

ESTELIONATO DIGITAL NO BRASIL: ENTRE A RACIONALIDADE CRIMINOSA E A FRAGILIDADE DO ESTADO

DIGITAL FRAUD IN BRAZIL: BETWEEN CRIMINAL RATIONALITY AND THE FRAGILITY OF THE STATE

Clodoaldo Matias da Silva

Mestrando em Antropologia Social

Instituição: Universidade Federal do Amazonas (UFAM)

Endereço: Manaus – Amazonas, Brasil

Orcid: <https://orcid.org/0000-0002-3923-8839>

E-mail: cms.1978@hotmail.com

Cláudio Sérgio Matias da Silva

Especialista em Leitura e Produção Textual

Instituição: Instituto Federal de Educação, Ciência e Tecnologia do Amazona (IFAM)

Endereço: Manaus – Amazonas, Brasil

Orcid: <https://orcid.org/0000-0002-8388-9209>

E-mail: clawdiosilva@gmail.com

Maria das Graças Maciel de Oliveira

Mestre em Ciência da Educação

Instituição: Universidad Del Norte (UNINORTE)

Endereço: Assunção, Paraguai

Orcid: <https://orcid.org/0009-0009-1529-9950>

E-mail: educadoragracamaci@gmail.com

RESUMO

O presente artigo analisa o estelionato digital à luz da Teoria Econômica do Crime, considerando sua estrutura racional, recorrência prática e os limites do sistema penal brasileiro. Parte-se da hipótese de que o agente infrator age com base em cálculos utilitários de custo e benefício, aproveitando-se da fragilidade normativa e institucional para obter vantagem ilícita com reduzido risco de punição. A pesquisa tem como objetivo examinar a dinâmica criminosa do estelionato virtual, sua tipologia e os mecanismos jurídicos existentes, a fim de avaliar se a resposta estatal é compatível com a complexidade da prática delitiva. A metodologia adotada consiste em revisão bibliográfica e análise crítica da legislação penal vigente, com base em autores clássicos e contemporâneos da criminologia econômica. A discussão percorre três eixos: fundamentos teóricos da racionalidade criminosa, evolução legislativa do estelionato digital e implicações jurídicas do crime como empreendimento reiterado. Os resultados indicam que a racionalidade do agente é favorecida pela ineficácia das políticas penais, morosidade processual, penas brandas e ausência de dissuasão real. Conclui-se que a permanência do estelionato digital está diretamente relacionada à lógica de impunidade, à ausência de responsabilização empresarial e à falta de um modelo repressivo integrado. Propõe-se, ao final, o fortalecimento legislativo, a reestruturação das práticas investigativas e o investimento em

mecanismos de prevenção e repressão coordenada como alternativas para conter a expansão desse crime no Brasil.

Palavras-chave: cibercrime, direito penal, estelionato, racionalidade, responsabilidade estatal.

ABSTRACT

This article examines digital fraud in Brazil through the lens of the Economic Theory of Crime, focusing on its rational structure, repeated occurrence, and the limitations of the national criminal justice system. It is based on the hypothesis that offenders act according to a utilitarian calculation of cost and benefit, taking advantage of legal and institutional weaknesses to obtain illicit gain with minimal risk of punishment. The aim is to investigate the criminal dynamics of digital fraud, its typology, and the legal mechanisms in place, in order to assess whether the state's response is adequate to the complexity of the offence. The methodology adopted involves a bibliographic review and critical analysis of current criminal legislation, supported by both classical and contemporary authors in economic criminology. The discussion is structured around three axes: theoretical foundations of criminal rationality, legislative evolution of digital fraud, and legal implications of crime as a repeated enterprise. The findings indicate that the offender's rationality is reinforced by ineffective penal policies, procedural delays, lenient sentencing, and lack of real deterrence. It concludes that the persistence of digital fraud is directly linked to a logic of impunity, lack of corporate accountability, and the absence of an integrated repressive model. The article proposes strengthening legislation, restructuring investigative practices, and investing in coordinated mechanisms of prevention and repression as necessary measures to curb the expansion of this crime in Brazil.

Keywords: criminal rationality, cybercrime, digital fraud, penal law, state accountability.

1 INTRODUÇÃO

A criminalidade digital tem se intensificado nas últimas décadas, acompanhando a expansão das tecnologias de informação e comunicação, entre os delitos mais recorrentes no ciberespaço, destaca-se o estelionato digital, prática que combina fraude, simulação e induzimento ao erro para obtenção de vantagem ilícita. A sofisticação dos meios utilizados pelos agentes, aliada à baixa efetividade das respostas estatais, transforma o ambiente virtual em espaço fértil para condutas delitivas, essa nova realidade desafia os instrumentos tradicionais do Direito Penal, exigindo análise crítica das causas e implicações do fenômeno, nesse contexto, compreende-se o estelionato digital como reflexo direto da racionalidade criminoso diante da fragilidade institucional.

