

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
II**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFRSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Clarisse Inês de Oliveira; Valter Moura do Carmo – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-591-0

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

APRESENTAÇÃO

Entre os dias 22 e 26 de junho de 2026, o Conselho Nacional de Pesquisa e Pós-Graduação em Direito realizou o IX Encontro Virtual do CONPEDI, que teve como tema “Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos”. Com a Instituição Toledo de Ensino de Bauru como parceira institucional, o evento reuniu pesquisadoras, pesquisadores, docentes e discentes vinculados a instituições de ensino e programas de pós-graduação de diferentes regiões do país, proporcionando um amplo espaço de apresentação, discussão e circulação da produção científica jurídica.

A programação, composta por palestra científica, painéis, Grupos de Trabalho de artigos e Grupos de Trabalho de pôsteres, permitiu o exame de temas relacionados aos desafios sociais, institucionais e democráticos que marcam o atual cenário jurídico. Ao favorecer o intercâmbio entre pesquisadores com distintas formações e perspectivas teóricas, o Encontro reafirmou a importância da pesquisa jurídica para a compreensão das transformações pelas quais passam o Estado, as instituições e as relações sociais.

Nesse contexto, o Grupo de Trabalho “Direito, Governança e Novas Tecnologias II”, coordenado por Clarisse Inês de Oliveira e Valter Moura do Carmo, reuniu dezenove trabalhos que discutiram os impactos da digitalização e da inteligência artificial sobre o Direito, a Administração Pública, o sistema de justiça, a democracia e o exercício dos direitos fundamentais.

Administração Pública, especialmente em atividades relacionadas à implementação de políticas públicas e à concessão de benefícios. O autor sustentou que o monitoramento e a avaliação não devem ocupar posição meramente gerencial, mas constituir mecanismos permanentes de preservação da legalidade, da accountability e da legitimidade democrática das decisões estatais automatizadas.

Na sequência, o artigo “Letramento digital na assessoria jurídica popular: introduzindo noções de algoritmo e inteligência artificial aos assistidos do Núcleo de Prática Jurídica”, de Clarisse Inês de Oliveira e Patrícia Garcia dos Santos, tratou da necessidade de promover o letramento digital dos jurisdicionados atendidos pelos Núcleos de Prática Jurídica. As autoras destacaram que o conhecimento mínimo acerca do funcionamento dos algoritmos e dos limites do emprego da inteligência artificial na advocacia e no Poder Judiciário constitui condição para uma participação consciente dos assistidos na condução de suas demandas.

O trabalho “Inclusão digital e serviços notariais: limites e potencialidades da plataforma e-Notariado à luz do constitucionalismo digital”, de Lígia Maria Silva Quaresma e José Carlos Francisco dos Santos, analisou a digitalização dos serviços notariais e as dificuldades enfrentadas pelos usuários da plataforma e-Notariado. Os autores compreenderam a inclusão digital como direito instrumental ao exercício da cidadania e de outros direitos, destacando a necessidade de ações de capacitação, particularmente em favor das pessoas idosas e daquelas que se encontram em situação de vulnerabilidade.

Em “Hermenêutica algorítmica e o dever de fundamentação das decisões judiciais”, Marcos Vinicius Conaciani de Souza e Flávio Luís de Oliveira investigaram a compatibilidade entre o emprego de sistemas algorítmicos no processo decisório judicial e o dever constitucional de fundamentação. Os autores defenderam que o uso dessas ferramentas deve ser acompanhado de mecanismos de transparência, explicabilidade e auditabilidade, além de um regime de responsabilidade compartilhada entre magistrados, tribunais e desenvolvedores.

decisões automatizadas sobre os direitos da personalidade, a privacidade, a igualdade e a autonomia informacional. O estudo questionou a suficiência dos modelos tradicionais de responsabilidade civil para o enfrentamento dos riscos algorítmicos e ressaltou a importância da supervisão humana, da prevenção de danos e da rastreabilidade das decisões.

As repercussões das novas tecnologias sobre a democracia e o processo eleitoral foram objeto do trabalho “Deep fakes e os riscos à democracia no contexto eleitoral: análise da insuficiência do ordenamento jurídico brasileiro e das alternativas regulatórias”, de Luiz Felipe de Farias Leite Borges e Glaucia Maria de Araújo Ribeiro. Os autores analisaram a capacidade dos conteúdos sintéticos de manipular a opinião pública e comprometer a integridade eleitoral, propondo uma resposta regulatória que articule atuação estatal, responsabilidade das plataformas e instrumentos tecnológicos de transparência e rastreabilidade.

Em “Golpe do ‘falso advogado’: estelionato digital, responsabilidade institucional e os limites da publicidade processual na era do processo eletrônico”, Murillo Silva da Rosa e Catarina Ribeiro Bragança Marques examinaram uma modalidade de fraude baseada na utilização de dados verdadeiros retirados de processos judiciais eletrônicos. O artigo discutiu a tensão entre publicidade processual e proteção de dados pessoais, bem como as responsabilidades dos tribunais e das instituições diante de golpes que atingem, sobretudo, pessoas idosas e outros indivíduos em situação de vulnerabilidade.

A proteção da infância no ambiente digital foi discutida no artigo “ECA Digital e monetização algorítmica da infância: governança de plataformas, proteção integral e responsabilidade digital”, de Andre Canuto Bezerra e Júlia Terra Nova dos Santos. Os autores abordaram a conversão da imagem, da rotina e dos dados de crianças e adolescentes em ativos econômicos, questionando se o ECA Digital oferece instrumentos suficientes para enfrentar o sharenting comercial, a publicidade direcionada, o impulsionamento pago e os sistemas de recomendação que favorecem a exploração econômica da exposição infantil.

Em “Controle e consumo na era digital: explorando o regime da informação no capitalismo através das perspectivas de Byung-Chul Han”, Andrezza Damasceno Machado, Felipe Ryuji Coimbra Miyamoto e Felipe Yasuhiro Mira Coimbra Miyamoto analisaram as transformações do capitalismo digital a partir dos conceitos de psicopolítica e infocracia. Os autores refletiram sobre a forma como a coleta e o tratamento de dados permitem influenciar comportamentos, orientar o consumo e produzir uma percepção de liberdade inserida em estruturas cada vez mais sofisticadas de controle.

