo de enfrentamento às fraudes eletrônicas, embora a repressão criminal deva ser acompanhada por investimentos em investigação tecnológica, segurança da informação, educação digital e prevenção.

Palavras-chave: Estelionato, Fraude eletrônica, Crimes cibernéticos, Direito Penal, Internet.

Abstract: The development of digital technologies has provided significant advances in social, commercial, and financial relations, but it has also favored the emergence and refinement of criminal practices carried out through electronic means. In this scenario, electronic fraud stands out, characterized by the use of fraudulent mechanisms designed to induce or maintain the victim in error to obtain illicit gain. This article aims to analyze the crime of fraud and the main electronic frauds practiced in Brazil, addressing its legal elements, the changes promoted by Law No. 14.155/2021, and the challenges faced by Criminal Law in the face of constant technological evolution. The research uses a deductive method, with a qualitative approach and bibliographic and documentary procedure, based on Brazilian legislation and criminal doctrine. It is observed that the expansion of social networks, messaging applications, digital banking services, and instant payment systems has broadened the possibilities for criminal activity, requiring greater legal protection for victims. It is concluded that strengthening criminal legislation represents an important mechanism for combating electronic fraud, although criminal repression must be accompanied by investments in technological research, information security, digital education, and

prevention.

Keywords: Fraud, Electronic fraud, Cybercrimes, Criminal law, Internet.

1 INTRODUÇÃO

O desenvolvimento das tecnologias digitais provocou mudanças profundas nas formas de comunicação, contratação, movimentação financeira e realização de negócios. Smartphones, redes sociais, aplicativos de mensagens, comércio eletrônico e serviços bancários digitais tornaram diversas atividades mais rápidas e acessíveis. A mesma infraestrutura, entretanto, passou a ser explorada para a prática de delitos patrimoniais, permitindo que criminosos alcancem vítimas a distância, utilizem identidades falsas e transfiram valores em poucos segundos.

Entre os delitos transformados por esse processo encontra-se o estelionato, previsto no artigo 171 do Código Penal. Sua estrutura tradicional permanece baseada no emprego de fraude para induzir ou manter alguém em erro, obter vantagem ilícita e causar prejuízo alheio. O que se alterou foi o modo de execução: páginas falsas, clonagem de perfis, falsas centrais de atendimento, mensagens de supostos familiares, boletos adulterados e transferências instantâneas passaram a integrar o cotidiano da criminalidade patrimonial.

A relevância social do tema é demonstrada pela dimensão dos registros. Segundo o Fórum Brasileiro de Segurança Pública (FBSP, 2026), foram contabilizados 2.261.055 estelionatos em 2025, dos quais 346.753 foram registrados especificamente como estelionato por meio eletrônico. A entidade aponta crescimento de 429,8% dos estelionatos desde 2018 e informa que 83,2% da população teme ser vítima de fraude pela internet ou pelo celular. A estatística deve ser interpretada com cautela, pois diferenças na classificação policial e a subnotificação impedem que os registros representem toda a criminalidade real.

A resposta legislativa mais expressiva foi a Lei nº 14.155/2021, que introduziu o § 2º-A no

artigo 171 do Código Penal, qualificou o furto mediante fraude eletrônica e alterou a competência territorial em determinadas hipóteses de estelionato. A mudança procurou conferir tratamento mais rigoroso às fraudes praticadas por redes sociais, contatos telefônicos, correio eletrônico e meios análogos. A elevação das penas, contudo, não resolve isoladamente problemas relacionados à autoria, à produção de provas, à cooperação institucional e à recuperação dos valores retirados das vítimas.

Diante desse contexto, formula-se o seguinte problema de pesquisa: em que medida a legislação penal brasileira, especialmente após a Lei nº 14.155/2021, oferece instrumentos adequados para prevenir e reprimir o estelionato e outras fraudes eletrônicas diante da constante evolução tecnológica? Parte-se da hipótese de que a reforma legislativa aperfeiçoou a tipificação e a persecução penal, mas apresenta eficácia limitada quando não acompanhada de investigação tecnológica, prevenção, integração entre instituições e proteção dos usuários do sistema financeiro.

O objetivo geral deste trabalho é analisar o crime de estelionato e as fraudes eletrônicas no ordenamento jurídico brasileiro. Como objetivos específicos, busca-se compreender os elementos do tipo penal, examinar as mudanças promovidas pela Lei nº 14.155/2021, identificar as modalidades mais recorrentes de fraude eletrônica, analisar dados estatísticos e decisões recentes do Superior Tribunal de Justiça, diferenciar o estelionato eletrônico do furto mediante fraude, comparar brevemente o modelo brasileiro com normas estrangeiras e discutir os desafios relacionados à investigação, à prova digital e à prevenção.

