Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

Estelionato eletrônico praticado mediante uso indevido de dados de advogados: Desafios penais e digitais na proteção da advocacia e dos clientes

Electronic fraud committed through the improper use of lawyer data: Criminal and digital challenges in protecting the legal profession and clients

Vanessa Susan de Araújo Lima[1] e Erick Wilson Pereira[2]

v. 14/ n. 3 (2026)
Julho/Setembro

Aceito para publicação em 16/06/2026.

[1]Graduanda em Direito pela Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0009-0005-2938-1964. E-mail: vanesusann@gmail.com;
[2]Doutor em Direito pela Pontifícia Universidade Católica de São Paulo, São Paulo, São Paulo. ORCID: 0009-0005-9147-9516. E-mail: ewp@erickpe-reira.adv.br.

https://www.gvaa.com.br/revista/index.php/RDG

RESUMO: O presente artigo aborda o crime de estelionato eletrônico praticado mediante a utilização indevida de dados de advogados, modalidade criminosa que passou a ameaçar diretamente a advocacia e seus clientes. A pesquisa analisa a evolução legislativa do estelionato no Brasil, desde o Código Criminal do Império (1830) até as inovações trazidas pela Lei nº 14.155/2021, que tipificou a fraude eletrônica no § 2º-A do Art. 171 do Código Penal, e pela Lei nº 15.397/2026, que introduziu a figura da cessão de conta laranja. Examina-se, em especial, a sistemática operacional do golpe do falso advogado, estruturado em núcleos de inteligência de dados, tecnologia, engenharia social e logística financeira. Investiga-se, ainda, a vulnerabilidade do sistema Processo Judicial Eletrônico (PJe) como fonte de dados para a perpetração das fraudes, discutindo a tensão entre transparência processual e proteção de dados. Conclui-se que o recrudescimento punitivo, desacompanhado de fortalecimento da capacidade investigativa estatal e de reformas na arquitetura de segurança dos sistemas judiciais eletrônicos, produz um punitivismo simbólico insuficiente para conter o avanço das organizações criminosas especializadas em fraudes digitais.
Palavras-chave: fraude eletrônica; golpe do falso advogado; processo judicial eletrônico; conta laranja; segurança cibernética.

ABSTRACT: This article addresses the crime of electronic fraud committed through the improper use of lawyer data, a criminal modality that has come to directly threaten the legal profession and its clients. The research analyzes the legislative evolution of fraud in Brazil, from the Criminal Code of the Empire (1830) to the innovations brought by Law No. 14,155/2021, which typified electronic fraud in § 2º-A of Art. 171 of the Penal Code, and by Law No. 15,397/2026, which introduced the figure of the orange account cession. It specifically examines the operational systematics of the fake lawyer scam, structured in data intelligence, technology, social engineering, and financial logistics nuclei. It also investigates the vulnerability of the Electronic Judicial Process (PJe) system as a data source for perpetrating frauds, discussing the tension between procedural transparency and data protection. It concludes that punitive recrudescence, unaccompanied by the strengthening of state investigative capacity and reforms in the security architecture of electronic judicial systems, produces a symbolic punitivism insufficient to contain the advance of criminal organizations specialized in digital fraud.
Keywords: electronic fraud; fake lawyer scam; electronic judicial process; orange account; cybersecurity.

1 CONSIDERAÇÕES INICIAIS

A expansão da criminalidade no ciberespaço impõe à jurisdição penal um problema de efetividade que este trabalho se propõe a examinar. O ponto de partida é constatar que as

fraudes patrimoniais se sofisticaram num ritmo que supera a capacidade de resposta das agências de controle — descompasso que exige reavaliar as políticas de segurança institucional no âmbito jurídico.

Discute-se, em primeiro lugar, como a instrumentalização de plataformas processuais públicas para a prática de ilícitos tensiona o direito fundamental à informação diante da autodeterminação informativa dos sujeitos processuais. A premissa que orienta essa análise é a de que arquiteturas de *software* desprovidas de salvaguardas preventivas podem atuar como facilitadoras involuntárias da delinquência sistêmica, transformando a transparência estatal em vetor de vulnerabilidade.

Na sequência, o texto aborda os limites do punitivismo quando dissociado de investigação eficaz. A literatura da teoria econômica do delito sustenta que medidas retributivas perdem impacto sem uma probabilidade real de punição — e a inflação legislativa, nesse contexto, gera uma falsa percepção de controle ao mesmo tempo que escamoteia a precariedade da infraestrutura investigativa.

Os estudos sobre persecução de ilícitos cibernéticos revelam, ademais, um gargalo operacional nas delegacias de base, onde a preservação da cadeia de custódia de vestígios voláteis enfrenta sérias dificuldades. Examina-se, por fim, como esse cenário compromete a utilidade prática do endurecimento penal.