O artigo “Constitucionalismo digital e equidade algorítmica: como combater os efeitos discriminatórios decorrentes do (mau) uso da inteligência artificial”, de Gabriella do Carmo Pantoja Duarte, abordou a reprodução de padrões discriminatórios por sistemas de inteligência artificial treinados com bases de dados enviesadas. A autora ressaltou que a alimentação humana dos sistemas pode perpetuar estereótipos e desigualdades históricas, razão pela qual defendeu mecanismos de rastreabilidade, supervisão humana, auditabilidade, explicabilidade e avaliação de impactos.

Em “Inteligência artificial: capitalismo de plataforma, desafios éticos e regulatórios no Brasil contemporâneo”, Irineu Francisco Barreto Junior discutiu a inteligência artificial no contexto do capitalismo de plataforma e da Sociedade da Informação. O estudo abordou a monetização de dados, a vigilância digital, as bolhas informacionais, a opacidade algorítmica e seus efeitos sobre a democracia, a privacidade e a autodeterminação informativa, defendendo a construção de parâmetros éticos e de um modelo regulatório policêntrico.

O trabalho “Chatbots sonham com advogados elétricos? Sobre regulamentação da inteligência artificial no contexto de crítica social”, de Bruno Gadelha Xavier e Amanda Schmid, examinou casos envolvendo interações entre usuários vulneráveis e sistemas automatizados de conversação. Os autores analisaram falhas dos mecanismos de segurança diante de sinais de sofrimento psicológico, automutilação e comportamento suicida, discutindo as dificuldades de imputação de responsabilidade civil e penal às empresas

No trabalho “A metamorfose do mediador judicial na Justiça 4.0: vulnerabilidade, datificação e democracia”, Juliana de Oliveira Sampaio Souto Queiroga e José Alexandre Ricciardi Sbizzera analisaram criticamente os efeitos da digitalização sobre a mediação judicial. Os autores destacaram que a submissão da atividade a metas, métricas e protocolos padronizados pode converter o mediador em gestor de fluxos institucionais, comprometendo as dimensões ética, relacional e democrática da mediação, particularmente em conflitos familiares marcados por vulnerabilidades.

Em “A memória de Funes: do direito ao esquecimento à gradação de remédios contra a hiperexposição algorítmica”, Thamires Ribas Lopes Smith, Rodrigo Plack Ferreira e Cláudio Augusto Diana Terra partiram do conto de Jorge Luis Borges para refletir sobre uma sociedade digital que registra e recupera indefinidamente acontecimentos da vida das pessoas. À luz do Tema 786 do Supremo Tribunal Federal, o estudo examinou os instrumentos jurídicos que permanecem disponíveis contra a circulação desproporcional e descontextualizada de informações, propondo uma gradação entre contextualização, desindexação e exclusão.

O artigo “Inclusão e exclusão digital no Brasil: o papel ambivalente da conectividade e novas tecnologias no acesso ao Direito”, de Jamerson Lima dos Santos, abordou as diferentes dimensões da exclusão digital e seus efeitos sobre o exercício da cidadania e o acesso à justiça. O autor demonstrou que a simples disponibilização de serviços digitais não assegura acesso efetivo, sobretudo quando persistem obstáculos relacionados à infraestrutura, ao custo da conectividade e à ausência de habilidades para utilização das tecnologias.

Encerrando o conjunto de pesquisas, o trabalho “A possibilidade do desenvolvimento da ação comunicativa entre adolescentes na era digital”, de Samira Bonfim Bernardi, analisou as relações comunicativas estabelecidas por adolescentes nas plataformas digitais a partir da teoria de Jürgen Habermas e do princípio da proteção integral. A autora reconheceu que esses ambientes ampliam as possibilidades de expressão e participação, mas observou que a

As discussões também evidenciaram a ambivalência que acompanha as novas tecnologias. Os mesmos instrumentos capazes de ampliar a eficiência administrativa, facilitar o acesso a serviços e favorecer a circulação de informações podem aprofundar desigualdades, reproduzir discriminações, intensificar formas de controle e expor a pessoa a riscos ainda não inteiramente alcançados pelas categorias jurídicas tradicionais. Essa constatação afasta tanto a aceitação acrítica da inovação quanto sua rejeição automática, impondo uma análise atenta aos contextos em que as tecnologias são desenvolvidas e utilizadas.

Os coordenadores agradecem aos autores pela qualidade das pesquisas apresentadas e pela contribuição aos debates realizados durante o Grupo de Trabalho. É necessário um agradecimento especial à monitora do Grupo de Trabalho, Maria Eduarda, pela dedicação, organização e apoio prestado durante a condução das apresentações e dos debates.

Espera-se que os artigos reunidos nestes anais contribuam para o aprofundamento das reflexões sobre Direito, governança e novas tecnologias e para a formulação de respostas institucionais que permitam aproveitar os benefícios da inovação sem desconsiderar os riscos que ela pode representar para a dignidade humana, a igualdade, a democracia e os direitos fundamentais.

Boa leitura!

Profa. Dra. Clarisse Inês de Oliveira

Universidade Federal Fluminense

Prof. Dr. Valter Moura do Carmo

Escola Superior da Magistratura Tocantinense (ESMAT)

**GOLPE DO "FALSO ADVOGADO": ESTELIONATO DIGITAL,
RESPONSABILIDADE INSTITUCIONAL E OS LIMITES DA PUBLICIDADE
PROCESSUAL NA ERA DO PROCESSO ELETRÔNICO**

**“FAKE LAWYER” SCAM: DIGITAL FRAUD, INSTITUTIONAL LIABILITY, AND
THE LIMITS OF PROCEDURAL PUBLICITY IN THE AGE OF ELECTRONIC
COURT PROCEEDINGS**

**Murillo Silva da Rosa
Catarina Ribeiro Bragança Marques**

Resumo

O presente artigo analisa o golpe do "falso advogado" como fenômeno jurídico multidimensional que mobiliza o direito penal, a proteção de dados pessoais, o processo civil eletrônico e a responsabilidade institucional do Estado, dos tribunais e da Ordem dos Advogados do Brasil. A partir da identificação do modus operandi da fraude, que consiste na apropriação de dados reais extraídos do Processo Judicial Eletrônico (PJe) para simular a identidade de profissionais do Direito e induzir partes litigantes à realização de transferências bancárias indevidas, o artigo examina a tipificação penal da conduta à luz da Lei n.º 14.155/2021, que qualificou o estelionato praticado por meios eletrônicos. Em seguida, enfrenta a tensão normativa entre o princípio constitucional da publicidade dos atos processuais e os deveres de proteção de dados pessoais impostos pela Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), apontando a ausência de solução legislativa precisa para esse conflito no ambiente do processo eletrônico. Por fim, investiga os fundamentos da responsabilidade civil do Estado por omissão na adoção de medidas de segurança informacional e avalia as respostas institucionais em curso, como a implementação de autenticação em dois fatores pelo Conselho Nacional de Justiça e as campanhas institucionais da OAB. A metodologia adotada é bibliográfica, documental e normativa. Conclui-se que o enfrentamento eficaz da fraude exige reforma normativa coordenada, adoção do princípio de privacy by design nos sistemas de processo eletrônico e definição clara dos critérios de responsabilidade estatal.