A pesquisa possui abordagem qualitativa e natureza exploratória e descritiva, sendo desenvolvida por meio do método dedutivo. O levantamento bibliográfico abrangeu obras de Direito Penal e de crimes cibernéticos. A pesquisa documental examinou o Código Penal, o Código de Processo Penal, a Lei nº 14.155/2021, decisões do Superior Tribunal de Justiça publicadas entre 2022 e 2026 e os Anuários Brasileiros de Segurança Pública com dados relativos ao período de 2020 a 2025.

Foram selecionados julgados diretamente relacionados às fraudes praticadas por transferência bancária, WhatsApp e PIX, bem como à competência territorial e ao dever de segurança das instituições financeiras. Para a comparação internacional, foram analisados o 18 U.S.C. § 1030, dos Estados Unidos, e as Diretivas 2013/40/UE e 2019/713 da União Europeia. Os dados e documentos foram interpretados mediante análise de conteúdo, considerando as convergências, as lacunas e os efeitos práticos das normas examinadas.

2 O CRIME DE ESTELIONATO NO DIREITO PENAL BRASILEIRO

2.1 Conceito e elementos caracterizadores

O estelionato encontra-se previsto no art. 171 do Código Penal e integra o conjunto dos crimes contra o patrimônio. A conduta consiste essencialmente na obtenção de vantagem ilícita, para o próprio agente ou para terceiro, em prejuízo de outra pessoa, mediante a utilização de artifício, ardil ou qualquer outro meio fraudulento capaz de induzir ou manter a vítima em erro.

Para Greco (2015), a compreensão do estelionato encontra-se diretamente relacionada ao binômio vantagem ilícita e prejuízo alheio. Isso significa que a conduta do autor deve possuir finalidade patrimonial e produzir uma situação na qual o agente obtém uma vantagem não reconhecida pelo ordenamento jurídico enquanto a vítima experimenta correspondente prejuízo econômico. O autor esclarece:

O crime de estelionato é regido pelo binômio vantagem ilícita / prejuízo alheio. A conduta do agente, portanto, deve ser dirigida a obter vantagem ilícita, em prejuízo alheio. (GRECO, 2015, p.59).

A afirmação demonstra que não basta a existência de uma mentira ou de um comportamento desonesto para caracterização do estelionato. A fraude deve estar relacionada à obtenção da vantagem ilícita e ao prejuízo experimentado pela vítima. Dessa

forma, existe uma sequência entre a conduta fraudulenta, o erro provocado, o comportamento da vítima e o resultado patrimonial.

Bitencourt (2012) também reconhece a fraude como elemento fundamental do delito e destaca a existência de uma relação causal entre o comportamento enganoso do agente, o erro da vítima e o resultado patrimonial. Para o autor, a vantagem ilícita precisa decorrer do erro provocado pelo próprio comportamento fraudulento.

Portanto, o estelionato não pode ser identificado apenas pela existência de prejuízo patrimonial. É necessário verificar se houve fraude anterior ou concomitante, se a vítima foi efetivamente induzida ou mantida em erro e se esse erro contribuiu para que o agente alcançasse a vantagem ilícita.

2.2 Fraude, erro da vítima, dolo e consumação

A fraude é o instrumento utilizado para criar uma falsa percepção da realidade. O artifício geralmente envolve recurso material ou encenação, enquanto o ardil corresponde à estratégia astuciosa utilizada para enganar a vítima. A expressão “qualquer outro meio fraudulento” permite abranger formas equivalentes que, embora não sejam expressamente descritas, possuam capacidade para induzir alguém em erro.

Cunha (2024) ressalta que o meio empregado deve possuir capacidade concreta de enganar, analisada conforme o contexto, as informações disponíveis e as características da vítima. Isso significa que a fraude deve ser examinada de acordo com as circunstâncias do caso, não sendo suficiente a intenção abstrata do agente de enganar.

O erro pode ser criado pelo próprio agente ou apenas mantido. Nos golpes eletrônicos, informações verdadeiras e falsas são frequentemente combinadas. O criminoso pode conhecer o nome de um familiar, utilizar a identidade visual de um banco ou mencionar dados de uma compra realizada pela vítima. Essa combinação reforça a aparência de

legitimidade e influencia a pessoa a fornecer credenciais ou realizar uma transferência.

O elemento subjetivo é o dolo dirigido à obtenção de vantagem ilícita. O estelionato consuma-se quando a vantagem ingressa na esfera de disponibilidade do agente e se produz o correspondente prejuízo patrimonial. Greco sintetiza esse entendimento da seguinte maneira:

Há necessidade, para efeitos de reconhecimento de consumação do estelionato, da afirmação do binômio vantagem ilícita/prejuízo alheio. (GRECO, 2010, p. 488).