O último eixo da discussão volta-se para a profissionalização das redes de estelionato. A análise empírica do fluxo financeiro e operacional de organizações criminosas documenta o emprego sistemático de contas de passagem manipuladas por indivíduos em graus variados de consciência e consentimento. Cabe ao trabalho investigar em que medida o fracionamento logístico dessas redes exige do Estado uma abordagem multifocal, capaz de ultrapassar a figura do executor direto e alcançar a cadeia como um todo — da mineração de dados à pulverização de ativos.

O argumento que percorre estas seções é o de que a superação do punitivismo retórico depende de ações estruturantes na governança das informações processuais sob guarda do poder público.

2 A ORIGEM DO ESTELIONATO

A formalização do crime de estelionato no Brasil teve início em 1830, no Código Criminal do Império, contexto em que a Proclamação da Independência (1822) e a Constituição de 1824 marcaram o início de uma ordem jurídica puramente brasileira. Nesse período, porém, ainda não existia uma figura autônoma chamado “estelionato”, o foco legislativo consistia na proteção da boa-fé nas relações comerciais, com as fraudes sendo punidas genericamente dentro do capítulo de "Falsidades", sem distinção entre falsificação documental e fraude patrimonial.

No entanto, essa lacuna foi sendo preenchida gradualmente. À vista disso, o Código Penal da República (1890), que se manifestou como um marco de ruptura com o passado monárquico e o surgimento de um novo Estado, introduziu, finalmente, o estelionato como delito autônomo, refletindo a necessidade de combater golpes mais sofisticados que emergiram com a urbanização e a especulação financeira da época. Contudo, foi apenas com o Código Penal de 1940 que o crime ganhou sua estrutura definitiva, consolidando-se como crime patrimonial de inteligência.

Hodiernamente, no Título II, Parte Especial, do Código Penal Brasileiro — Lei nº 2.848, de 7 de dezembro de 1940 — encontram-se delimitados os "Crimes contra o patrimônio", dentre os quais o Art. 171 conceituando o crime de "Estelionato" nos seguintes termos:

> Estelionato
> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 15.397, de 2026)

3 O ADVENTO DO ESTELIONATO ELETRÔNICO — ART. 171, § 2º-A, DO CÓDIGO PENAL

O crime de estelionato, codificado em 1940, ainda passou por diversas alterações legislativas ao longo dos anos, adaptando-se conforme as necessidades do contexto social vivido. Assim, quando a sociedade brasileira emergiu num cenário de intensa evolução tecnológica e ampliação das relações sociais no ambiente digital, essa capacidade de evolução do tipo penal tornou-se especialmente relevante. Pois, paralelamente ao desenvolvimento tecnológico legítimo, surgiu uma nova modalidade de fraude patrimonial: o chamado estelionato eletrônico.

O ponto de inflexão para a tipificação específica desse crime ocorreu durante a pandemia da COVID-19. O isolamento social forçou o deslocamento massivo para o meio digital: *home office*, compras *online*, audiências virtuais, ensino a distância e operações financeiras — como o Pix e o *Open Banking* — tornaram-se atividades cotidianas.

Simultaneamente, os golpistas também migraram para essa nova atmosfera, utilizando-se dos meios eletrônicos e das técnicas de engenharia social para a aplicação das fraudes, causando um aumento exponencial da lesividade dos delitos patrimoniais. De acordo com Arthur Sabbat, Diretor do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), os crimes cibernéticos registraram um aumento de aproximadamente 300% desde o início da pandemia (ANPD, 2021).

Além disso, o CP não tinha uma tipificação específica para fraude eletrônica, o tratamento jurídico brasileiro relacionado aos crimes cibernéticos se iniciou com a Lei 12.737/2012, conhecida

como Lei Carolina Dieckmann, em virtude da atriz brasileira ter seu computador invadido e ter suas fotos íntimas divulgadas, numa tentativa de extorsão. Diante de tais fatos, a nova lei introduziu dois novos artigos no CP tipificando criminalmente o delito informático: Invasão de dispositivo informático, Art. 154-A e o Art. 154-B que trata da representação nos crimes do 154-A.

Segundo a classificação doutrinária de Damásio de Jesus, inspirado pelo sistema binário proposto por Hervé Croze e Yves Bismuth — doutrinadores franceses —, os crimes virtuais dividem-se em:

> I - Puros ou Próprios: Condutas ilícitas que se valem do aparato informático e têm por vítima o sistema de processamento de dados e suas infraestruturas tecnológicas;
> II - Impuros ou Impróprios: A tecnologia informática é utilizada como meio para prejudicar bens e direitos que não estão relacionados com a própria informática.

Nessa senda, o delito de invasão de dispositivo informático pode ser classificado como crime cibernético puro, pois o legislador visou punir a invasão de dispositivos alheios, a quebra de sistemas de segurança ou a instalação de *malwares*; todavia, o Art. 154-A não cobria *phishing*, engenharia social ou fraudes via redes sociais.