transfers, the article examines the criminal classification of the conduct in light of Law No. 14,155/2021, which qualified fraud committed by electronic means. It then addresses the normative tension between the constitutional principle of procedural publicity and the duties of personal data protection imposed by the General Data Protection Law (Law No. 13,709/2018), pointing to the absence of a precise legislative solution to this conflict in the electronic process environment. Finally, it investigates the legal basis for State civil liability for omission in the adoption of informational security measures and evaluates ongoing institutional responses. The methodology is bibliographic, documentary and normative. The conclusion is that effective combating of the fraud requires coordinated normative reform, adoption of the privacy by design principle in electronic judicial systems and clear definition of state liability criteria.

Keywords/Palabras-claves/Mots-clés: Fake lawyer scam, Digital fraud, Procedural publicity, Personal data protection, State liability

1 INTRODUÇÃO

A digitalização do sistema judicial brasileiro produziu transformações que vão muito além da substituição do papel pelo arquivo eletrônico. O Processo Judicial Eletrônico (PJe), instituído no plano legislativo pela Lei n.º 11.419/2006, reorganizou a arquitetura do acesso à Justiça e conferiu maior celeridade à tramitação dos feitos, mas também criou uma superfície de ataque que agentes criminosos exploram com sofisticação crescente.

A manifestação mais visível desse fenômeno é o chamado golpe do "falso advogado": uma modalidade de estelionato digital em que criminosos se apropriam de dados reais disponíveis nos sistemas eletrônicos de processo para se apresentar, perante as partes litigantes, como os advogados que as representam, induzindo-as à realização de transferências bancárias indevidas. A fraude alcançou escala nacional relevante ao longo de 2025, motivando operações policiais, campanhas institucionais da Ordem dos Advogados do Brasil e alertas de tribunais federais em diversas regiões do país.

O fenômeno revela uma tensão normativa que o ordenamento jurídico brasileiro ainda não resolveu com precisão suficiente: de um lado, o princípio constitucional da publicidade dos atos processuais, assegurado pelo art. 5.º, inciso LX, e pelo art. 93, inciso IX, da Constituição Federal de 1988, como garantia de controle social sobre o exercício da jurisdição; de outro, os deveres de proteção de dados pessoais estabelecidos pela Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), que impõem ao tratamento de informações de pessoas naturais condições de segurança, adequação e minimização que não se harmonizam, sem tensão, com a ampla publicidade processual.

O problema de pesquisa que orienta este artigo pode ser formulado nos seguintes termos: em que medida a configuração atual do processo eletrônico brasileiro, especialmente no que diz respeito à publicidade de dados pessoais das partes e de seus patronos, cria condições normativas e tecnológicas para a ocorrência do golpe do falso advogado, e quais são os instrumentos jurídicos disponíveis para prevenir a fraude e responsabilizar os atores institucionais omissos?

Para responder a esse problema, o artigo divide-se em quatro seções de desenvolvimento. A primeira examina o *modus operandi* da fraude e sua dimensão empírica. A segunda analisa a tipificação penal da conduta, com ênfase nas qualificadoras introduzidas pela Lei n.º 14.155/2021. A terceira enfrenta a tensão entre publicidade processual e LGPD no ambiente do PJe. A quarta investiga a responsabilidade institucional do Estado, dos tribunais, da OAB e dos próprios advogados. Ao final, são apresentadas propostas de aperfeiçoamento

normativo e institucional. A metodologia é bibliográfica, documental e normativa, com análise de legislação, doutrina, jurisprudência e fontes institucionais verificáveis.

2 O GOLPE DO FALSO ADVOGADO: CARACTERIZAÇÃO DA CONDUTA E DIMENSÃO EMPÍRICA

O golpe do "falso advogado" pertence à categoria dos estelionatos de engenharia social digital: fraudes em que a persuasão não se funda em falsidades genéricas, mas na apresentação de informações verdadeiras sobre a vítima, criando uma aparência de legitimidade que desativa o seu juízo crítico. É exatamente essa característica que distingue essa modalidade de outras fraudes eletrônicas e confere ao tema relevância jurídica específica.

O *modus operandi* é relativamente uniforme. O agente criminoso acessa o sistema do Processo Judicial Eletrônico, que na maior parte dos tribunais brasileiros é de consulta pública, e coleta dados reais do processo: nome da parte, número dos autos, nome e número de inscrição na OAB do advogado constituído, vara e comarca, e até o teor de decisões recentes. De posse dessas informações, o estelionatário entra em contato com a parte litigante, geralmente por aplicativo de mensagens como WhatsApp, apresentando-se como o advogado que a representa e anunciando uma vantagem processual iminente, como a liberação de valores, o resultado favorável em julgamento ou a necessidade de pagamento de custas para que determinado ato seja praticado. A vítima, que reconhece os dados mencionados como corretos, tende a confiar na comunicação e realiza a transferência solicitada, apenas descobrindo o golpe posteriormente (RODRIGUES; MARTINS; AMORIM, 2025).

Reportagem do programa Fantástico, exibida pela Rede Globo em outubro de 2025, documentou a existência de grupos criminosos organizados que atuavam com divisão de tarefas: alguns integrantes eram responsáveis pela coleta e sistematização dos dados processuais, outros pela abordagem das vítimas e outros pelo recebimento e movimentação dos valores obtidos (G1, 2025). Em julho do mesmo ano, operação policial realizada em São Paulo identificou estelionatários que utilizavam cartilhas padronizadas para orientar a execução do golpe, sugerindo a profissionalização e a escala da atividade criminosa (GAÚCHAZH, 2025; CORREIO BRAZILIENSE, 2025b). O Correio Braziliense também noticiou, em maio de 2025, que os criminosos cruzavam dados do PJe com informações obtidas em redes sociais para personalizar ainda mais a abordagem às vítimas (CORREIO BRAZILIENSE, 2025a).

