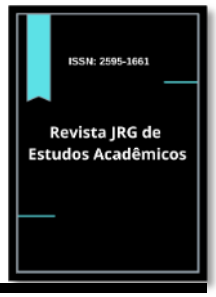
Listas de conteúdos disponíveis em Portal de Periódicos CAPES

ISSN: 2595-1661

ARTIGO

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg



Golpe do falso advogado: estelionato digital, publicidade processual e proteção de dados no sistema de justiça brasileiro

Fake lawyer scam: digital fraud, procedural advertising, and data protection in the brazilian justice system

DOI: 10.55892/jrg.v8i19.2796
ARK: 57118/JRG.v8i19.2796

Recebido: 03/12/2025 | Aceito: 12/12/2025 | Publicado *on-line*: 16/12/2025

Fabriny Souza Rodrigues[1]
https://orcid.org/0009-0007-8515-0276
http://lattes.cnpq.br/6786464685347433
Faculdade dos Carajás, PA, Brasil
E-mail: fabrinyrodriguessenai@gmail.com

Juliana Jorge Martins[2]
https://orcid.org/0009-0002-7802-112X
https://lattes.cnpq.br/3073247401510234
Faculdade dos Carajás, PA, Brasil
E-mail: juju.jorge14@gmail.com

Ieda Cristina Dias Amorim[3]
https://orcid.org/0000-0001-9037-8469
http://lattes.cnpq.br/9430338897750822
Faculdade dos Carajás, PA, Brasil
E-mail: ieda.amorim@carajasedu.com.br

Resumo

Este trabalho analisa o golpe do falso advogado como uma modalidade de estelionato digital que utiliza informações reais extraídas de processos públicos para enganar clientes de advogados. Nessa prática, criminosos passam-se pelo advogado da vítima por meio de aplicativos de mensageria e apresentam dados reais presentes no processo vinculado ao advogado constituído nos autos e noticiam vantagens judiciais de ganho de causa, liberação de pagamentos inexistentes que a parte interessada aguardava poder receber, desse modo, induzindo-a a realização de pagamentos para obter supostos benefícios. O estudo discute dois princípios constitucionais em confronto, a publicidade processual, que garante transparência aos atos e decisões do sistema de justiça, e a proteção de dados pessoais, buscando por finalidade compreender e propor caminhos jurídicos para reduzir tais vulnerabilidades. No decorrer desta pesquisa analisa-se como a ampla divulgação de dados pessoais em ações judiciais tem favorecido a atuação de pessoas mal-intencionadas, chegando à formação de organizações criminosas digitais. A exposição de dados pessoais das partes em processos em andamento serve como material para a personalização do golpe, uma vez que muitos jurisdicionados desconhecem o devido funcionamento do processo judicial. Assim, ao receberem mensagens supostamente enviadas por seu

[1] Graduanda em Direito pela Faculdade dos Carajás.
[2] Graduanda em Direito pela Faculdade dos Carajás.
[3] Mestra em Propriedade Intelectual e Transferência de Tecnologia para Inovação. Unifesspa, Marabá, Pará.

advogado, são levados a confiar e realizar pagamentos fraudulentos, percebendo posteriormente que foram vítimas do golpe do falso advogado. Esse cenário torna a prática do referido golpe especialmente atrativa aos agentes criminosos, dada a facilidade de acesso às informações e o elevado potencial de retorno econômico. A pesquisa, de natureza bibliográfica, documental e normativa, busca apontar medidas institucionais e tecnológicas voltadas ao enfrentamento do problema, como implementação de controles mais rígidos de acesso a dados processuais, iniciativa já observada em tribunais estaduais e federais do país. O estudo demonstra como a configuração atual do processo eletrônico ampliou a circulação de informações sensíveis, contribuindo para a sofisticação dessas fraudes. Portanto, não basta aprimorar mecanismos de controle de acesso, sendo necessário também ponderar quais dados pessoais das partes e patronos devem permanecer públicos, a fim de compatibilizar os princípios constitucionais da publicidade com a proteção de dados, mitigando riscos e fortalecendo a segurança dos jurisdicionados e advogados.

Palavras-chave: Estelionato digital. Golpe do falso advogado. Publicidade processual.