A tentativa é possível quando a execução é iniciada, mas o resultado não ocorre por circunstâncias alheias à vontade do agente. Isso acontece, por exemplo, quando a vítima percebe o golpe antes de realizar o pagamento ou quando a instituição financeira bloqueia preventivamente a operação.

A velocidade das transferências realizadas pelo PIX intensifica o problema. Os valores podem ser enviados, fracionados e encaminhados sucessivamente a contas de passagem antes da atuação policial ou bancária, dificultando a recuperação do dinheiro e a identificação dos responsáveis.

3 FRAUDES ELETRÔNICAS E A LEI Nº 14.155/2021

3.1 Transformação das fraudes no ambiente digital

A tecnologia não eliminou a estrutura tradicional do estelionato, mas ampliou sua escala, velocidade, alcance territorial e capacidade de simulação. Perfis, números telefônicos e páginas podem ser criados com baixo custo, enquanto dados expostos nas redes sociais ajudam a personalizar as abordagens realizadas pelos criminosos.

O delito deixou de depender da presença física do autor e passou a atingir simultaneamente grande quantidade de pessoas. A facilidade de criação de perfis e páginas digitais permite

que os criminosos construam identidades aparentemente legítimas. Fotografias, nomes, logotipos de empresas e informações publicamente disponíveis são utilizados para convencer a vítima de que está mantendo contato com uma pessoa ou instituição verdadeira.

Entre as modalidades recorrentes encontra-se o *phishing*, caracterizado pelo envio de mensagens ou pela criação de páginas falsas destinadas à obtenção de informações pessoais, credenciais de acesso e dados financeiros. O criminoso reproduz a aparência de uma empresa ou instituição legítima e induz o usuário a inserir suas informações.

Outra prática frequente é o golpe do falso familiar pelo WhatsApp. O agente utiliza fotografia e nome de determinada pessoa e entra em contato com familiares ou conhecidos solicitando transferências. A confiança previamente existente entre a vítima e a pessoa cuja identidade foi utilizada torna-se o principal instrumento da fraude.

Também são recorrentes os golpes da falsa central bancária. Os criminosos entram em contato informando uma suposta movimentação irregular na conta e solicitam procedimentos destinados, teoricamente, ao bloqueio da operação. Na realidade, as orientações podem possibilitar transferências, contratação de empréstimos ou obtenção das credenciais bancárias da vítima.

Existem, ainda, fraudes relacionadas a boletos adulterados, anúncios e lojas inexistentes, falsas oportunidades de emprego ou investimento e relacionamentos afetivos. Em todas essas modalidades, o agente explora a confiança, a urgência, o medo ou a expectativa de ganho para reduzir a capacidade de verificação da vítima.

3.2 Conteúdo e alcance da Lei nº 14.155/2021

A Lei nº 14.155/2021 inseriu o § 2º-A no artigo 171 do Código Penal. A fraude eletrônica passou a ser punida com reclusão de quatro a oito anos e multa quando praticada mediante informações fornecidas pela vítima ou por terceiro induzido em erro por meio de redes

sociais, contatos telefônicos, envio de correio eletrônico fraudulento ou qualquer outro meio fraudulento análogo.

A pena é mais elevada do que aquela prevista para o estelionato simples, cuja sanção corresponde à reclusão de um a cinco anos e multa. O agravamento foi justificado pela maior capacidade de alcance das fraudes eletrônicas, pela rapidez das operações financeiras e pelas dificuldades enfrentadas na identificação dos autores.

O § 2º-B do artigo 171 prevê aumento da pena quando o crime utiliza servidor mantido fora do território nacional. A aplicação do aumento deve considerar a relevância do resultado gravoso. O § 4º estabelece tratamento agravado quando a vítima é idosa ou vulnerável, considerando a importância do prejuízo sofrido.

A mesma lei incluiu no artigo 155 do Código Penal o furto mediante fraude cometido por dispositivo eletrônico ou informático. Também acrescentou o § 4º ao artigo 70 do Código de Processo Penal. Nos estelionatos praticados mediante depósito, emissão de cheque sem fundos ou com pagamento frustrado e transferência de valores, a competência passou a ser definida pelo domicílio da vítima. Havendo várias vítimas, a competência é estabelecida pela prevenção.

A alteração buscou reduzir controvérsias e facilitar o acesso da vítima à persecução penal. Antes da reforma, existiam divergências sobre a definição do local de consumação do estelionato praticado mediante transferências bancárias. A nova regra aproxima o processo do domicílio da pessoa prejudicada nas situações expressamente previstas.