A Ordem dos Advogados do Brasil, em resposta ao aumento dos casos, lançou, em abril de 2025, uma campanha nacional de prevenção e uma plataforma digital de verificação de

identidade de advogados, além de publicar cartilhas em diversas seções estaduais, entre elas São Paulo, Rio de Janeiro e Ceará (ORDEM DOS ADVOGADOS DO BRASIL, 2025). O Tribunal Regional Federal da 3.^a Região e o Tribunal Regional Federal da 1.^a Região também emitiram alertas públicos e desenvolveram campanhas informativas para orientar os jurisdicionados (TRIBUNAL REGIONAL FEDERAL DA 3.^a REGIÃO, 2025; TRIBUNAL REGIONAL FEDERAL DA 1.^a REGIÃO, 2025a).

Do ponto de vista criminológico, o perfil das vítimas tende a incluir pessoas com processos judiciais em andamento que envolvem expectativa de recebimento de valores, como trabalhadores com ações previdenciárias ou trabalhistas, beneficiários do INSS em litígio e partes em ações de cobrança. A vulnerabilidade dessas vítimas não é apenas econômica: decorre do desconhecimento sobre o funcionamento do processo judicial, que as torna incapazes de identificar, por si mesmas, que advogados não costumam solicitar transferências bancárias por aplicativos de mensagem. Essa combinação de dado verdadeiro com narrativa fraudulenta é o que torna o golpe eficaz e, ao mesmo tempo, juridicamente complexo, pois ele não seria possível sem o acesso às informações processuais públicas, o que situa o debate muito além da criminalidade comum e impõe uma reflexão sobre as condições normativas que o viabilizam.

3 TIPIFICAÇÃO PENAL: ESTELIONATO DIGITAL E CRIMES CONEXOS

3.1 O tipo penal do estelionato e a qualificadora eletrônica

A conduta central do golpe do falso advogado enquadra-se no tipo penal do estelionato, previsto no art. 171 do Código Penal. O caput do dispositivo descreve o crime na sua forma básica: 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, com pena de reclusão de um a cinco anos e multa. Para a configuração do tipo, a doutrina exige a presença de três elementos estruturais: o meio fraudulento, o induzimento ou manutenção em erro e a obtenção de vantagem ilícita em detrimento da vítima. No golpe do falso advogado, todos esses elementos estão presentes: o meio fraudulento é a usurpação de identidade do advogado mediante uso de dados processuais reais; o erro consiste na crença da vítima de que está se comunicando com o seu representante legal; e a vantagem ilícita é o valor transferido mediante essa falsa crença.

Mais relevante para o caso em análise é o § 2.º-A do art. 171 do Código Penal, acrescido pela Lei n.º 14.155, de 27 de maio de 2021. Esse dispositivo qualifica o estelionato quando a fraude é cometida com a utilização de informações fornecidas pela própria 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 similar, elevando a pena para reclusão de quatro a oito anos, além de multa. O golpe do falso advogado se enquadra com precisão na cláusula residual "qualquer outro meio fraudulento similar", pois utiliza contato por aplicativo de mensagem para induzir a vítima em erro.

A Lei n.º 14.155/2021 surgiu em resposta ao crescimento expressivo das fraudes digitais no Brasil, especialmente durante o período de distanciamento social provocado pela pandemia de Covid-19, e representa um avanço relevante na tutela penal das relações mediadas por tecnologia. No entanto, como observam Rodrigues, Martins e Amorim (2025), a norma ainda não havia produzido impacto significativo sobre a frequência do golpe do falso advogado ao longo de 2025, o que sugere que a resposta penal, embora necessária, não é suficiente por si só para coibir o fenômeno.

Há ainda uma qualificadora adicional prevista no § 2.º-B do art. 171, introduzido pela mesma lei, que aumenta a pena em um terço quando a vítima é idosa, nos termos da Lei n.º 10.741/2003. Considerando o perfil das vítimas desse golpe, frequentemente aposentados e pensionistas envolvidos em ações previdenciárias, essa qualificadora tem aplicação concreta no contexto em exame e reforça o dever de atenção que os órgãos investigativos e o Ministério Público devem dispensar a essas situações.

3.2 Crimes conexos e concurso de delitos

A conduta dos estelionatários não se esgota no crime patrimonial. O agente que se apresenta como advogado, utilizando o nome verdadeiro e o número de OAB de um terceiro, pratica, concomitantemente, o crime de falsa identidade, tipificado no art. 307 do Código Penal: atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem. A pena cominada é de detenção de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

A questão do concurso de crimes entre estelionato e falsa identidade não é pacífica na jurisprudência brasileira. Uma corrente entende que a falsa identidade seria crime-meio absorvido pelo estelionato, na linha do princípio da consunção, desde que praticado com o fim exclusivo de viabilizar a fraude patrimonial. Outra corrente sustenta a autonomia dos tipos e o concurso formal, especialmente quando a falsa atribuição de identidade afeta bens jurídicos distintos: não apenas o patrimônio da vítima, mas também a honra profissional e a imagem do advogado cujo nome foi usurpado, que pode ter sua reputação prejudicada pela associação com a fraude. O Superior Tribunal de Justiça tem precedentes em ambas as direções, a depender das

circunstâncias concretas do caso, razão pela qual se recomenda verificar a orientação jurisprudencial mais recente antes de adotar posição definitiva sobre o tema.

Quando a fraude é praticada por organização criminosa estruturada com divisão de tarefas, como os grupos identificados nas operações policiais de julho de 2025 (GAÚCHAZH, 2025), incide também a Lei n.º 12.850/2013, que define organização criminosa e estabelece penas autônomas, além de regime diferenciado de investigação que inclui colaboração premiada, ação controlada e infiltração policial. A existência de cartilhas de treinamento para novos integrantes, documentada em reportagens jornalísticas, é indício robusto de estrutura hierárquica estável, elemento caracterizador da organização criminosa para fins dessa lei.

3.3 Competência, prova digital e investigação

No plano processual penal, a competência para apurar o crime deve ser definida conforme o local da consumação do delito, nos termos do art. 70 do Código de Processo Penal. Quando a fraude envolve valores depositados judicialmente em processos federais, ou quando os dados explorados foram extraídos de sistema administrado por tribunal federal, surgem argumentos para cogitar da competência da Justiça Federal, com base no art. 109, inciso IV, da Constituição Federal, pois a atividade criminosa atinge, ainda que reflexamente, a credibilidade do sistema de Justiça federal. Nos demais casos, aplica-se a regra geral da Justiça Estadual.