Nesse cenário, anos se passaram e conforme a tecnologia e suas aplicações avançavam, as vítimas de fraudes eletrônicas se multiplicavam e, consequentemente, o Poder Judiciário enfrentava dificuldades com a legislação penal para estabelecer a condenação de golpistas que operavam exclusivamente online, pois o estelionato não diferenciava a gravidade entre um golpe físico e direto e um golpe digital em grande escala.

De acordo com senador Izalci Lucas - autor do projeto de ley original (PL 4.554/2020) que deu origem à Lei nº 14.155/2021 - um dos motivos para essa explosão de fraudes digitais seria uma legislação branda para punir esse tipo de crime.

Foi nesse contexto que a Lei nº 14.155, de 27 de maio de 2021, introduziu a modalidade qualificada do estelionato eletrônico, inserindo o §2º-A ao Art. 171 do Código Penal, estabelecendo penas significativamente mais severas para fraudes cometidas mediante o uso de tecnologia digital, sob a seguinte disposição:

> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

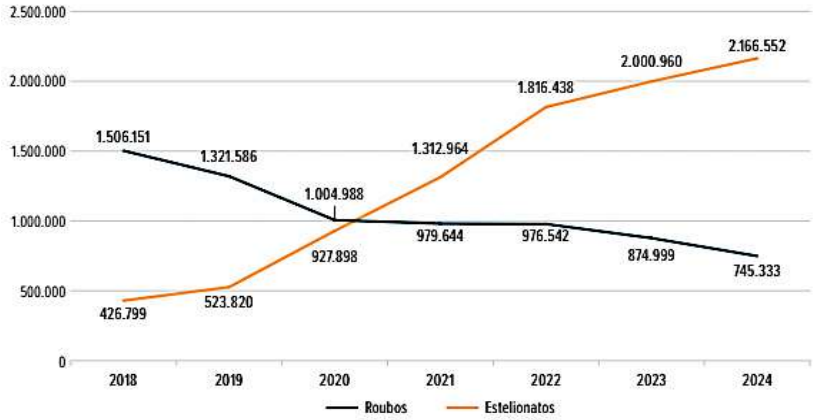
É de se notar que a pressão legislativa foi efetiva ao se deparar com o novo dispositivo legal especificando a fraude eletrônica e punindo de modo mais severo a sua prática. Ademais, é inegável que o alcance das redes de internet vão além dos limites geográficos, razão pela qual o § 2º-B foi preciso ao considerar os agentes que se utilizam de servidores estrangeiros para mascarar sua localização e dificultar a apuração da autoria do crime, majorando a pena nesses casos de 1/3 a 2/3.

Nesse diapasão, apesar do endurecimento punitivo aos crimes cibernéticos promovido pela lei nº 14.155/2021, o Brasil ainda vivenciava uma crescente insegurança pública relacionada aos golpes digitais e fraudes eletrônicas, pois as organizações criminosas sofisticaram seus métodos fraudulentos e passaram a utilizar massivamente o ambiente digital.

4 O GOLPE DO FALSO ADVOGADO

Nesse sentido, o estelionato emergiu como grave problema de segurança pública no Brasil já no período pandêmico, mantendo-se em crescimento exponencial nos anos seguintes, como pode se verificar no gráfico seguir:

Gráfico 1 — Evolução dos roubos e estelionatos, ns. absolutos - Brasil, 2018-2024



Fonte: Fórum Brasileiro de Segurança Pública (2025, p. 107)

De acordo com o 19º Anuário Brasileiro de Segurança Pública, publicado pelo Fórum Brasileiro de Segurança Pública em julho de 2025, foram registrados 2.166.552 estelionatos em 2024, representando um crescimento de 7,8% em relação a 2023, com taxa nacional de 1.019,2 registros por 100 mil habitantes.

Desde 2018, o aumento acumulado foi de 408%, equivalente a uma média de quatro estelionatos por minuto no território brasileiro ao longo de 2024 (FBSP, 2025, p. 107). Dentro desse aumento exponencial, os estelionatos perpetrados por meios eletrônicos cresceram 17% de 2023 para 2024, evidenciando a sofisticação e a expansão dessa modalidade criminosa.

Como consequência do aumento dos golpes digitais nos últimos anos, o judiciário brasileiro também passou a ser alvo de ataques cibernéticos através de um novo esquema de fraude denominado de golpe do falso advogado. Esta prática estelionatária caracteriza-se pelo uso da identidade de profissionais jurídicos, através de aplicativos de comunicação instantânea e com a apropriação de informações processuais legítimas.