Abstract

This study examines the "false attorney scam" as a type of digital fraud that uses real information extracted from public court records to deceive clients of legal professionals. In this scheme, criminals impersonate the victim's attorney through messaging applications, presenting authentic procedural data linked to the lawyer appointed in the case and promising nonexistent judicial advantages that the party believes are pending. As a result, victims are induced to make payments in order to obtain supposed procedural benefits. The study analyzes the conflict between two constitutional principles: procedural publicity, which ensures transparency in judicial acts and decisions, and the protection of personal data. It aims to identify legal measures that can reduce the vulnerabilities created by this tension. The research shows how the extensive disclosure of personal and procedural information in judicial proceedings has facilitated the activities of malicious actors and contributed to the emergence of organized digital criminal groups. The exposure of sensitive data from ongoing cases allows the scam to be tailored to each victim, particularly because many individuals are unfamiliar with the structure and functioning of the judicial process. When contacted through messages that appear to be from their lawyer, victims often trust the information and make fraudulent payments, only later realizing they have fallen prey to the false attorney scam. This scenario makes the scheme especially attractive to criminal agents, given the ease of accessing judicial information and the high potential for financial gain. Conducted through bibliographical, documentary, and normative analysis, the research seeks to identify institutional and technological measures to address the issue, such as implementing stricter access controls to judicial data, an initiative already adopted by some state and federal courts in Brazil. The study demonstrates that the current configuration of electronic judicial systems has expanded the circulation of sensitive information, increasing the sophistication of such frauds. It concludes that improving access-control mechanisms is not enough; it is also necessary to reassess which personal data of parties and attorneys should remain public, in order to harmonize the constitutional principles of publicity and data protection, mitigate risks, and enhance the security of litigants and legal professionals.

Keywords: *Digital fraud. False attorney scam. Procedural publicity.*

1. Introdução

O ambiente digital tem se tornado, ao mesmo tempo, uma ferramenta essencial e um espaço de novos riscos para a sociedade brasileira. À medida que serviços públicos, comunicações e procedimentos judiciais migram para plataformas eletrônicas, cresce também o número de golpes que exploram essa realidade. Entre essas práticas, o chamado “golpe do falso advogado” ganhou destaque por utilizar dados pessoais das partes e de seus advogados constituídos nos autos, extraídos de processos públicos em andamento. Criminosos passam-se pelo advogado da vítima por meio de aplicativos de mensagens e a induzem à realização de pagamentos para a obtenção de supostos benefícios concedidos pela justiça. Esse cenário revela a necessidade de compreender como informações pessoais vazadas na internet, associadas a dados processuais públicos, podem ser manipuladas por terceiros e empregadas na aplicação de estelionato digital, afetando diretamente a confiança dos cidadãos no sistema de justiça. O chamado golpe do falso advogado, enquadra-se na tipificação penal do estelionato digital, previsto no art. 171 do Código Penal, especialmente após a inclusão do §2º-A pela Lei nº 14.155/2021, que estabeleceu majorantes específicas para crimes cometidos por meio eletrônico, de acordo com Rogério Greco, o legislador buscou conferir maior reprovação ao estelionato praticado mediante fraude eletrônica, diante da maior vulnerabilidade das vítimas no ambiente virtual (GRECO, 2022, p. 412) portanto, reconhecendo a crescente sofisticação das fraudes digitais e a vulnerabilidade dos usuários diante de mecanismos de engenharia social. A manipulação de informações judiciais públicas, combinada com dados pessoais vazados e facilmente obtidos na internet, permite que criminosos simulem a identidade de advogados constituídos para induzir vítimas ao erro, obtenção vantagem econômica ilícita, configurando claramente o tipo penal de estelionato cometido mediante fraude eletrônica.

A inclusão do §2º - A no art. 171 do Código Penal pela Lei nº 14.155/2021 surge como resposta ao aumento expressivo dos crimes de fraude eletrônica no Brasil. Levantamentos recentes sobre segurança digital apontam um crescimento contínuo de golpes praticados por meios eletrônicos, sobretudo aqueles que se valem de dados obtidos em bases públicas e privadas, em 2024, registraram-se 281,2 mil ocorrências de estelionato eletrônico, montante que superou em 17% o total de 2023, segundo análise jornalística ancorada no Anuário Brasileiro de Segurança Pública. Em estudo voltado à publicidade processual e à proteção de dados, Cardoso (2021) destaca que a ampla disponibilização de informações judiciais, embora vinculada ao princípio constitucional da publicidade, cria zonas de risco quando não acompanhada de salvaguardas tecnológicas adequadas, possibilitando o uso indevido dessas informações por terceiros mal-intencionados. Essa constatação dialoga diretamente com o avanço dos casos de estelionato digital, evidenciando que essa prática criminosa se sustenta na combinação entre exposição excessiva de dados e fragilidade dos mecanismos institucionais de proteção.