A prova digital adquire centralidade na persecução penal do golpe do falso advogado. Registros de conversas nos aplicativos de mensagens, dados de transferências bancárias, endereços de IP utilizados no acesso ao PJe e logs dos sistemas judiciais são os principais elementos probatórios disponíveis. A obtenção dessas provas requer, em regra, autorização judicial: para o acesso a registros telemáticos armazenados, como conversas em aplicativos de mensagem, aplica-se o Marco Civil da Internet (Lei n.º 12.965/2014); para a interceptação de comunicações em fluxo, a Lei n.º 9.296/1996; e para o afastamento de sigilo bancário e financeiro, a Lei Complementar n.º 105/2001. Embora a Lei n.º 13.964/2019 (Pacote Anticrime) tenha introduzido os arts. 158-A a 158-F no Código de Processo Penal, disciplinando a cadeia de custódia da prova, essa regulamentação foi concebida primordialmente para provas físicas e revela-se insuficiente diante das especificidades da prova digital, o que pode comprometer a validade desses elementos em juízo, especialmente quando coletados pelas próprias vítimas sem o auxílio de especialistas forenses (FILHO; CASTRO; UGALDE, 2025 apud PESSOA et al., 2026).

4 O PJE COMO VETOR DE VULNERABILIDADE: PUBLICIDADE PROCESSUAL E PROTEÇÃO DE DADOS

4.1 O princípio constitucional da publicidade e sua projeção no processo eletrônico

A publicidade dos atos processuais é garantia constitucional de dupla dimensão: protege a parte no processo, assegurando transparência no exercício do poder jurisdicional, e serve ao controle social democrático sobre as instituições judiciárias. O art. 5.º, inciso LX, da Constituição Federal estabelece que a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem, e o art. 93, inciso IX, determina que todos os julgamentos dos órgãos do Poder Judiciário serão públicos. No plano infraconstitucional, os arts. 11 e 189 do Código de Processo Civil de 2015 concretizam esse princípio, admitindo o segredo de justiça apenas nas hipóteses taxativamente previstas.

No ambiente digital, a publicidade processual ganhou um alcance que seus arquitetos não anteciparam. Se antes o acesso aos autos exigia presença física no fórum e consulta ao cartório, hoje qualquer pessoa pode, de qualquer ponto do território nacional, acessar o conteúdo de processos em tramitação, incluindo o nome completo das partes, o CPF em alguns sistemas, o endereço, dados financeiros constantes das peças processuais e, crucialmente, o nome e o número de inscrição na OAB do advogado constituído. Essa acessibilidade é, ao mesmo tempo, a virtude democrática do sistema e sua vulnerabilidade mais explorada pelos agentes criminosos (BEZERRA; PEREIRA; COSTA, 2026; PESSOA et al., 2026). O que era instrumento de transparência converte-se, quando mal calibrado, em insumo para a fraude.

4.2 A LGPD e sua aplicação ao ambiente processual

A Lei n.º 13.709/2018 (LGPD) estabelece um conjunto de princípios para o tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (art. 6.º). O art. 2.º elenca os fundamentos que justificam a proteção de dados pessoais, entre os quais o respeito à privacidade, à autodeterminação informativa, à inviolabilidade da intimidade, da honra e da imagem, e ao livre desenvolvimento da personalidade.

A aplicação da LGPD ao ambiente processual enfrenta, contudo, uma tensão estrutural. O art. 4.º, inciso III, da própria lei exclui de seu âmbito os tratamentos realizados para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais. No caso do processo judicial, a questão é mais sutil: o tratamento de dados nas plataformas processuais não se destina a fins de segurança

pública, mas o princípio da publicidade processual tem assento constitucional que a lei ordinária não pode suprimir, o que cria uma zona cinzenta normativa que nenhum dos dois diplomas resolve com precisão.

Essa tensão é identificada por Bezerra, Pereira e Costa (2026) como o nó central do problema: nem a publicidade pode ser suprimida a pretexto de proteção de dados, nem a proteção de dados pode ser ignorada em nome de uma publicidade irrestrita que já não serve ao seu propósito democrático quando utilizada como instrumento de fraude. A solução, como defendem os autores, está na calibragem do que deve ser público e em que formato, distinguindo a publicidade necessária ao controle social da exposição de dados que apenas alimenta a vulnerabilidade das partes.

O princípio da minimização de dados, derivado do princípio da necessidade previsto no art. 6.º, inciso III, da LGPD, oferece um critério interpretativo relevante: apenas os dados estritamente necessários ao exercício do direito de publicidade dos atos processuais devem ser tornados amplamente acessíveis sem qualquer credenciamento. O número de CPF de uma parte, por exemplo, não é necessário para que um terceiro compreenda o andamento de um processo, mas é suficiente para que um fraudador confirme a identidade da vítima antes de aplicar o golpe. Essa distinção, porém, ainda carece de regulamentação específica, e a Autoridade Nacional de Proteção de Dados (ANPD) não produziu, até o momento, diretrizes dirigidas especificamente ao ambiente processual.

4.3 Respostas institucionais em curso e suas limitações

O Conselho Nacional de Justiça iniciou, em novembro de 2025, a implementação de autenticação em dois fatores para usuários credenciados do PJe, medida que representa avanço relevante na segurança de acesso ao sistema pelos advogados e demais operadores do Direito (TRIBUNAL REGIONAL FEDERAL DA 1.ª REGIÃO, 2025b). Alguns tribunais estaduais e federais adotaram restrições de acesso a determinadas categorias de dados, como números de CPF e endereços, em consultas abertas ao público, mantendo essas informações disponíveis apenas para usuários credenciados.

Essas iniciativas são louváveis, mas permanecem fragmentadas e insuficientes. Na ausência de orientação normativa uniforme do CNJ, cada tribunal decide autonomamente o que restringir e o que manter público, gerando disparidade de proteção entre jurisdições. Há, ainda, o problema mais profundo que a autenticação em dois fatores não resolve: o fraudador não precisa acessar o sistema como advogado para coletar os dados das vítimas. Basta-lhe a consulta pública aberta, que permite a qualquer pessoa visualizar os autos sem qualquer credenciamento.

É esse vetor de acesso que ainda carece de disciplina normativa específica (RODRIGUES; MARTINS; AMORIM, 2025; PESSOA et al., 2026).