3.3 Dados estatísticos entre 2020 e 2025

A expansão das fraudes coincide com a intensificação do uso de serviços digitais durante e após a pandemia. As séries do Fórum Brasileiro de Segurança Pública indicam crescimento significativo dos registros gerais de estelionato e aumento específico das ocorrências

eletrônicas.

A categoria “estelionato por meio eletrônico” não foi informada de maneira uniforme por todas as unidades federativas em todos os anos. Por esse motivo, a comparação deve considerar alterações na forma de registro, na cobertura estatística e na classificação policial.

Em 2020, durante a pandemia, verificou-se uma forte aceleração das ocorrências de estelionato, influenciada pela ampliação das compras on-line, dos serviços bancários digitais e da comunicação realizada por aplicativos. Em 2021, foram consolidados 120.470 registros de estelionato eletrônico.

Em 2022, foram contabilizados 200.322 registros, representando aumento de 65,2% em comparação com o ano anterior. Em 2023, o Brasil registrou aproximadamente dois milhões de estelionatos, dos quais cerca de 223 mil foram classificados como eletrônicos.

De acordo com a série atualizada pelo Fórum Brasileiro de Segurança Pública, em 2024 foram registrados 2.193.122 estelionatos e 286.226 estelionatos eletrônicos. Em 2025, o número total chegou a 2.261.055 registros, enquanto as ocorrências eletrônicas alcançaram 346.753, representando aumento de 20,6% nessa categoria específica.

Os dados demonstram uma profunda modificação na criminalidade patrimonial brasileira. Os meios digitais passaram a ocupar posição central nas estratégias utilizadas pelos criminosos, substituindo ou complementando práticas patrimoniais tradicionalmente executadas mediante contato presencial.

Esses números, contudo, não medem diretamente a eficácia da Lei nº 14.155/2021. O aumento pode decorrer simultaneamente da maior incidência, da intensificação das relações econômicas digitais, do crescimento das denúncias e do aperfeiçoamento da classificação policial.

Apesar dessas limitações, a persistência de centenas de milhares de ocorrências demonstra que o agravamento penal, isoladamente, não produziu contenção suficiente das fraudes eletrônicas. A análise estatística reforça a necessidade de combinar a legislação com medidas preventivas, investigativas e tecnológicas.

3.4 Análise crítica da Lei nº 14.155/2021

A Lei nº 14.155/2021 apresenta importantes aspectos positivos. Em primeiro lugar, reconhece que a fraude eletrônica possui capacidade de atingir grande quantidade de vítimas e dificultar a investigação. Em segundo lugar, fornece uma descrição mais específica para as condutas praticadas por redes sociais, telefone, correio eletrônico e meios semelhantes. Em terceiro lugar, altera a competência em hipóteses de transferência de valores, aproximando o processo do domicílio da vítima.

Apesar desses avanços, a principal lacuna da reforma está no predomínio da resposta punitiva. A elevação da pena modifica a consequência jurídica depois da prática do delito, mas não impede o uso de contas bancárias pertencentes a terceiros, a engenharia social, a circulação rápida do dinheiro ou a ocultação da identidade do criminoso.

A efetividade da legislação depende da probabilidade de identificação e responsabilização do autor, e não apenas da pena abstratamente prevista. Sem integração de dados, equipes especializadas e preservação tempestiva dos registros, a ameaça penal perde parte de sua capacidade preventiva.

Também existem desafios interpretativos. A expressão “qualquer outro meio fraudulento análogo” permite que a norma acompanhe o surgimento de novas tecnologias, mas exige cuidado com os princípios da legalidade e da taxatividade. Nem toda fraude que utiliza celular ou internet se enquadra automaticamente no § 2º-A do artigo 171.

É necessário demonstrar que o erro foi produzido mediante informações fornecidas pela

vítima ou por terceiro induzido em erro por meio dos canais descritos na legislação ou de mecanismo funcionalmente equivalente. Caso contrário, pode incidir o tipo básico do estelionato ou outra figura penal.

Outro problema relevante é a fronteira entre o estelionato eletrônico e o furto mediante fraude eletrônica. A classificação depende da participação da vítima no ato de disposição patrimonial. A semelhança tecnológica entre as condutas não substitui a análise da forma como os valores foram obtidos.

A aplicação inconsistente da norma pode gerar conflitos de competência, respostas penais diferentes para situações semelhantes e insegurança jurídica. Por isso, a autoridade deve reconstruir detalhadamente a sequência dos fatos antes de definir o enquadramento penal.