Partindo desse cenário, questiona-se: Por que o estelionato digital tem se expandido de forma significativa no Brasil, mesmo após avanços legislativos e tecnológicos? A pergunta exige reflexão sobre os incentivos que sustentam a prática e as falhas que comprometem a

repressão penal. A partir de uma perspectiva teórico-crítica, o estudo propõe uma leitura do crime como resultado de escolhas racionais por parte dos infratores, nesse sentido, as condutas não são aleatórias, mas fruto de estratégias que avaliam riscos, ganhos e lacunas jurídicas, essa análise da legislação penal e da atuação estatal se torna, portanto, essencial para a compreensão do problema.

O objetivo principal desta pesquisa é analisar o estelionato digital como prática racionalmente estruturada, à luz da Teoria Econômica do Crime, e identificar os fatores que fragilizam o enfrentamento penal no contexto brasileiro, busca-se compreender de que forma as normas jurídicas, os procedimentos processuais e as limitações investigativas contribuem para a permanência e expansão do delito. Para tanto, articula-se a análise doutrinária com a legislação vigente, especialmente o Código Penal e as reformas promovidas pela Lei nº 14.155/2021, o estudo também considera os impactos processuais advindos do Pacote Anticrime (Lei nº 13.964/2019), que alterou a natureza da ação penal no estelionato.

A escolha do tema justifica-se pela urgência do debate sobre o papel do Estado na repressão a delitos que envolvem tecnologia, anonimato e grande alcance social, essa racionalidade do infrator, ao se apoiar na ineficiência institucional, revela falhas que vão além do sistema jurídico e atingem a confiança pública. O estelionato digital, ao contrário do crime violento, se dissimula, se adapta e se repete com facilidade, isso porque, a legislação, muitas vezes reativa e fragmentada, carece de instrumentos eficazes para prevenir, investigar e punir com a agilidade exigida pelas dinâmicas contemporâneas, nesse aspecto, a pesquisa busca contribuir com uma abordagem crítica e propositiva.

Do ponto de vista social, o tema assume relevância por afetar diretamente a segurança patrimonial, a integridade dos dados pessoais e a confiança nas instituições, no plano jurídico, a análise do estelionato digital exige revisão de conceitos tradicionais e atualização de mecanismos legais e processuais. A incapacidade do sistema penal de acompanhar as transformações tecnológicas compromete sua função preventiva e punitiva, assim, compreender os limites e possibilidades da atuação estatal diante da lógica racional da criminalidade digital é essencial para o fortalecimento do Estado de Direito, o problema, mais do que normativo, é estrutural e requer soluções integradas.

Os resultados da pesquisa indicam que o estelionato digital se consolida como uma conduta economicamente vantajosa em razão de falhas normativas, baixa taxa de

responsabilização e ausência de resposta célere por parte do sistema de justiça criminal, constatou-se que, mesmo após a reforma legislativa, os mecanismos de repressão continuam aquém da sofisticação da prática delitiva. A racionalidade do agente infrator não encontra contraponto eficiente nas políticas públicas penais, com isso, o estudo conclui pela necessidade de reformulação legislativa, fortalecimento investigativo e integração institucional como caminhos para o enfrentamento efetivo do estelionato digital no Brasil.

2 A TEORIA ECONÔMICA DO CRIME: FUNDAMENTOS, EVOLUÇÃO E APLICAÇÕES

A Teoria Econômica do Crime, proposta inicialmente por Gary Becker em 1968, estabeleceu um marco teórico na análise do comportamento delitivo como uma escolha racional baseada em cálculo utilitário, o agente infrator, nesse modelo, pondera os custos e benefícios esperados de sua conduta, decidindo cometer o crime se o ganho ilícito superar o risco de punição. Essa abordagem parte da premissa de que a criminalidade, sobretudo patrimonial, decorre de incentivos estruturais do próprio sistema jurídico e social, assim, crimes como o estelionato passam a ser vistos sob a ótica da lógica mercadológica, onde o “empreendimento criminoso” é racionalizado como atividade economicamente viável.