O golpe do "falso advogado", espécie de estelionato por fraude eletrônica, consiste na exploração das informações de acesso público nos processos judiciais eletrônicos pelos golpistas. Estes, se utilizam da atribuição da identidade do advogado verdadeiro e dos dados públicos dos clientes como ferramenta para passar credibilidade à fraude, assim, entram em contato com as vítimas por intermédio das redes sociais - principalmente pelo aplicativo *WhatsApp* - ou contatos telefônicos e as induzem a acreditar que estão em contato com o advogado real.

Desse modo, na intenção de obterem vantagem indevida, os autores do delito informam falsamente sobre supostos ganhos de causa e orientam as vítimas a realizarem transferências bancárias sob o pretexto de liberação de valores judiciais ou para evitar bloqueios de contas.

Como se nota, os dados judiciais disponibilizados constituem o principal instrumento utilizado pelos golpistas na execução das fraudes. O sistema em questão é o Processo Judicial Eletrônico (PJe), desenvolvido pelo Conselho Nacional de Justiça em parceria com os tribunais brasileiros e a Ordem dos Advogados do Brasil. Embora o PJe possibilite o acesso aos autos processuais tanto de modo público, quanto mediante autenticação e certificação digital, essa facilidade de acesso — ainda que benéfica para a transparência — resulta na exposição desprotegida de dados sensíveis das partes processuais.

Pela simples consulta pública no PJe, encontram-se à disposição múltiplos dados suscetíveis de apropriação indevida pelos estelionatários. Esses dados proporcionam matéria suficiente para a execução do golpe, incluindo: a classe judicial do processo, o assunto tratado, o órgão julgador, as movimentações processuais nas suas respectivas datas, os participantes dos polos ativo e passivo com seus nomes e CPFs, e, em regra, os documentos juntados ao processo.

A vulnerabilidade agrava-se significativamente quando se considera o acesso ao PJe mediante autenticação ou certificado digital. Nesse contexto, conforme a reportagem veiculada no programa Fantástico, os criminosos contornam as barreiras de segurança adquirindo *logins* de advogados no "mercado paralelo" (G1, 2025), obtendo assim, acesso privilegiado ao sistema. O acesso interno não se limita aos autos processuais públicos; permite, igualmente, a visualização de informações críticas à privacidade das partes, tais como documentos anexados, e-mail, número telefônico e localização residencial. Além disso, possibilita o acesso aos valores envolvidos nos pleitos e informações

bancárias dos clientes, transformando o PJe em uma verdadeira base de dados para a execução de fraudes sofisticadas.

Verifica-se, portanto, que a transparência processual, embora fundamental para o Estado Democrático de Direito, não pode prescindir de salvaguardas técnicas e legais. Sob essa ótica, a ausência de controles que diminuam os perigos da exposição de dados processuais vulnerabiliza tanto os profissionais jurídicos quanto seus constituintes, criando ambiente propício para a perpetração de fraudes digitais.

Outrossim, para que o estelionato por fraude eletrônica alcance simultaneamente uma ampla quantidade de vítimas, não basta a vulnerabilidade dos dados públicos judiciais, também é necessário que exista uma organização estruturada com divisão clara de tarefas. No golpe do falso advogado a segmentação da organização criminosa (ORCRIM) pode ser definida nos parâmetros a seguir:

A) Setor de Inteligência de Dados

Utilizando-se de bancos de dados vazados e comercializados ilegalmente, o setor de inteligência da organização filtra as vítimas por perfil e fica responsável pela monitoração constante dos Diários de Justiça Eletrônicos e sistemas de tribunais (como o PJe). Os golpistas nessa etapa, buscam processos em fase de finalização, especialmente aqueles que envolvem o pagamento de precatórios, alvarás judiciais ou revisões previdenciárias.

É justamente nesse setor que se extraem as informações públicas como ferramenta para o início da aplicação do estelionato.

4.1.1 Setor de Tecnologia e Infraestrutura

Nessa categoria os fraudadores salvam as fotos do advogado legítimo, que podem ser extraídas de redes sociais ou do Cadastro Nacional de Advogados da OAB, e criam um perfil de *WhatsApp* utilizando o nome do profissional ou o logotipo do escritório de advocacia. Logo após, os golpistas criam robôs de disparo em massa de *SMS/WhatsApp* que lhes permitem iniciar milhares de tentativas de golpe diárias.

4.1.2 Setor de Engenharia Social

Na engenharia social, os operadores entram em contato com a vítima se passando pelo advogado ou por um assistente do escritório, informando que o juiz liberou o pagamento do precatório ou alvará, mas que, para a liberação do dinheiro pelo banco, é necessário o pagamento prévio de uma "taxa de custas", "imposto de renda sobre ganho judicial" ou "emolumentos cartorários". Além disso,

criam um senso de urgência que, se o depósito não for feito nas próximas horas, o valor retornará para os cofres públicos.