A Lei nº 14.155/2021 pode ser considerada parcialmente eficaz. A norma aperfeiçoa a proteção penal e facilita o enquadramento de golpes comuns, mas não supera isoladamente as limitações operacionais. Sua avaliação deve considerar não apenas o número de registros, mas também os índices de esclarecimento, condenação, tempo de resposta, bloqueio e recuperação dos valores.

4 DISTINÇÃO ENTRE ESTELIONATO ELETRÔNICO E FURTO MEDIANTE FRAUDE

A utilização de tecnologia não determina, isoladamente, a classificação jurídica da conduta. No furto mediante fraude, o engano reduz a vigilância da vítima ou permite ao agente subtrair o bem sem um ato consciente de entrega. No estelionato, a fraude vicia a vontade e leva a própria vítima a realizar o ato de disposição patrimonial.

Bitencourt (2024) e Cunha (2024) adotam esse critério como elemento central da distinção. No furto mediante fraude, a vontade da vítima não participa diretamente da transferência do bem. No estelionato, embora enganada, a pessoa entrega o bem ou realiza a operação patrimonial.

Se a vítima recebe uma mensagem falsa e, acreditando falar com um familiar, realiza espontaneamente um PIX, a estrutura aproxima-se do estelionato eletrônico. Nesse caso, o comportamento da vítima, embora influenciado pelo erro, participa diretamente da transferência.

Por outro lado, se o agente invade ou manipula o dispositivo e transfere os valores sem a participação voluntária da vítima, o fato pode configurar furto mediante fraude eletrônica. Dependendo das circunstâncias, também deve ser analisada a ocorrência de invasão de dispositivo informático ou de concurso de crimes.

A distinção produz efeitos relevantes quanto à pena, à competência, à ação penal e à descrição da imputação. A autoridade deve reconstruir a sequência dos fatos, identificando quem iniciou a operação, de onde partiram as credenciais, se houve fornecimento de informações, qual foi a atuação da vítima e em que momento ocorreu o prejuízo.

A prova técnica deve complementar, e não substituir, a análise dos elementos do tipo penal. A existência de uma transferência digital não permite concluir automaticamente pela ocorrência de furto ou estelionato. O enquadramento depende do modo concreto de execução.

5 JURISPRUDÊNCIA RECENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA

5.1 Competência territorial e local do prejuízo

No Conflito de Competência nº 185.983/DF, julgado em 2022, a Terceira Seção do Superior Tribunal de Justiça esclareceu que a alteração do artigo 70, § 4º, do Código de Processo Penal incide apenas nas hipóteses expressamente previstas, como os estelionatos praticados mediante depósito ou transferência de valores.

Fora dessas situações, permanece a regra geral de competência baseada no local da consumação da infração. O precedente é relevante porque evita a aplicação indistinta do

domicílio da vítima a toda forma de estelionato e evidencia que a Lei nº 14.155/2021 solucionou apenas parte das controvérsias territoriais (BRASIL, STJ, 2022).

A orientação também revela um efeito prático positivo. Nos golpes em que a vítima realiza transferência de valores, o processamento no local de seu domicílio reduz dificuldades de acesso e deslocamento. Nos casos com várias vítimas, entretanto, a prevenção concentra a competência, exigindo coordenação entre investigações iniciadas em diferentes localidades.

5.2 WhatsApp, PIX e responsabilidade das instituições financeiras

Embora a responsabilidade civil das instituições financeiras não substitua a responsabilização penal do autor, a jurisprudência oferece elementos importantes sobre a prevenção das fraudes eletrônicas.

No Recurso Especial nº 2.124.423/SP, julgado em 20 de agosto de 2024, o STJ entendeu que a responsabilização da instituição que mantém a conta utilizada no golpe exige demonstração de falta de diligência na abertura, manutenção ou fiscalização da conta. O simples uso criminoso de uma conta bancária não produz responsabilidade automática da instituição (BRASIL, STJ, 2024).

Em outra direção, ao examinar situações nas quais as operações destoam do perfil do consumidor, o STJ reconheceu que a ausência de mecanismos adequados de detecção e bloqueio pode caracterizar defeito na prestação do serviço.

No Recurso Especial nº 2.220.333/DF, a Terceira Turma afastou a alegação de culpa concorrente quando a falha de segurança bancária contribuiu decisivamente para o dano sofrido pelo consumidor (BRASIL, STJ, 2025a).

O conjunto dos julgados demonstra que a solução depende das provas produzidas em cada processo. Devem ser analisados o perfil transacional da vítima, a sequência das operações, os mecanismos de autenticação, os alertas emitidos e as providências adotadas após a

comunicação da fraude.