A teoria de Becker encontra respaldo nas ideias clássicas de Jeremy Bentham, que, ao formular o utilitarismo penal, já defendia a função preventiva da pena por meio do equilíbrio entre prazer e dor, para Bentham (1974), o indivíduo calcula os efeitos de sua conduta conforme a maximização do prazer e a minimização da dor, o que inspira um sistema penal dissuasório e proporcional. A pena justa seria aquela suficiente para desincentivar o crime, sem exceder a necessidade de contenção, tal raciocínio serviu como alicerce para o pensamento econômico do crime, consolidando a ideia de que o Estado deve aumentar os custos esperados da prática criminosa para impedir sua recorrência, assim, a punição eficiente se vincula diretamente à redução da vantagem ilícita esperada pelo infrator.

Em Becker e Landes (1974), observa-se o deslocamento da análise penal para o campo microeconômico, considerando o infrator um sujeito racional que responde a estímulos legais, sociais e econômicos, ao tratar o crime como escolha racional, os autores propõem que as decisões dos criminosos sejam afetadas pela probabilidade de punição, pela severidade da sanção e pela expectativa de lucro. Essa perspectiva levou à redefinição do papel do Direito

Penal, que deixa de ser apenas instrumento de retribuição moral, para atuar estrategicamente como ferramenta de gestão comportamental, sendo assim, a racionalidade passa, portanto, a ser um critério de mensuração de eficácia das normas penais, essa virada teórica permite compreender crimes como o estelionato digital sob um novo paradigma.

Ao aplicar esse modelo ao crime de estelionato, especialmente em sua forma digital, é possível identificar com nitidez os elementos do cálculo racional proposto por Becker, onde o agente infrator, ao se valer de meios virtuais, encontra baixo risco de identificação e punição, o que eleva a atratividade da conduta criminosa. Como observa Capez (2012), a fragilidade da resposta penal e a ineficácia da persecução criminal estimulam o comportamento ilícito reiterado, ademais, a morosidade judicial, somada à previsibilidade de penas brandas ou alternativas, contribui para o estímulo da delinquência econômica, nesse sentido, o sistema penal, ao invés de inibir, termina por fomentar condutas delituosas patrimoniais de natureza sofisticada.

Outro aspecto fundamental da Teoria Econômica do Crime está na noção de “dissuasão”, entendida como a função essencial do Direito Penal frente à criminalidade racional, quando o agente percebe que o custo potencial de sua ação supera os benefícios, ele tende a não delinquir. Greco (2011) salienta que, na ausência de instrumentos eficazes de repressão e punição, o sistema jurídico assume postura leniente que afeta diretamente a credibilidade das normas, nesse contexto, a lógica da dissuasão exige, portanto, eficiência investigativa, celeridade processual e proporcionalidade nas sanções aplicadas, assim, o Direito Penal passa a atuar como mecanismo de controle preventivo, voltado à racionalização do comportamento humano.

Nesse contexto, Albanese (2000) introduz o conceito de “empreendedorismo criminoso”, afirmando que, quando há falhas sistemáticas de controle, onde o indivíduo tende a profissionalizar sua atividade delitiva, nesse contexto, o crime deixa de ser episódico para assumir características de empreendimento contínuo, dotado de organização, estratégia e busca de lucro. Isso é particularmente observável em crimes como o estelionato digital, cuja repetição e complexidade demonstram planejamento e adaptação tecnológica, a atividade criminosa passa a seguir modelos empresariais, explorando brechas normativas e estruturais, assim, a compreensão econômica do crime se torna indispensável para o enfrentamento eficaz dessas práticas organizadas.

Para além da dissuasão, a Teoria Econômica também se apoia no conceito de “incapacitação”, que consiste em retirar o criminoso do “mercado delituoso” por meio de penas eficazes e desestimuladoras, isso implica repensar o regime de cumprimento de pena, a possibilidade de acordos processuais e a execução penal. A lógica beckeriana propõe que o Estado atue estrategicamente, retirando da sociedade aqueles agentes cujos comportamentos reiterados afetam a ordem econômica e social, na perspectiva de Greco (2011) a privação de liberdade, em casos de crimes reiterados e sofisticados como o estelionato digital, deve ser acompanhada de políticas que limitem o reingresso do infrator no circuito ilícito, essa atuação deve visar não apenas a punição, mas a desarticulação da lógica de lucro.

O ponto central dessa abordagem está no reconhecimento de que o crime é uma resposta racional às oportunidades permitidas pelo ordenamento, nesse sentido, a ausência de vigilância tecnológica, a fragilidade probatória e a ausência de penas rigorosas funcionam como incentivos indiretos à prática delituosa. Monteiro (2010) reforça que, sem políticas de *enforcement* e atualização legislativa, a criminalidade econômica tende à expansão, criando novos mercados ilícitos, isso se mostra ainda mais evidente no ambiente virtual, onde a fiscalização é limitada e as estruturas de anonimato ampliam a impunidade, nesse cenário, a Teoria Econômica do Crime, portanto, não apenas explica o fenômeno, mas aponta caminhos para sua contenção.