Diante desse cenário, torna-se essencial entender a importância do princípio da publicidade processual, uma vez que a compreensão de sua função e de seus limites é determinante para compreender por que determinadas informações passam a ser exploradas em práticas criminosas. A ideia de publicidade está ligada ao ato de tornar algo acessível ao conhecimento coletivo, segundo o entendimento de Norberto Bobbio; a publicação dos atos

"[...] representa o verdadeiro momento de reviravolta na transformação do estado moderno, que passa do estado absoluto a estado de direito" (BOBBIO, 1997, p. 103).

Essa concepção evidencia que a publicidade dos atos do poder público surge como instrumento de controle social e de limitação estatal, fundamento que se mantem atual, mesmo no contexto digital.

O referido princípio constitui um dos pilares estruturantes do processo democrático, assegurando transparência, controle social e legitimidade à atuação jurisdicional. De acordo com Cardoso, a publicidade decorre da própria ideia de tornar os atos do Estado "acessíveis ao público", garantindo que qualquer pessoa possa fiscalizar a atuação do Poder Judiciário e compreender como se formam as decisões (CARDOSO, 2020, p. 2–3).

No plano constitucional, tal princípio encontra fundamento no art. 5º, LX, que estabelece que todos os julgamentos serão públicos e fundamentadas todas as decisões, admitindo-se sigilo apenas quando a defesa da intimidade ou o interesse social o exigirem. O Código de Processo Civil, em consonância, reafirma essa diretriz no art. 11 e no art. 189, que tratam tanto da publicidade como regra quanto das hipóteses de exceção.

A publicidade processual possui dupla função: viabilizar o controle social dos atos judiciais e garantir às partes o pleno conhecimento do procedimento. Como observa Dinamarco, a transparência impede que a atuação jurisdicional se torne oculta ou imune ao julgamento dos cidadãos, assegurando o caráter republicano da jurisdição (DINAMARCO apud CARDOSO, 2020, p. 3–4). Todavia, a própria Constituição estabelece que a publicidade não é absoluta. Há processos que tramitam sob sigilo, como ações de família, adoção, violência sexual ou casos que envolvem dados sensíveis de quebra de sigilo de aparelhos e situações em que o sigilo é parcial, restringindo-se a divulgação de documentos ou trechos específicos que possam comprometer a privacidade das partes.

Cardoso ressalta que o sigilo, quando presente, não suprime o direito de acesso das partes aos autos, mas apenas limita a publicidade externa, impedindo que terceiros tenham acesso irrestrito às informações (CARDOSO, 2020, p. 4–5). Assim, "não existe processo sigiloso para as partes"; o sigilo opera exclusivamente contra terceiros, como mecanismo de proteção da privacidade e de prevenção a danos decorrentes da divulgação indevida de informações pessoais ou sensíveis. Essas exceções demonstram que o ordenamento não concebe a publicidade como valor absoluto, mas como um princípio que deve ser ponderado com outros direitos fundamentais, especialmente a intimidade e a proteção de dados pessoais.

A necessidade de limitar a publicidade processual em determinadas situações se torna ainda mais evidente diante da evolução do marco constitucional e legal de proteção de dados no Brasil. Com a promulgação da Emenda Constitucional nº 115/2022, a proteção de dados passou a integrar expressamente o rol dos direitos e garantias fundamentais, reforçando o dever do Estado de assegurar o tratamento adequado das informações pessoais sob sua guarda. Conforme apontam Silva e Araújo, a inclusão desse direito no art. 5º da Constituição consolida a proteção de dados como garantia essencial à dignidade humana, impondo aos órgãos públicos o dever de adotar medidas efetivas de segurança, prevenção e governança no tratamento de informações sensíveis (SILVA; ARAÚJO, 2022, p. 4–6).

Além disso, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece princípios e obrigações que vinculam diretamente o Poder Judiciário, que passa a ser responsável tanto pela transparência quanto pela proteção e mitigação de riscos no

tratamento de dados pessoais. Essa obrigação institucional foi reforçada pelo Conselho Nacional de Justiça por meio da Resolução CNJ nº 363/2021, que determinou aos tribunais a implementação de políticas internas de privacidade, controles de acesso e mecanismos de segurança compatíveis com a LGPD. Assim, a proteção de dados se consolida como um contrapeso necessário ao princípio da publicidade, demonstrando que a exposição indiscriminada de informações judiciais pode gerar vulnerabilidades incompatíveis com o dever constitucional de resguardar segurança informacional dos jurisdicionados.