No Agravo Interno no Recurso Especial nº 2.209.954/SP, relativo a fraude praticada por WhatsApp e depósitos realizados via PIX para conta de terceiro, o STJ manteve a conclusão fundamentada na culpa exclusiva da vítima porque a modificação do entendimento exigiria reexame de provas (BRASIL, STJ, 2025b).

Os precedentes não estabelecem uma regra automática favorável ou contrária às instituições financeiras. Eles indicam que a responsabilidade depende do nexo entre a fraude e uma eventual falha concreta na prestação do serviço.

5.3 Limites temporais e tipicidade

A qualificadora introduzida pela Lei nº 14.155/2021 não pode retroagir para prejudicar fatos praticados antes de sua entrada em vigor, conforme o artigo 5º, inciso XL, da Constituição Federal. Para os fatos posteriores, a acusação deve demonstrar os elementos específicos do § 2º-A do artigo 171, não sendo suficiente afirmar genericamente que houve utilização de tecnologia.

Essa exigência preserva o princípio da legalidade e impede que qualquer estelionato com comunicação digital seja automaticamente submetido à pena mais grave. O simples uso de um aparelho celular ou aplicativo não dispensa a demonstração do meio fraudulento e de sua relação com o erro da vítima.

A jurisprudência atualizada confirma duas conclusões críticas. A primeira é que a reforma possui aplicação delimitada pelos elementos descritos na legislação. A segunda é que a resposta aos golpes depende da reconstrução probatória do caso.

O avanço legislativo, portanto, precisa ser acompanhado por decisões coerentes e pela capacidade institucional de produzir provas digitais confiáveis. A utilização imprecisa da qualificadora pode violar a legalidade e comprometer a legitimidade da responsabilização

penal.

6 INVESTIGAÇÃO, PROVA DIGITAL E RESPONSABILIZAÇÃO PENAL

A investigação das fraudes eletrônicas enfrenta obstáculos relacionados à distância entre o autor e a vítima, ao uso de contas de passagem, aos números telefônicos cadastrados em nome de terceiros, aos perfis falsos e aos serviços mantidos em diferentes jurisdições.

A fragmentação das informações entre bancos, plataformas digitais, operadoras de telefonia e órgãos policiais pode fazer com que registros relevantes desapareçam antes da expedição das ordens necessárias. A investigação exige atuação rápida e cooperação entre instituições públicas e privadas.

Conversas realizadas em aplicativos, registros de acesso, comprovantes de transferência, metadados, arquivos e dados de localização podem contribuir para a identificação dos responsáveis. A captura de tela isolada, entretanto, nem sempre demonstra a autoria ou a integridade do conteúdo apresentado.

É necessário preservar o dispositivo e documentar a origem, a coleta, o armazenamento, a extração e a análise das informações. Esses procedimentos devem observar a cadeia de custódia prevista nos artigos 158-A a 158-F do Código de Processo Penal.

A cadeia de custódia representa o conjunto dos procedimentos utilizados para manter e documentar a história cronológica do vestígio. No ambiente digital, pequenas alterações podem comprometer informações relevantes, tornando indispensável a utilização de técnicas adequadas para garantir a autenticidade e a confiabilidade da prova.

Nucci (2024) ressalta que a responsabilização exige correspondência entre o fato praticado e os elementos do tipo penal. No ambiente digital, esse dever impede que a autoria seja inferida exclusivamente porque determinada conta recebeu valores provenientes da fraude.

É necessário investigar quem controlava a conta, qual era o conhecimento do titular, se houve participação consciente, cessão deliberada, utilização indevida dos dados pessoais ou eventual lavagem de capitais. A condição de titular formal da conta não demonstra, isoladamente, a autoria do estelionato.

A cooperação institucional deve ser célere e proporcional, respeitando a reserva de jurisdição, a intimidade, a proteção de dados e o direito de defesa. O combate aos crimes eletrônicos não autoriza o afastamento dos princípios da legalidade e da autenticidade.

Ao contrário, a facilidade de alteração dos dados digitais exige documentação técnica mais rigorosa. A prova obtida sem preservação adequada pode perder confiabilidade e comprometer a responsabilização dos verdadeiros autores.

7 COMPARAÇÃO COM LEGISLAÇÕES ESTRANGEIRAS

7.1 Estados Unidos

Nos Estados Unidos, o *Computer Fraud and Abuse Act*, incorporado ao 18 U.S.C. § 1030, concentra-se no acesso não autorizado ou no excesso de autorização em computadores protegidos. A legislação abrange hipóteses de obtenção de informações e de vantagem mediante fraude.