Contudo, é necessário reconhecer as limitações dessa teoria, especialmente em crimes que envolvem fatores sociais, emocionais ou psicológicos complexos, embora eficaz na análise de condutas patrimoniais racionais, como o estelionato, a teoria pode ser insuficiente diante de crimes passionais, culturais ou de subsistência. Ainda assim, sua aplicação em delitos como fraudes digitais é amplamente reconhecida pela doutrina contemporânea, justamente por seu enfoque na lógica de ganhos ilícitos, isso porque, a criminalidade moderna, ao incorporar tecnologias e estruturas de mercado, demanda respostas igualmente racionais e fundamentadas, essa compreensão do crime como escolha estratégica impõe ao Direito Penal a responsabilidade de se tornar mais eficiente e proativo.

Conclui-se, portanto, que a Teoria Econômica do Crime oferece uma chave interpretativa eficaz para compreender a lógica do estelionato na era digital, seu foco na racionalidade, na dissuasão e na incapacitação permite não apenas explicar a persistência desse delito, mas também propor políticas penais mais eficazes. Contudo, para que tais propostas

sejam aplicadas, é necessário entender como o estelionato digital se manifesta, quais são suas formas predominantes e como o ordenamento jurídico brasileiro tem respondido a essa nova realidade. É nesse sentido que se justifica a próxima seção deste trabalho, que tratará especificamente da evolução legislativa, tipificação e estratégias do estelionato digital no Brasil.

3 ESTELIONATO DIGITAL NO BRASIL: EVOLUÇÃO, TIPOLOGIA E LEGISLAÇÃO

Diante das transformações impostas pela era digital, o crime de estelionato passou por relevantes alterações em sua execução e na forma como se apresenta perante o ordenamento jurídico, sob essa perspectiva, torna-se imprescindível analisar as adaptações normativas e interpretativas que buscam responder à nova realidade criminosa. A fraude, elemento central do tipo penal previsto no art. 171 do Código Penal, ganhou contornos tecnológicos que exigem releituras doutrinárias e jurisprudenciais (Brasil, 1940), nesse contexto, a criminalidade migrada para o ambiente virtual revela a fragilidade dos instrumentos legais tradicionais.

Com efeito, a Lei nº 14.155/2021 representou um marco normativo ao modificar o Código Penal, agravando a pena do estelionato praticado por meio eletrônico (Brasil, 2021), essa alteração legislativa foi resultado direto da intensificação dos golpes cometidos por meio de redes sociais, aplicativos de mensagens e plataformas de comércio digital. Conforme esclarecem Barata e Andrade Filho (2023), o uso de tecnologias emergentes ampliou o alcance das condutas fraudulentas, tornando a fraude virtual um dos delitos patrimoniais mais recorrentes da contemporaneidade, dessa forma, o legislador buscou adequar a resposta penal à gravidade dos fatos e à sofisticação dos meios empregados.

Convém destacar que, sob a ótica jurídica, o estelionato digital guarda os mesmos elementos estruturais do tipo penal clássico: vantagem ilícita, prejuízo alheio, erro da vítima e emprego de ardil. No entanto, a forma de execução se complexifica com o uso de tecnologias, exigindo do intérprete atenção aos meios com que se dá o engano. Como afirma Greco (2011), o estelionatário digital não atua mais de forma física, mas sim mediado por dispositivos tecnológicos, simulando identidades, falsificando documentos eletrônicos ou manipulando dados, diante disso, a fronteira entre a fraude tradicional e a fraude digital se desloca, exigindo aprimoramentos interpretativos por parte da doutrina e da jurisprudência.

Ademais, autores como Martinez (2023) advertem que a prática do estelionato no ambiente virtual cria novos obstáculos à persecução penal, a utilização de contas falsas, redes descentralizadas e sistemas de criptografia dificultam a identificação dos autores e a produção de provas, isso, por conseguinte, fragiliza a atuação da polícia judiciária e do Ministério Público, contribuindo para a sensação de impunidade. Conforme reitera Aristides (2023), a ausência de flagrante, a pulverização das transações e o uso de intermediários — como “laranjas” — tornam o combate ao estelionato cibernético um dos maiores desafios investigativos da atualidade, logo, não basta agravar a pena, é necessário repensar os meios de investigação.