4.1.3 Setor de Logística Financeira

No momento em que a vítima concorda em pagar, o setor financeiro fornece a chave Pix para o depósito. A partir desse momento, as contas laranjas se tornam fundamentais para o prejuízo de milhares de vítimas, pois servirão para ocultar a identidade dos líderes da organização criminosa e para dificultar o rastreamento dos valores subtraídos.

O fluxo financeiro do golpe inicia assim que a vítima realiza a transferência e o dinheiro cai na conta de um "Laranja Involuntário" - vítimas de vazamento de dados - dificultando o trabalho investigativo das autoridades policiais. Em uma fração de segundos, sistemas automatizados ou operadores pulverizam frações desse valor para dezenas de outras contas laranjas; "Laranja Profissional - Consciente", "Laranja Enganado - Inocente Útil" ou ambos, dificultando o rastreamento e burlando o Mecanismo Especial de Devolução do Banco Central.

Por fim, o dinheiro pulverizado é rapidamente convertido em criptomoedas ou sacado em espécie em caixas eletrônicos, rompendo definitivamente o lastro digital da fraude.

Os perfis de contas laranjas utilizados pelos criminosos para a estruturação do esquema estão conceituados da seguinte forma:

a) Laranja Profissional - Consciente: Pessoas que deliberadamente "alugam" ou vendem o acesso às suas contas bancárias e chaves Pix para os criminosos, em troca de comissões ou valores fixos. Atuam como peça voluntária da engrenagem financeira da organização criminosa. Nível de consentimento: Totalmente consciente do ato ilícito.
b) Laranja Enganado - Inocente Útil: Vítimas atraídas por falsas promessas de "trabalho em casa" ou "renda extra". A tarefa supostamente consiste apenas em receber transferências e repassá-las a terceiros. O agente atua sob erro de tipo (Art. 20 do CP) ou erro de proibição escusável (Art. 21 do CP), tornando sua conduta atípica por ausência de dolo. Nível de consentimento: Acredita estar realizando um trabalho legítimo.
c) Laranja Involuntário - Fraude de Identidade: Cidadãos que tiveram seus dados pessoais vazados ou roubados. Os criminosos utilizam essas informações para abrir contas digitais em instituições financeiras que possuem processos de validação frágeis. Por inexistir qualquer conduta por parte do indivíduo, não há dolo nem culpa, sendo este considerado estritamente vítima — tanto da organização criminosa quanto da falha na prestação de

serviços dos bancos. Nível de consentimento: Nenhum (a pessoa não sabe que a conta existe).

Diante desse cenário, a Lei n.° 15.397, de 30 de abril de 2026, foi sancionada pelo Presidente Lula e publicada no Diário Oficial da União em 4 de maio de 2026. A nova normativa, com o intuito de conter o avanço das quadrilhas organizadas especializadas em fraudes digitais, promoveu uma importante inovação dogmática no Código Penal Brasileiro ao introduzir a figura específica da "Cessão de conta laranja" no Artigo 171, § 2º, inciso VII, conforme se segue:

> Cessão de conta laranja (Incluído pela Lei nº 15.397, de 2026)
> VII – cede, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto. (Incluído pela Lei nº 15.397, de 2026)

A grande relevância desse novo inciso está na responsabilização e na punição das contas laranjas, a qual se fundamentará no elemento subjetivo (dolo) e na existência de conduta voluntária. Nesses termos, o inc. VII, do § 2º do art. 171 tem como alvo a conduta típica do “Laranja profissional”, pois o agente, de forma voluntária e consciente, vende ou aluga suas credenciais bancárias para que a organização criminosa movimente o dinheiro dos golpes.

Ao contrário do laranja consciente, o “Laranja enganado” é o indivíduo em situação de vulnerabilidade atraído por falsos anúncios de emprego, como por exemplo, de "intermediador de transferências" e que por essas razões tende a ceder sua conta sem saber que ela será utilizada para fins ilícitos.

Ademais, como só existe estelionato na modalidade dolosa, do mesmo modo suas figuras equiparadas, a conduta do agente é considerada atípica, tendo em vista que o agente atuou sob erro de tipo (Art. 20 do CP) ou erro de proibição escusável (Art. 21 do CP), pois foi enganado sobre a realidade da situação.

Em última análise, o "Laranja involuntário" é o cidadão comum que teve seus dados pessoais vazados ou roubados e utilizados por criminosos para a abertura de contas digitais falsas sem sua participação ou conhecimento. Nesse caso, por não existir conduta, não há dolo e não há culpa por parte do indivíduo, sendo este considerado estritamente vítima da organização criminosa e também vítima de falha na prestação de serviços das instituições financeiras.