Os golpes eletrônicos também podem ser alcançados por outros tipos federais, como o *wire fraud*. O modelo norte-americano é fragmentado de acordo com a conduta e com a dimensão interestadual ou federal do caso, diferentemente do Brasil, que inseriu uma qualificadora específica dentro do crime patrimonial de estelionato (UNITED STATES, 2026).

A comparação demonstra que o § 1030 é mais diretamente voltado à violação ou utilização indevida de sistemas informáticos. O artigo 171, § 2º-A, do Código Penal brasileiro pode incidir mesmo sem a invasão de um dispositivo, quando a própria vítima fornece informações ou realiza o pagamento por ter sido enganada.

A experiência norte-americana reforça a necessidade de distinguir a fraude praticada por engenharia social do acesso indevido a sistemas. Na engenharia social, o criminoso manipula psicologicamente a vítima para obter informações ou valores. Na invasão, o agente supera ou viola mecanismos de acesso ao sistema.

7.2 União Europeia

A Diretiva 2013/40/UE estabelece regras mínimas sobre ataques contra sistemas de informação. O documento orienta a criminalização do acesso ilegal, da interferência em sistemas e dados e da utilização de instrumentos destinados à prática desses ataques.

A norma também procura facilitar a prevenção e melhorar a cooperação entre autoridades judiciais e outras instituições competentes. A natureza transnacional dos delitos eletrônicos exige mecanismos rápidos de intercâmbio de informações e preservação de provas.

A Diretiva 2019/713 trata especificamente da fraude e da falsificação relacionadas a meios de pagamento que não utilizam dinheiro físico. A norma abrange instrumentos materiais e digitais e reforça a cooperação e a assistência entre autoridades dos Estados integrantes da União Europeia (UNIÃO EUROPEIA, 2013; 2019).

O modelo europeu separa com maior clareza os ataques contra a integridade dos sistemas e as fraudes relacionadas aos meios de pagamento. O Brasil possui tipos penais capazes de alcançar ambas as categorias, especialmente os artigos 154-A, 155, § 4º-B, e 171, § 2º-A, do Código Penal.

Apesar disso, o sistema brasileiro ainda enfrenta fragmentação investigativa, dificuldades de cooperação e ausência de indicadores nacionais uniformes sobre a resposta penal, o esclarecimento dos casos e a recuperação dos valores.

7.3 Contribuições da comparação

A comparação com legislações estrangeiras não autoriza a aplicação automática de regras de outros países no Brasil. Ela evidencia, entretanto, três caminhos relevantes para o aperfeiçoamento da política nacional de enfrentamento às fraudes eletrônicas.

O primeiro consiste em separar conceitualmente a invasão de sistemas e a engenharia social. O segundo envolve o fortalecimento de pontos permanentes de cooperação entre autoridades. O terceiro corresponde à integração entre a proteção penal e as regras de segurança dos meios de pagamento.

A experiência estrangeira confirma que a tipificação penal é apenas um componente de uma política mais ampla. A prevenção, a investigação, a cooperação internacional e a segurança tecnológica possuem importância equivalente para a redução dos delitos.

8 PREVENÇÃO E DESAFIOS PARA O ENFRENTAMENTO DAS FRAUDES ELETRÔNICAS

O enfrentamento das fraudes eletrônicas não pode ficar restrito ao aumento das penas. Masson (2024) destaca que o Direito Penal deve atuar de maneira subsidiária e dentro dos limites constitucionais. Sua utilização não elimina a necessidade de políticas preventivas e de segurança.

A prevenção exige educação digital, comunicação clara, autenticação segura, monitoramento das transações incompatíveis com o perfil do usuário e canais rápidos para bloqueio e contestação de operações.

As instituições financeiras devem conhecer seus clientes, identificar contas utilizadas repetidamente para recepção e dispersão de valores e adotar barreiras proporcionais ao risco. Movimentações muito diferentes do comportamento habitual do consumidor devem receber análise e confirmação adicionais.

As plataformas digitais e as operadoras de telefonia podem aperfeiçoar os mecanismos de verificação de identidade, denúncia, preservação de registros e resposta às ordens legais.

Essas medidas devem observar a proteção de dados e a transparência, evitando transferir integralmente à vítima o custo da segurança.

O Estado deve investir em delegacias e perícias especializadas, protocolos nacionais, capacitação profissional e cooperação interestadual e internacional. A velocidade das mudanças tecnológicas exige atualização constante dos agentes responsáveis pela investigação e aplicação da lei.

Também é necessário padronizar os registros de estelionato eletrônico e divulgar dados relacionados às taxas de esclarecimento, condenação e recuperação de valores. Sem esses indicadores, a eficácia da legislação é medida principalmente pelo número de ocorrências, que não representa todo o funcionamento do sistema de justiça criminal.