Em continuidade, observa-se que a tipologia do estelionato digital é ampla e em constante evolução, o que dificulta sua catalogação, há, por exemplo, fraudes por meio de perfis falsos em redes sociais, clonagem de contas de aplicativos de mensagens, golpes com uso de *deepfakes*, além de falsificações em ambientes de *e-commerce*. Segundo Alves (2020), mesmo plataformas digitais consideradas seguras têm falhado na proteção de dados, possibilitando que criminosos tenham acesso a informações sensíveis das vítimas, tais falhas ampliam a vulnerabilidade dos consumidores e exigem um reforço na responsabilidade civil e penal das empresas envolvidas.

Do ponto de vista normativo, além do Código Penal, destacam-se a Constituição Federal, o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais, que estabelecem garantias ao cidadão quanto à privacidade e à proteção de dados. Da Silva et al. (2018) apontam que, diante de vazamentos ocasionados por negligência de empresas, pode-se cogitar não apenas a responsabilidade civil, mas também a penal, caso se verifique o concurso de pessoas. Embora a legislação penal ainda não contemple expressamente a modalidade culposa no crime de estelionato, autores como Aristides (2023), têm defendido a ampliação interpretativa com base na teoria do risco, isso revela um movimento doutrinário em busca de maior eficácia repressiva.

A jurisprudência, por sua vez, tem se mostrado sensível ao agravamento do estelionato digital, em decisões recentes, tribunais estaduais e superiores têm reconhecido a periculosidade de condutas reiteradas em ambiente cibernético, a gravidade dos prejuízos causados e o risco

de reiteração delitiva. Consoante julgado do TJDF (2021)¹, a prática sequencial de fraudes virtuais, com emprego de dados de cartões de crédito, justifica a prisão preventiva diante da ameaça à ordem pública, essa atuação jurisdicional, ainda que tímida, demonstra uma tentativa de adaptar a atuação estatal às novas realidades do crime informático, contudo é necessário, maior uniformidade e tecnicidade nos julgados, a fim de garantir segurança jurídica.

Cumprido observar, também, que a atuação do estelionatário digital se dá dentro de estruturas cada vez mais organizadas, aproximando-se do modelo de criminalidade econômica empresarial, a esse respeito, Aristides (2023) destaca que os cibercrimes frequentemente envolvem ações transnacionais, o que impõe desafios adicionais quanto à jurisdição, cooperação internacional e aplicação do princípio da ubiquidade. Essa pesquisa comenta que, o estelionato digital rompe fronteiras físicas e exige atuação coordenada entre instituições nacionais e estrangeiras, isso porque, a ausência de tratados eficazes e mecanismos céleres de cooperação tem contribuído para a perpetuação dessas práticas, assim, a dimensão internacional do estelionato eletrônico deve ser incorporada nas análises jurídicas contemporâneas.

Por outro lado, autores como Feitoza (2012) demonstram preocupação com a constante defasagem entre o avanço tecnológico e a legislação penal, onde o Direito, muitas vezes, atua de forma reativa, o que compromete sua eficácia frente a delitos que evoluem em tempo real. Nesse cenário, a legislação brasileira, apesar dos avanços, ainda carece de atualização sistemática para enfrentar a complexidade das fraudes digitais, o fato é que, a criminalidade informacional exige normas penais abertas, mas também claras, que permitam a aplicação efetiva sem violar o princípio da legalidade, nesse sentido, urge a construção de um microsistema penal cibernético, que una proteção de dados, segurança digital e repressão eficiente.

Posto isso, evidencia-se que o estelionato digital constitui não apenas uma nova forma de fraude, mas uma realidade criminosa que desafia os fundamentos clássicos do Direito Penal, a legislação, a doutrina e a jurisprudência precisam caminhar no sentido de construir respostas adequadas, céleres e eficazes. Com base nessas considerações, torna-se indispensável analisar como a racionalidade econômica, conforme delineada na seção anterior, encontra terreno fértil

¹ Nesse contexto, destaca-se o julgamento do Habeas Corpus nº 0737096-07.2021.8.07.0000, em que a Corte manteve a decretação da prisão preventiva de indivíduo acusado da prática reiterada de fraudes virtuais com uso de cartões de crédito. A decisão fundamentou-se na habitualidade criminosa e no risco concreto de reiteração delitiva, elementos que, diante das peculiaridades do caso concreto, justificaram a medida excepcional como forma de resguardar a ordem pública.

para se desenvolver no contexto digital, é nesse cenário que se insere a próxima seção, a qual examinará o estelionato como um empreendimento racional, considerando suas implicações jurídicas e a necessidade de reformulação das estratégias punitivas estatais.