5 DESAFIOS PENAIS E DIGITAIS NA PROTEÇÃO DA ADVOCACIA E DOS CLIENTES

Uma vez compreendida a complexidade da estrutura dessas organizações, sobressai o desafio estatal de combatê-las. Diante de quadrilhas altamente sofisticadas — segmentadas em núcleos de inteligência, tecnologia, engenharia social e logística financeira —, a resposta do Estado tem se concentrado, majoritariamente, na inflação punitiva e no recrudescimento normativo.

Essa aposta legislativa, no entanto, parece ignorar a atemporal advertência de Cesare Beccaria em *Dos Delitos e das Penas* (publicado em 1764): "A certeza de uma punição, ainda que moderada, exerce um impacto dissuasório muito maior do que o temor de uma sanção severa acompanhada pela esperança de impunidade".

O esvaziamento prático dessa estratégia estritamente punitivista no ambiente digital é explicado pela Teoria Econômica do Crime, desenvolvida pelo economista Gary Becker, cuja premissa central demonstra que o aumento na probabilidade de punição é estatisticamente mais eficaz para dissuadir o infrator do que apenas aumentar a severidade da pena.

No ciberespaço, quando a severidade da lei não vem acompanhada de investimentos robustos em capacidade investigativa, o resultado é uma falsa sensação de segurança. Instala-se, assim, um nítido punitivismo simbólico. Afinal, como já alertavam autores consagrados da criminologia, como Baratta (2011, p. 161) e Zaffaroni (2011, p. 232), o aumento das penas assume um caráter meramente retórico se o Estado não fortalecer as instituições encarregadas de aplicá-las.

Sob o prisma da realidade fática, a prática diária das delegacias revela o choque direto entre o rigor da norma e a escassez de recursos. Esse abismo material reflete-se na ausência de unidades especializadas em crimes cibernéticos na maioria dos municípios brasileiros — restritas, via de regra, às capitais e regiões metropolitanas —, o que gera um gargalo investigativo imediato.

Nesses termos, quando uma vítima do golpe do falso advogado procura uma delegacia de bairro, é comum que o plantonista não disponha do treinamento técnico exigido para registrar corretamente os vestígios digitais, como cabeçalhos de e-*mail*, *IDs* de transações via Pix ou *logs* de IP. Essa deficiência inicial compromete toda a viabilidade da investigação.

Embora a desarticulação do estelionato eletrônico exija o emprego de ferramentas de inteligência em fontes abertas (OSINT), análise de metadados e *softwares* forenses avançados, a realidade impõe às unidades locais uma dependência crônica dos núcleos centralizados. Esse engessamento técnico interno soma-se a um obstáculo externo: a morosidade rotineira de provedores e bancos em fornecer dados telemáticos e financeiros, o que, via de regra, inviabiliza a identificação dos autores.

O déficit investigativo desdobra-se, ainda, em um desafio processual de extrema gravidade: a preservação da cadeia de custódia da prova digital, nos moldes dos artigos 158-A a 158-F do Código de Processo Penal.

Dada a natureza volátil e imaterial dos vestígios eletrônicos, a falta de laboratórios periciais capilarizados e de protocolos rígidos de congelamento de dados — a exemplo da extração de imagens forenses (*bitstream*) e do cálculo de *hash* no ato da denúncia — corrói a confiabilidade dos elementos colhidos.

O Superior Tribunal de Justiça já pacificou o entendimento de que a validade da prova digital está condicionada à comprovação inquestionável de sua integridade. Logo, falhas metodológicas na coleta ou a simples juntada informal de *prints* abrem caminho direto para a nulidade absoluta do acervo probatório. O recente retorno do estelionato à regra da ação penal pública incondicionada, promovido pela Lei nº 15.397/2026, que revogou o § 5º do art. 171 do CP, ilustra com precisão esse paradoxo.

Ao dispensar a representação da vítima, o Estado avocou o dever de atuar de ofício contra as fraudes digitais. Todavia, ao expandir sua responsabilidade persecutória sem o devido aparelhamento das forças de segurança, o poder público esbarra no princípio da vedação da proteção deficiente. O direito à segurança e à propriedade das vítimas — frequentemente hipervulneráveis nesse ecossistema — acaba sendo violado não pela escassez de leis, mas pela incapacidade material de aplicá-las no ciberespaço.

Nota-se, ainda, que a atual política de acesso aos autos eletrônicos carrega brechas severas, perfeitamente ilustradas por esse tipo de estelionato. A facilidade com que qualquer pessoa extrai detalhes privados dos processos mostra que a transparência desmedida atua, hoje, como um vetor para práticas criminosas.

Essas ocorrências revelam uma grave fragilidade arquitetônica dos sistemas eletrônicos do Judiciário, que falha ao não aplicar o princípio do *security by design* (segurança desde a concepção), no qual a segurança do *software* é integrada em todas as etapas do ciclo de vida do desenvolvimento desde o início, em vez de adicionar defesas apenas no final.