5 RESPONSABILIDADE INSTITUCIONAL: ESTADO, TRIBUNAIS, OAB E ADVOGADOS

5.1 A responsabilidade civil do Estado por omissão na proteção de dados processuais

A Constituição Federal estabelece, no art. 37, § 6.º, a responsabilidade objetiva do Estado pelos danos que seus agentes causarem a terceiros no exercício de suas funções. A doutrina e a jurisprudência do Supremo Tribunal Federal têm reconhecido que essa responsabilidade objetiva alcança tanto os danos causados por ação direta dos agentes estatais quanto os decorrentes de omissão específica do Estado, entendida como aquela em que havia dever legal de agir para evitar o dano e o Estado permaneceu inerte. A distinção entre omissão genérica e omissão específica é o critério que define a aplicabilidade da responsabilidade objetiva: na omissão genérica, a teoria objetiva temperada adotada pelo STF afasta a responsabilidade automática; na omissão específica, o fundamento constitucional da responsabilidade objetiva se sustenta com maior solidez.

No contexto do golpe do falso advogado, a questão que se coloca é se o Poder Judiciário, por intermédio dos tribunais que administram os sistemas de processo eletrônico, tem o dever legal de adotar medidas de segurança informacional que previnam a extração e utilização indevida de dados processuais para fins fraudulentos. A LGPD, em seu art. 43, estabelece que os controladores de dados só se eximem de responsabilidade quando demonstrarem que não realizaram o tratamento de dados que lhes é atribuído, que, embora o tenham realizado, não houve violação à legislação de proteção de dados, ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. O art. 44, por sua vez, prevê que o tratamento é irregular quando não fornece a segurança que o titular dele pode razoavelmente esperar.

Pessoa et al. (2026) observam que a responsabilidade civil do Estado por danos decorrentes de fraudes que exploram vulnerabilidades dos sistemas de processo eletrônico permanece juridicamente indefinida no direito brasileiro, pela ausência de regulamentação específica que defina critérios claros de imputação, mecanismos de reparação e limites da responsabilidade em contextos de omissão digital. Essa indefinição não é apenas um problema acadêmico: ela desincentiva as vítimas de buscar reparação judicial e retira dos tribunais o estímulo para investir em medidas preventivas mais robustas. A hipótese de que, uma vez

notificados da existência e da escala do golpe, os tribunais que mantiveram sistemas de consulta pública ampla sem qualquer filtro de minimização de dados podem ter incorrido em omissão específica é plausível e merece ser testada na via judicial.

Importa registrar, contudo, que a responsabilidade civil do Estado não equivale à responsabilidade penal dos seus agentes. Salvo nos casos em que servidores ou magistrados tenham concorrido dolosamente para o acesso indevido a dados processuais, a responsabilidade estatal aqui discutida é de natureza objetiva, fundada na inadequação do sistema, e não na culpa individual de quem quer que seja.

5.2 Deveres institucionais da OAB

A Ordem dos Advogados do Brasil, enquanto entidade de classe com função constitucional de defesa da ordem jurídica e dos direitos dos advogados (art. 44 da Lei n.º 8.906/1994), desempenhou papel ativo no enfrentamento do golpe do falso advogado a partir de 2025. A campanha nacional com plataforma de verificação de identidade profissional, as cartilhas elaboradas pelas seções estaduais e os protocolos de orientação aos advogados são iniciativas que merecem reconhecimento. No entanto, essas respostas foram, em sua maioria, reativas, formuladas após a escalada do problema e não em antecipação a ele.

Há nesse ponto uma tensão análoga à da publicidade processual: a OAB disponibiliza em sua página institucional os dados cadastrais dos advogados inscritos, incluindo nome, número de inscrição, seccional e situação, para permitir que o público verifique a regularidade dos profissionais, o que é uma exigência legítima de transparência e de proteção dos jurisdicionados contra o exercício irregular da advocacia. Contudo, essas mesmas informações servem ao fraudador para conferir autenticidade à sua abordagem, criando um paradoxo em que o instrumento de proteção torna-se, simultaneamente, insumo para a fraude. A solução não está em suprimir essa publicidade, mas em aprimorar os mecanismos de verificação de identidade no momento do contato entre o advogado e o cliente.

Iniciativas como a criação de QR codes verificáveis nos cartões profissionais e a disponibilização de canais de confirmação de identidade em tempo real representam caminhos promissores que algumas seções estaduais já estão explorando. A OAB-SP, por exemplo, criou mecanismo específico de prevenção de crimes no âmbito de sua força-tarefa contra o golpe do falso advogado (OAB-SP, 2025b). A generalização dessas práticas para o conjunto do sistema OAB, por deliberação do Conselho Federal, seria medida de elevado impacto preventivo.

5.3 Deveres do advogado perante seus constituintes

A dimensão frequentemente negligenciada no debate é a responsabilidade do advogado individualmente considerado. O Estatuto da Advocacia e o Código de Ética e Disciplina da OAB impõem ao profissional deveres de diligência, lealdade e comunicação clara com seus clientes. Quando o advogado deixa de orientar expressamente seus constituintes sobre as formas seguras de comunicação, informando, por exemplo, que jamais solicitará transferências bancárias por aplicativo de mensagem e fornecendo um canal de contato verificado, contribui, por omissão, para a vulnerabilidade que o golpe explora.

Isso não implica atribuir ao advogado responsabilidade civil pelos danos causados pela fraude de terceiros, cujo nexos causal determinante é a conduta criminosa dos estelionatários. Mas o dever de diligência, previsto no art. 2.º do Código de Ética e Disciplina da OAB, inclui o dever de alertar o cliente sobre riscos previsíveis relacionados ao processo. O golpe do falso advogado, dada sua ampla notoriedade ao longo de 2025, já pode ser considerado um risco previsível que o profissional tem o dever funcional de comunicar preventivamente. A inclusão de cláusula informativa nos contratos de prestação de serviços advocatícios, descrevendo os canais verificados de comunicação e alertando sobre o golpe, é medida simples, sem custo e de alta eficácia preventiva.