4 O ESTELIONATO COMO EMPREENDIMENTO RACIONAL: IMPLICAÇÕES JURÍDICAS E POLÍTICAS DE ENFRENTAMENTO

À luz da Teoria Econômica do Crime, o estelionato digital revela-se como uma forma de empreendimento ilícito, fundado na lógica da racionalidade instrumental, o agente, ao ponderar riscos e ganhos, opta por atuar na ilegalidade quando identifica brechas no sistema punitivo que lhe garantam retorno expressivo com baixa probabilidade de punição. Conforme Albanese (2000), tal comportamento se insere no conceito de “empreendedorismo criminoso”, no qual a prática reiterada do crime é racionalizada como meio de vida, nesse contexto, o estelionatário atua com profissionalismo, planejamento e uso estratégico de recursos tecnológicos.

Cumprе observar que essa racionalidade criminosa é favorecida por fatores estruturais do ordenamento jurídico brasileiro, a pena prevista para o estelionato simples, mesmo após as alterações trazidas pela Lei nº 14.155/2021, ainda se mostra inferior à de outros delitos patrimoniais violentos. Conforme Capez (2012), a pena mínima e a possibilidade de acordos penais — como o não oferecimento de denúncia, a suspensão condicional do processo e a substituição por penas restritivas de direitos — favorecem o cálculo do infrator. A percepção de que o custo da punição é irrisório estimula a reincidência e a sofisticação das condutas, tornando ineficaz o caráter dissuasório da sanção penal.

Adicionalmente, a imprevisibilidade na resposta penal e a morosidade dos processos judiciais contribuem para o fortalecimento da criminalidade digital, segundo Greco (2011), a eficácia do Direito Penal está diretamente ligada à certeza da punição, e não apenas à sua severidade. No caso do estelionato digital, a dificuldade de investigação e a baixa taxa de condenações reforçam o sentimento de impunidade.

O agente infrator, diante desse cenário, continua a operar como empreendedor do crime, utilizando-se da tecnologia e das deficiências estatais para ampliar seus lucros ilícitos, trata-se

de um desequilíbrio sistêmico que necessita ser enfrentado com estratégias mais rigorosas e coordenadas.

Com base nesse diagnóstico, é necessário refletir sobre as medidas que podem ser adotadas para alterar os incentivos presentes na prática do estelionato digital, nesse sentido, a Teoria Econômica do Crime propõe a elevação dos custos da conduta delitiva por meio do fortalecimento da dissuasão e da incapacitação.

Para tanto, deve-se investir em mecanismos de investigação tecnológica, inteligência policial e cooperação institucional, conforme Aristides (2023), a repressão eficaz aos cibercrimes exige, ainda, integração normativa entre o sistema penal e a proteção de dados pessoais, com sanções claras para quem contribui, ainda que culposamente, com a prática delitiva, a eficiência do *enforcement*, portanto, é essencial à neutralização da lógica econômica do crime.

Sob essa ótica, a responsabilização de terceiros, notadamente empresas que, por negligência, possibilitam o vazamento de dados, tem sido objeto de crescente debate na doutrina contemporânea, conforme assevera Da Silva et al. (2018), o princípio da confiança e a teoria do risco criam pressupostos normativos para a responsabilização civil e até penal de agentes que, por omissão relevante, contribuam para o êxito da fraude. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) impôs às pessoas jurídicas o dever de segurança informacional, e seu descumprimento pode, em determinadas hipóteses, ensejar corresponsabilidade penal (Brasil, 2018), tal avanço é compatível com a ideia de prevenção ampliada, indispensável ao combate ao estelionato moderno.

Ainda no campo da repressão estatal, propõe-se o agravamento específico das penas nos casos em que a fraude for facilitada por negligência empresarial ou tecnológica, como observado por Andrade, Gama e Medrado (2024), a sofisticação dos golpes digitais depende, em muitos casos, da exploração de falhas em sistemas de segurança.

A criminalização de condutas culposas nesse contexto ampliaria a eficácia da norma penal, promovendo um ambiente de maior responsabilização, a inserção de qualificadoras no art. 171 do Código Penal é medida que pode ser discutida no plano legislativo, tendo em vista o princípio da proporcionalidade, nesse sentido, a pena deve corresponder à gravidade da ofensa e à complexidade da prática delitiva.