A vulnerabilidade evidencia-se pela ausência de mecanismos básicos de segurança da informação. Nota-se, de plano, a dispensa da Autenticação de Dois Fatores (2FA) para o acesso aos sistemas, bem como a inexistência de ferramentas de detecção de anomalias — camadas de inteligência capazes de cruzar dados de geolocalização e IP para bloquear comportamentos atípicos. Esse cenário é agravado pela fragilidade na rastreabilidade das sessões (*logs*).

Atualmente, as plataformas costumam registrar apenas genericamente a entrada de um usuário credenciado, omitindo metadados cruciais como o endereço IP e a identificação do dispositivo. Sem a captura granular desses rastros, inviabiliza-se qualquer auditoria ou bloqueio automatizado.

A infraestrutura do PJe tem seu quadro agravado ao falhar na anonimização de dados sensíveis disponíveis ao público. Essa exposição irrestrita permite que criminosos utilizem robôs de extração

(*crawlers*) para realizar varreduras em massa nos autos, capturando informações de forma automatizada e sem deixar rastros nominais. É justamente essa coleta sistemática de dados que fornece o insumo necessário para a engenharia social aplicada no golpe do falso advogado.

Por conseguinte, fica evidente a necessidade imperiosa de recalibrar a tensão entre o livre acesso aos autos e a autodeterminação informativa. Ainda que a visibilidade dos processos seja um pilar do controle social, há um consenso técnico de que os tribunais devem redesenhar seus protocolos de transparência. A meta é ocultar os dados que municiam a falsificação de contatos jurídicos. Na prática, frear as fraudes cibernéticas exige uma triagem rigorosa do que é publicado e a adoção de chaves de acesso restritas, promovendo a segurança digital sem limitar o direito à informação.

6 CONSIDERAÇÕES FINAIS

A arquitetura atual dos sistemas judiciais eletrônicos foi concebida sem o modelo de segurança desde a origem — e essa omissão teve consequências diretas: A viabilização da extração massiva de informações sensíveis e, com isso, fornece o insumo indispensável para a engenharia social que alimenta fraudes contra o jurisdicionado. As organizações delitivas, por sua vez, operam com alta segmentação. De um lado, monitoram estrategicamente o fluxo de dados processuais; de outro, estruturam o aparelhamento tecnológico das abordagens e executam a rápida pulverização financeira por meio de diferentes perfis de interpostas pessoas. O diagnóstico, portanto, não é apenas técnico — é estrutural.

Esse quadro se agrava quando se examina a resposta do Estado. Com efeito, o recrudescimento normativo chancelado pelas legislações recentes revela-se materialmente insuficiente no ambiente cibernético. Isso porque a ampliação da responsabilização penal e a conversão do delito em ação pública incondicionada esbarram no desaparelhamento crônico das unidades de investigação locais. Sem inteligência tecnológica nem laboratórios periciais capilarizados, a cadeia de custódia se corrói — e a volatilidade dos vestígios eletrônicos, que deveria ser enfrentada com método e recursos, converte-se em impunidade sistêmica.

O punitivismo, isolado, não sustenta a persecução penal, e a experiência examinada confirma que leis mais severas, desacompanhadas de capacidade investigativa, produzem tão somente uma falsa sensação de controle.

Daí decorre que a mitigação efetiva das fraudes processuais depende, antes de tudo, da recalibragem dos protocolos de transparência judiciária. Superar a vulnerabilidade institucional exige medidas concretas e articuladas: autenticação de múltiplos fatores como requisito obrigatório,

rastreabilidade pormenorizada de todos os acessos e anonimização das informações críticas nos portais de consulta pública.

Sem restrições arquitetônicas rigorosas, a publicidade dos atos processuais — pilar do Estado Democrático de Direito — continuará em rota de colisão com a proteção do patrimônio e da privacidade da sociedade. O desafio, em última análise, é conciliar transparência e segurança sem sacrificar nenhuma das duas, tarefa que exige do legislador e do Judiciário uma postura tão inovadora quanto a das organizações criminosas que se busca enfrentar.

7. REFERÊNCIAS

BANCO DO BRASIL. Entenda o risco de emprestar sua conta bancária. **Blog BB**. Disponível em: https://blog.bb.com.br/entenda-o-risco-de-emprestar-sua-conta-bancaria/. Acesso em: 22 jun. 2026.

BARATTA, A. **Criminologia crítica e crítica do direito penal**: introdução à sociologia do direito penal. Trad. Juarez Cirino dos Santos. 6. ed. Rio de Janeiro: Revan, 2011.

BECCARIA, C. **Dos delitos e das penas**. Trad. J. Cretella Jr. e Agnes Cretella. 2. ed. São Paulo: Revista dos Tribunais, 1999.