6 LACUNAS NORMATIVAS E PROPOSTAS DE APERFEIÇOAMENTO

6.1 A ausência de regulamentação específica para o conflito publicidade-privacidade

O golpe do falso advogado expõe uma lacuna normativa estrutural: não existe, no ordenamento jurídico brasileiro, uma regra que defina, com precisão, quais dados pessoais de partes e advogados devem ser tornados públicos nos sistemas de processo eletrônico, em que formato, para quem e com quais restrições de acesso. O conflito entre publicidade processual e proteção de dados pessoais é reconhecido pela literatura jurídica mais recente (BEZERRA; PEREIRA; COSTA, 2026; RODRIGUES; MARTINS; AMORIM, 2025; PESSOA et al., 2026), mas ainda não encontrou solução normativa específica, seja por lei, seja por resolução do CNJ, seja por instrução da ANPD. Essa omissão regulatória produz consequências práticas concretas: os tribunais decidem autonomamente o que proteger, gerando disparidades de proteção entre jurisdições; as vítimas não encontram critérios jurídicos claros para pleitear reparação; e os fraudadores continuam explorando dados que o próprio Estado coloca à disposição pública.

6.2 O princípio de privacy by design como vetor de reforma

O princípio de *privacy by design*, consolidado no Regulamento Geral de Proteção de Dados da União Europeia (RGPD/2016), estabelece que a proteção de dados pessoais deve ser incorporada desde a concepção dos sistemas, e não acrescentada como resposta a incidentes já ocorridos. Aplicado ao processo eletrônico, esse princípio exigiria que os sistemas de PJe fossem projetados para distinguir automaticamente os dados necessários à publicidade dos atos processuais dos que devem ser protegidos, mediante mecanismos de anonimização, tokenização ou acesso diferenciado por nível de credenciamento (REIS; SAIKALI; FREITAS, 2022 apud PESSOA et al., 2026).

A adoção do *privacy by design* no processo eletrônico brasileiro não implica restringir o acesso à Justiça nem suprimir a transparência democrática. Implica repensar o que precisa ser público para que essa transparência seja alcançada. O número do processo, o tipo de ação, o andamento processual e o nome do juiz são informações cuja publicidade serve ao controle democrático sobre o exercício da jurisdição. O CPF da parte, seu endereço residencial e o número de celular do advogado não servem a esse propósito, mas são exatamente as categorias de dados que os fraudadores utilizam para personalizar o golpe e conferir verossimilhança à abordagem criminosa.

A comparação com o sistema europeu é instrutiva. O RGPD não veda a publicidade dos atos processuais, mas impõe que os dados pessoais disponibilizados nesses atos sejam estritamente os necessários para a finalidade que justifica sua divulgação, com medidas técnicas de pseudonimização e controle de acesso. Experiências de anonimização de dados em sistemas judiciais de países como Portugal e Alemanha demonstram que é possível compatibilizar publicidade e proteção de dados sem comprometer a função democrática da transparência judicial (TAVARES; ALVAREZ apud BEZERRA; PEREIRA; COSTA, 2026).

6.3 Propostas concretas de aperfeiçoamento

A partir do diagnóstico apresentado, identificam-se ao menos quatro linhas de atuação que o ordenamento jurídico brasileiro deve perseguir de forma coordenada. A primeira é a edição de resolução pelo CNJ que estabeleça critérios uniformes e obrigatórios para todos os tribunais sobre quais dados processuais devem ser disponibilizados publicamente sem credenciamento, quais devem exigir cadastro prévio e quais devem ser acessíveis apenas às partes e seus representantes legais. Essa resolução deve ser elaborada em diálogo com a ANPD, com o Conselho Federal da OAB e com os órgãos competentes em matéria de segurança da informação.

A segunda linha é a criação, pela ANPD, de diretrizes específicas sobre a aplicação da LGPD no ambiente processual, preenchendo a lacuna que a tensão entre publicidade e privacidade tem deixado sem resposta normativa. Embora o Poder Judiciário goze de autonomia constitucional, a ANPD tem competência para orientar o tratamento de dados pessoais por entidades públicas em geral, e essa orientação pode induzir práticas mais protetivas sem violar a separação de poderes.

A terceira é a regulamentação legislativa da responsabilidade civil do Estado por danos decorrentes de fraudes que exploram vulnerabilidades nos sistemas de processo eletrônico. Essa regulamentação deve definir critérios objetivos de imputação, prazos de reparação e mecanismos de indenização simplificados que dispensem a vítima de demonstrar a culpa específica do órgão judicial, tornando efetiva a proteção prevista nos arts. 37, § 6.º, da Constituição e 43 da LGPD.

A quarta, de natureza educacional e institucional, é a incorporação, pelos programas de capacitação dos tribunais e pela OAB, de protocolos padronizados de orientação ao jurisdicionado sobre as formas seguras de comunicação com seu advogado, bem como a exigência de que os profissionais incluam, nos contratos de prestação de serviços advocatícios, cláusulas informativas sobre os riscos do golpe e os canais verificados de contato. Essas medidas, de baixo custo e imediata implementação, têm potencial preventivo considerável, pois atacam o elo mais frágil da cadeia: a credulidade da vítima diante de informações que lhe parecem verdadeiras porque efetivamente o são.

7 CONCLUSÕES

O golpe do "falso advogado" é, em sua essência, um sintoma jurídico de um problema estrutural: a digitalização do sistema de Justiça brasileiro avançou com rapidez suficiente para criar novos vetores de vulnerabilidade, mas sem a construção simultânea das salvaguardas normativas e tecnológicas necessárias para proteger os dados pessoais das partes contra usos ilegítimos. O problema que este artigo se propôs a responder não se esgota na persecução penal dos fraudadores; ele diz respeito às condições que o próprio Estado criou para que a fraude fosse possível.

Do ponto de vista penal, a Lei n.º 14.155/2021 representou avanço ao qualificar o estelionato praticado por meios eletrônicos, com penas que chegam a oito anos de reclusão, e ao prever majorante específica para vítimas idosas. Contudo, a efetividade da tutela penal é limitada quando os mecanismos investigativos são lentos para identificar os autores, quando a

disciplina da cadeia de custódia da prova digital permanece insuficiente para as especificidades do ambiente eletrônico e quando a escala do crime sugere a existência de organizações criminosas cujo desmantelamento exige instrumentos além da persecução individual.

No plano da proteção de dados, a LGPD oferece princípios relevantes, especialmente o da minimização e o da segurança, mas sua aplicação ao ambiente processual ainda não dispõe de regulamentação específica que resolva a tensão com o princípio constitucional da publicidade. Enquanto essa tensão permanecer juridicamente indefinida, cada tribunal decidirá autonomamente o que proteger, com resultados desiguais para os jurisdicionados de diferentes regiões do país.