Sob outro aspecto, a utilização de ferramentas como *deepfakes*, algoritmos de clonagem de voz e perfis falsos amplia o poder de convencimento do estelionatário, Ribeiro, Silva e Viana (2024) sustentam que a inteligência artificial tem potencializado a capacidade de simulação do crime, tornando o engano mais verossímil e a vítima mais vulnerável. Isso exige do legislador uma postura proativa, capaz de atualizar constantemente o tipo penal frente às novas formas de execução. Sendo assim, a pena, além de justa, deve ser atual, eficaz e capaz de demonstrar à sociedade que o ordenamento jurídico acompanha a evolução das práticas criminosas.

Por conseguinte, a atuação estatal deve se orientar por uma política criminal articulada, que una repressão, prevenção e educação digital, como destacam Oliveira, Silva e Almeida (2023), o Direito Penal, enquanto último recurso (*ultima ratio*), precisa dialogar com outras áreas jurídicas e com políticas públicas de conscientização e proteção de dados.

A prevenção não se restringe à punição; ela envolve campanhas de informação, investimentos em segurança digital e fortalecimento das capacidades técnicas dos órgãos de investigação, a repressão isolada, sem apoio institucional e social, não basta para romper a lógica econômica do estelionato virtual.

Dessa forma, evidencia-se que o estelionato digital, sob o prisma da Teoria Econômica do Crime, configura uma escolha racional estimulada por um sistema penal ineficiente e por um ambiente digital permissivo, o Estado, ao não responder adequadamente, termina por se tornar partícipe indireto da perpetuação da conduta.

Cabe, portanto, aos operadores do Direito repensar os fundamentos do sistema penal frente à nova morfologia da criminalidade contemporânea, nesse sentido, a racionalidade que embasa a prática criminosa exige uma racionalidade equivalente na elaboração e aplicação das normas, o enfrentamento eficaz do estelionato passa pela compreensão integral de seus mecanismos econômicos, sociais e tecnológicos.

Nesse sentido, para além da abordagem teórica, é indispensável verificar empiricamente como os elementos analisados se manifestam na realidade concreta, considerando dados e tendências observadas em registros oficiais e estudos recentes. A análise empírica permitirá não apenas validar os pressupostos teóricos aqui discutidos, mas também propor recomendações práticas para o aprimoramento da legislação penal e da atuação estatal diante da criminalidade econômica em ambiente virtual.

5 CONCLUSÃO

A análise do estelionato digital sob a ótica da Teoria Econômica do Crime demonstrou que o comportamento delitivo, longe de ser mero desvio moral, constitui resposta racional a estímulos normativos, institucionais e tecnológicos, o agente infrator avalia os custos e benefícios de sua ação e, ao identificar falhas sistêmicas, opta pela prática criminosa como estratégia economicamente vantajosa.

Assim, a conduta delitiva se insere na lógica de mercado e responde a estímulos de impunidade, desorganização institucional e baixa eficácia da pena, nesse contexto, o crime é gerido como um empreendimento racional e recorrente.

Verificou-se que o ordenamento jurídico brasileiro, embora tenha promovido avanços importantes com a promulgação da Lei nº 14.155/2021, ainda se mostra defasado diante da complexidade das fraudes digitais, o estelionato digital, embora preserve os elementos clássicos do tipo penal, apresenta novas formas de execução, com elevado grau de sofisticação tecnológica e dificuldade de rastreamento.

Tais características desafiam os instrumentos tradicionais da persecução penal, exigindo, por consequência, interpretações atualizadas e mecanismos mais ágeis de repressão, nesse cenário, a legislação, por si só, não é suficiente sem articulação com as estruturas investigativas e processuais.

A partir da lógica de dissuasão e incapacitação, princípios centrais da teoria analisada, conclui-se que o enfrentamento do estelionato digital deve se basear na elevação concreta dos custos da prática delitiva, isso pressupõe, entre outros fatores, a celeridade processual, a uniformização da jurisprudência e o fortalecimento da capacidade investigativa do Estado.

A racionalidade criminosa só poderá ser desestimulada se houver certeza de punição e efetividade na sanção, do contrário, a permanência das brechas normativas e a morosidade judicial continuarão a reforçar o caráter lucrativo da fraude eletrônica.

Além disso, o estelionato digital tem se expandido de forma compatível com modelos de organização empresarial, exigindo políticas penais articuladas e integradas, a atuação estatal deve considerar não apenas o autor direto do crime, mas também os facilitadores institucionais, como plataformas tecnológicas e empresas que agem com negligência.

A responsabilização por omissão, prevista na doutrina moderna, deve ser incorporada ao combate às fraudes digitais, sendo assim, a proteção de dados pessoais e a governança da

informação passam a ser elementos centrais para a contenção da atividade criminosa economicamente estruturada.