BECKER, G. S. **Crime and punishment**: an economic approach. Journal of Political Economy, Chicago, v. 76, n. 2, p. 169-217, mar./abr. 1968. Disponível em: http://users.soc.umn.edu/~uggen/Becker_JPE_68.pdf. Acesso em: 22 jun. 2026.

BEZERRA, E. V.; PEREIRA, L. M.; COSTA, M. L. Golpe do "falso advogado" e o PJE: transparência processual em conflito com a proteção de dados pessoais. **Observatório de la Economía Latinoamericana**, v. 24, n. 3, p. e13150, 2026. DOI: 10.55905/oelv24n3-015. Disponível em: https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/13150. Acesso em: 22 jun. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. ANPD participa de seminário que discute o combate aos crimes cibernéticos. **Portal Gov.br**, Brasília. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-seminario-que-discute-o-combate-aos-crimes-ciberneticos. Acesso em: 22 jun. 2026.

BRASIL. Código Criminal do Império. Lei de 16 de dezembro de 1830. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lim/lim-16-12-1830.htm. Acesso em: 22 jun. 2026.

BRASIL. Código Penal da República. Decreto n.º 847, de 11 de outubro de 1890. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm. Acesso em: 22 jun. 2026.

BRASIL. Código Penal. Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 22 jun. 2026.

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 jun. 2026.

BRASIL. Lei n.º 14.155, de 27 de maio de 2021. **Diário Oficial da União.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 22 jun. 2026.

BRASIL. Senado Federal. Lei com penas mais duras contra crimes cibernéticos é sancionada. **Senado Notícias**, Brasília, 28 maio 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada. Acesso em: 22 jun. 2026.

BRASIL. Tribunal Regional Federal (1. Região). TRF1 alerta sobre golpe do falso advogado: entenda como funciona a fraude. **Portal TRF1**, Brasília. Disponível em: https://www.trf1.jus.br/trf1/noticias/trf1-alerta-sobre-golpe-do-falso-advogado-entenda-como-funciona-a-fraude-que-usa-dados-reais-para-enganar-vitimas. Acesso em: 22 jun. 2026.

CHECK POINT. Secure by design: the complete guide. **Check Point Cyber Hub**. Disponível em: https://www.checkpoint.com/pt/cyber-hub/cloud-security/what-is-developer-security/secure-by-design-the-complete-guide/. Acesso em: 22 jun. 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: **Fórum Brasileiro de Segurança Pública**, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 22 jun. 2026.

G1. **Fantástico**: Quadrilhas usam o 'Golpe do Falso Advogado' para roubar suas vítimas. Youtube, 29 out. 2025. 1 vídeo (11 min.). Disponível em: https://www.youtube.com/watch?v=F_f-z7M4v0A. Acesso em: 22 fev. 2026.

GALINDO, G. D. **Evolução do estelionato pelo meio digital**. 2022. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/52a88851-2b2b-46ff-962d-8ab0aad7686c/content. Acesso em: 22 jun. 2026.

GOMINHO, V. D. C. P. Crimes virtuais: o sequestro de dados na doutrina brasileira. **Portal de Trabalhos Acadêmicos**, v. 8, n. 1, 2022. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/2152. Acesso em: 22 jun. 2026.

JESUS, D. de. **Direito penal**: parte especial. 35. ed. São Paulo: Saraiva, 2015. v. 2.

RIGHI IVAHY BADARÓ, G. H. 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://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 22 jun. 2026.

SANTA CATARINA. Polícia Civil. Em Fortaleza, Polícia Civil prende autor de golpe do "Falso Advogado" que causou prejuízo aproximado de R$ 750 mil à idosa de Florianópolis. **Portal da Polícia Civil de SC**, Florianópolis. Disponível em: https://pc.sc.gov.br/?p=39016. Acesso em: 22 jun. 2026.

SOUZA, A. J. S. *et al*. Punitivismo sem resultados: as leis n. 15.397/2026 e 15.358/2024, o populismo penal e o encarceramento em massa no Brasil. **Revista Tópicos**, Rio de Janeiro, v. 4, n. 33, p. 1-26, 2026. Disponível em: https://revistatopicos.com.br/artigos/punitivismo-sem-resultados-as-leis-n-15-397-2026-e-15-358-2024-o-populismo-penal-e-o-encarceramento-em-massa-no-brasil. Acesso em: 22 jun. 2026.

VIEIRA, V. R. N. Golpe do falso advogado e instituições bancárias: jurimetria e responsabilização civil nos TJs (2023–2025). **Revista de Direito da ADVOCEF**, [S. l.], v. 22, n. 41, p. 537-564, 2026. Disponível em: https://revista.advocef.org.br/index.php/ra/article/view/541. Acesso em: 21 jun. 2026.

ZAFFARONI, E. R. **Em busca das penas perdidas**: a perda de legitimidade do sistema penal. 5. ed. Rio de Janeiro: Revan, 2010.