Quanto à responsabilidade institucional, as lacunas são significativas: os critérios de responsabilidade civil do Estado por omissão na proteção de dados processuais não estão definidos; a ANPD ainda não produziu diretrizes específicas para o ambiente judicial; e o CNJ, embora tenha iniciado medidas técnicas pontuais como a autenticação em dois fatores no PJe, não editou resolução normativa uniforme que enfrente o conflito publicidade-privacidade.

A conclusão sustentada neste artigo é a de que o enfrentamento eficaz do golpe do falso advogado exige resposta coordenada em três frentes: normativa, com regulamentação clara pelo CNJ e pela ANPD sobre os dados processuais que devem e os que não devem ser publicamente acessíveis sem credenciamento; tecnológica, com a adoção do princípio de *privacy by design* nos sistemas de processo eletrônico, incorporando desde a concepção dos sistemas os mecanismos de minimização e anonimização de dados; e institucional, com a definição de critérios de responsabilidade estatal pelos danos causados por omissão e com a criação de protocolos educativos padronizados para advogados e jurisdicionados. Uma abordagem fragmentada, que responde ao problema após seus danos, continuará sendo insuficiente diante do grau de sofisticação que as fraudes digitais já atingiram no Brasil.

REFERÊNCIAS

BEZERRA, Eudes Vitor; PEREIRA, Leonardo Marques; COSTA, Monique Leray. Golpe do "falso advogado" e o PJe: transparência processual em conflito com a proteção de dados pessoais. *Revista Observatorio de la Economía Latinoamericana*, Curitiba, v. 24, n. 3, p. 01-22, 2026. DOI: 10.55905/oelv24n3-015.

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

Disponível

em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 maio 2026.

BRASIL. Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 8.906, de 4 de julho de 1994. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/11419.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 13.105, de 16 de março de 2015. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 14.155, de 27 de maio de 2021. Torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou informática. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm. Acesso em: 10 maio 2026.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 10 maio 2026.

CORREIO BRAZILIENSE. Golpe do falso advogado usa dados de processos para enganar vítimas. Brasília, DF: Correio Braziliense, 27 maio 2025a. Disponível em:

<https://www.correiobraziliense.com.br/direito-e-justica/2025/05/7158575>. Acesso em: 10 maio 2026.

CORREIO BRAZILIENSE. Suspeitos de aplicar golpe do falso advogado são alvo de operação. Brasília, DF: Correio Braziliense, 17 jul. 2025b. Disponível em: <https://www.correiobraziliense.com.br/cidades-df/2025/07/7190540>. Acesso em: 10 maio 2026.

G1. Fantástico: golpe do falso advogado; quadrilhas usam dados reais da Justiça para roubar vítimas. Rio de Janeiro: G1, 26 out. 2025. Disponível em: <https://g1.globo.com/fantastico/noticia/2025/10/26/golpe-do-falso-advogado-quadrilhas-usam-dados-reais-da-justica-para-roubar-vitimas.ghtml>. Acesso em: 10 maio 2026.

GAÚCHAZH. Estelionatários com "cartilha" para ensinar golpe do falso advogado são alvo da polícia em SP. Porto Alegre: GZH, 17 jul. 2025. Disponível em: <https://gauchazh.clicrbs.com.br/seguranca/noticia/2025/07>. Acesso em: 10 maio 2026.

ORDEM DOS ADVOGADOS DO BRASIL (Conselho Federal). OAB lança campanha nacional e plataforma de verificação contra o "golpe do falso advogado". Brasília, DF: OAB, 29 abr. 2025. Disponível em: <https://www.oab.org.br/noticia/63063>. Acesso em: 10 maio 2026.

ORDEM DOS ADVOGADOS DO BRASIL – SEÇÃO SÃO PAULO. Cartilha: Golpe do Falso Advogado. São Paulo: OAB-SP, 2024. Disponível em: <https://www.oabsp.org.br/upload/1164693296.pdf>. Acesso em: 10 maio 2026.

ORDEM DOS ADVOGADOS DO BRASIL – SEÇÃO SÃO PAULO. Força-tarefa contra o golpe do falso advogado cria novo mecanismo de prevenção de crimes. São Paulo: OAB-SP, 25 jul. 2025b. Disponível em: <https://www.oabsp.org.br/jornaldaadvocacia/25-07-25-1632-forca-tarefa-contra-o-golpe-do-falso-advogado>. Acesso em: 10 maio 2026.

PESSOA, Wendelson Pereira et al. A vulnerabilidade dos dados nos processos judiciais eletrônicos: análise dos golpes digitais e da responsabilidade do Estado na proteção das informações processuais. Revista Aracê, São José dos Pinhais, v. 8, n. 3, p. 1-15, 2026. DOI: 10.56238/arev8n3-134.

RODRIGUES, Fabriny Souza; MARTINS, Juliana Jorge; AMORIM, Ieda Cristina Dias. Golpe do falso advogado: estelionato digital, publicidade processual e proteção de dados no sistema de justiça brasileiro. Revista JRG de Estudos Acadêmicos, ano 8, v. XIX, n. 19, p. 01-12, jul.-dez. 2025. DOI: 10.55892/jrg.v8i19.2796.

TRIBUNAL REGIONAL FEDERAL DA 1.^a REGIÃO. TRF1 alerta sobre golpe do falso advogado: entenda como funciona a fraude que usa dados reais para enganar vítimas. Brasília, DF: TRF1, 25 jul. 2025a. Disponível em: <https://www.trf1.jus.br/sjpi/noticias/trf1-alerta-sobre-golpe-do-falso-advogado>. Acesso em: 10 maio 2026.

TRIBUNAL REGIONAL FEDERAL DA 1.^a REGIÃO. Em combate ao golpe do falso advogado, CNJ inicia autenticação em dois fatores para usuários do PJe. Teresina: SJPI/TRF1, 3 nov. 2025b. Disponível em: <https://www.trf1.jus.br/sjpi/noticias/em-combate-ao-golpe-do-falso-advogado-cnjinicia-autenticacao-em-dois-fatores>. Acesso em: 10 maio 2026.

TRIBUNAL REGIONAL FEDERAL DA 3.^a REGIÃO. Golpe do falso advogado: saiba o que é e como se proteger. São Paulo: TRF3, 2025. Disponível em: <https://www.trf3.jus.br/campanhas/2025/golpe-falso-advogado>. Acesso em: 10 maio 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD). Jornal Oficial da União Europeia, L 119/1, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 10 maio 2026.