Ressalta-se, também, que a criminalidade digital transcende fronteiras físicas e exige cooperação jurídica internacional eficaz, essa ausência de tratados específicos e de mecanismos céleres de cooperação compromete a repressão de crimes transnacionais, frequentemente praticados com servidores hospedados no exterior.

A resposta estatal, para ser proporcional, deve unir esforços legislativos, diplomáticos e institucionais, fortalecendo canais de comunicação entre os países e assegurando a efetividade das investigações, a construção de um microssistema penal cibernético é, nesse sentido, um caminho necessário para acompanhar a transformação dos delitos patrimoniais.

Conclui-se, portanto, que o estelionato digital é expressão clara da racionalidade criminosa diante de um Estado ainda desarticulado e reativo, onde o avanço da tecnologia impõe ao Direito Penal o dever de se reinventar, adotando um modelo mais estratégico, integrado e eficiente. A aplicação da Teoria Econômica do Crime ao contexto digital não apenas explica a permanência da fraude como aponta direções para seu enfrentamento, nesse cenário, o fortalecimento da repressão penal, aliado a políticas públicas preventivas, é essencial para romper com o ciclo de lucratividade que sustenta o estelionato na era da informação.

REFERÊNCIAS

ALBANESE, J. **The causes of organized crime**: do criminals organize around opportunities for crime or do opportunities create new offenders?. *Journal of Contemporary Criminal Justice*, v. 16, 2000.

ANDRADE, T. R. A.; GAMA, G. B. A. C. V. R. N.; MEDRADO, L. C. **Responsabilidade culposa pelo vazamento de dados**: a inteligência artificial como agravante no estelionato digital. *Revista Filosofia Capital*, Brasília, v. 20, n. 26, p. 1-19, 2024. DOI: 10.51497/rfc.v20n26-013.

ARISTIDES, C. J. **Crimes cibernéticos e jurisdição**: desafios e propostas de solução. *Revista Cognitio Juris*, 2023.

BARATA, J. A.; ANDRADE FILHO, J. L. J. **Crimes cibernéticos e o estelionato virtual**. *FADAP - Revista Jurídica*, n. 2, 2023.

BECKER, G.; LANDES, W. M. **Crime and Punishment: An Economic Approach**. University of Chicago and National Bureau of Economic Research, 1974.

BENTHAM, J. **Os Pensadores**: Uma Introdução aos Princípios da Moral e da Legislação. São Paulo: Abril Cultural, 1974.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial [da] República Federativa do Brasil. Rio de Janeiro: 31 dez. 1940.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial [da] República Federativa do Brasil. Brasília: 15 ago. 2018.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Altera o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), e outras leis. Diário Oficial [da] República Federativa do Brasil. Brasília: 24 dez. 2019.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal e o Código de Processo Penal para agravar a pena do estelionato cometido por meio eletrônico. Diário Oficial [da] República Federativa do Brasil. Brasília: 28 maio 2021.

CAPEZ, F. **Curso de Direito Processual Penal**. 19. ed. São Paulo: Saraiva, 2012.

DA SILVA, D. L. *et al.* **Os direitos básicos do consumidor protegidos pela Lei nº 8.078/1990**. Anais do Seminário Científico do UNIFACIG, n. 4, 2018.

FEITOZA, L. G. M. **Crimes cibernéticos**: o estelionato virtual. Brasília, 2012. Disponível em: <https://repositorio.ucb.br>. Acesso em: 18 abr. 2025.

GRECO, R. **Código Penal Comentado**. 5. ed. Rio de Janeiro: Impetus, 2011.

MARTINEZ, S. R. A. **O crime de estelionato no ambiente virtual**: um estudo da produção dos meios de prova. Jus.com.br, 2024. Disponível em: <https://jus.com.br/artigos/107580>. Acesso em: 17 abr. 2025.

MONTEIRO, R. L. **Crimes eletrônicos**: uma análise econômica e constitucional. 2010. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf>. Acesso em: 15 abr. 2025.

OLIVEIRA, Í.; SILVA, U.; ALMEIDA, F. **Estelionato cibernético: estratégias, respostas legais e desafios na era digital**. Revista FT, 2024. ed. 128, vol. 27.

POLÍCIA CIVIL DO ESTADO DO PARANÁ. **Cibercrimes: estelionato digital – orientações técnicas da 14ª Subdivisão Policial de Guarapuava**. Guarapuava: 14ª SDP, 2022.

RIBEIRO, L. H. C.; SILVA, C. M.; VIANA, P. W. P. **Artificial intelligence as a tool for predicting crime in large Brazilian cities**. Revista FT, 2024. ed. 133, vol. 28.