A educação digital deve priorizar os grupos mais expostos, mas sem culpabilizar as vítimas. Mensagens que apresentam situações de urgência devem ser confirmadas por canal independente. Senhas e códigos de segurança não devem ser compartilhados, enquanto links, destinatários e beneficiários precisam ser verificados antes da realização de pagamentos.

Os incidentes devem ser comunicados rapidamente à instituição financeira e à autoridade policial. Essas providências podem aumentar a possibilidade de bloqueio dos valores e preservação dos registros eletrônicos.

As medidas preventivas reduzem as oportunidades de atuação dos criminosos, mas não afastam o dever dos prestadores de manter sistemas seguros. A proteção exige responsabilidade compartilhada entre Estado, empresas, instituições financeiras e usuários.

9 CONSIDERAÇÕES FINAIS

A pesquisa demonstrou que o estelionato mantém seus elementos tradicionais, mas adquiriu maior escala, velocidade e complexidade no ambiente digital. A Lei nº 14.155/2021

representou avanço ao conferir tratamento penal específico à fraude eletrônica e ao disciplinar aspectos relacionados ao furto eletrônico e à competência territorial, sem eliminar, contudo, os desafios de enquadramento jurídico e produção probatória.

Os dados analisados entre 2020 e 2025 evidenciam a elevada dimensão social das fraudes eletrônicas, embora devam ser interpretados considerando a subnotificação e as diferenças de classificação policial. A jurisprudência examinada também demonstra que a solução dos casos depende das circunstâncias concretas, especialmente da forma de transferência dos valores, da participação da vítima e da existência de falha efetiva nos mecanismos de segurança.

Em resposta ao problema de pesquisa, conclui-se que a legislação penal brasileira oferece instrumentos relevantes, porém de eficácia prática parcial. O enfrentamento do fenômeno exige que a aplicação da lei seja acompanhada de investigação especializada, preservação adequada da prova digital, mecanismos de bloqueio e recuperação de ativos, cooperação institucional e medidas de prevenção e educação digital.

Assim, a proteção penal deve integrar uma política mais ampla de segurança no ambiente digital, sem afastar os princípios da legalidade, da taxatividade, do devido processo legal e das demais garantias fundamentais. A efetividade da resposta estatal depende menos do simples aumento da pena abstrata e mais da capacidade de prevenir os golpes, identificar seus autores e produzir provas confiáveis para a responsabilização.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Código Penal comentado**. 7. ed. São Paulo: Saraiva, 2012.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial: crimes contra o patrimônio**. São Paulo: SaraivaJur, 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF:

Presidência da República, 1988.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, RJ, 1940.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ, 1941.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF, 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF, 2018.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal e o Código de Processo Penal para tornar mais graves crimes cometidos de forma eletrônica ou pela internet. Brasília, DF, 2021.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência nº 185.983/DF. Relator: Ministro Joel Ilan Paciornik, Terceira Seção, julgado em 11 maio 2022, Dje 13 maio 2022. Brasília, DF: STJ, 2022.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2.124.423/SP. Relatora: Ministra Nancy Andrichi, Terceira Turma, julgado em 20 ago. 2024, Dje 27 ago. 2024. Brasília, DF: STJ, 2024.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2.220.333/DF. Relator: Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 7 out. 2025, DJEN 13 out. 2025. Brasília, DF: STJ, 2025a.

BRASIL. Superior Tribunal de Justiça. Agravo Interno no Recurso Especial nº 2.209.954/SP. Relatora: Ministra Maria Isabel Gallotti, Quarta Turma, sessão virtual de 9 a 15 set. 2025, DJe 18 set. 2025. Brasília, DF: STJ, 2025b.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial (arts. 121 ao 361)**. Salvador: JusPodivm, 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2023.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **20º Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2026.

GRECO, Rogério. **Código Penal comentado**. 4. ed. Niterói: Impetus, 2010.

GRECO, Rogério. **Código Penal comentado**. 9. ed. Niterói: Impetus, 2015.

MASSON, Cleber. **Direito penal: parte especial**. São Paulo: Método, 2024.

NUCCI, Guilherme de Souza. **Código Penal comentado**. Rio de Janeiro: Forense, 2024.

UNIÃO EUROPEIA. **Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013**, relativa a ataques contra os sistemas de informação. Jornal Oficial da União Europeia, L 218, 14 ago. 2013.

UNIÃO EUROPEIA. **Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de**

17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário. Jornal Oficial da União Europeia, L 123, 10 maio 2019.

UNITED STATES. **United States Code. Title 18, § 1030: Fraud and related activity in connection with computers.** Washington, DC, 2026.