Nesse contexto, diversas iniciativas institucionais têm buscado mitigar os riscos decorrentes da exposição de dados processuais no ambiente digital. Tribunais estaduais e federais passaram a adotar controles mais rígidos de acesso, como autenticação em dois fatores e restrição de visualização de documentos sensíveis, medidas alinhadas às diretrizes da Resolução CNJ nº 363/2021 e às orientações da ANPD sobre prevenção de incidentes de segurança. Órgãos como o TRF1, o CNJ e seccionais da OAB também têm desenvolvido campanhas educativas e sistemas de verificação da identidade profissional de advogados, visando reduzir a vulnerabilidade dos jurisdicionados diante de golpes baseados em engenharia social. Essas ações evidenciam um movimento institucional de fortalecimento da segurança informacional, cujo aprofundamento será examinado ao longo deste trabalho.

Diante desse panorama, nota-se uma tensão relevante entre os dois princípios constitucionais que, embora essenciais ao sistema de justiça, podem produzir efeitos distintos no ambiente digital. Considerando a importância dessa temática para o funcionamento da justiça e para a proteção da sociedade, torna-se necessário debater e avaliar caminhos jurídicos e institucionais capazes de reduzir vulnerabilidades sem comprometer a transparência jurisdicional. Além do aprimoramento dos mecanismos de controle de acesso, impõe-se refletir sobre quais dados pessoais devem permanecer públicos, de modo a compatibilizar a publicidade processual com a proteção de dados e preservar a segurança dos jurisdicionados e advogados.

2. Metodologia

A pesquisa desenvolvida neste trabalho baseia-se em levantamento bibliográfico, documental e normativo. Na qual foram consultados livros, artigos científicos, legislações, decisões judiciais e atos institucionais relacionados à publicidade processual, proteção de dados e crimes digitais. O estudo dialoga com autores que analisam os impactos do processo eletrônico na exposição de dados pessoais e processuais de partes de processos judiciais, fundamentado os novos riscos decorrentes dessa nova configuração tecnológica do judiciário. Também foram examinadas medidas e orientações emitidas por órgãos como o Conselho Nacional de Justiça, a Autoridade Nacional de Proteção de Dados e a Ordem dos Advogados do Brasil, além de normas do sistema de justiça e dispositivos da legislação penal que tratam do estelionato digital, evidenciando a preocupação institucional sobre o tema.

O estudo utiliza método dedutivo, partindo da análise de normas constitucionais, legais e regulamentares, como a Lei Geral de Proteção de Dados, a Emenda Constitucional nº 115/2022 e a Lei nº 14.155/2021, para compreender a aplicação desses dispositivos ao problema pesquisado. Também foram analisadas decisões judiciais e documentos oficiais que descrevem o funcionamento do golpe e as medidas adotadas pelas instituições para reduzir riscos e proteger os usuários.

O recorte temporal adotado abrange materiais produzidos entre 2018 e 2025, período marcado pela vigência da LGPD, pelo reconhecimento constitucional da proteção de dados pessoais e pela atualização do tipo penal de estelionato eletrônico.

Os documentos selecionados foram organizados por temas e confrontados entre si, permitindo identificar convergências, riscos e possíveis medidas de prevenção no sistema de justiça. A coleta ocorreu por meio de buscas em portais oficiais, seguida da conferência da integridade das fontes.

3. Resultados e Discussão

Os resultados obtidos mostram que o golpe do falso advogado se consolidou como uma modalidade específica de estelionato digital potencializada pelo acesso indiscriminado a dados processuais públicos. A pesquisa evidenciou que informações reais extraídas dos autos, como nomes das partes, números de processos, valores, prazos e movimentações, conferem credibilidade às abordagens criminosas e tornam a fraude mais persuasiva, dificultando a identificação imediata pelas vítimas.

Verificou-se que fragilidades relacionadas à proteção de dados no âmbito do Judiciário, somadas à tardia implementação de medidas de segurança, favoreceram a sofisticação do golpe e ampliaram o número de vítimas em especial as partes processuais e os advogados vinculados ao feito. A associação entre dados vazados e informações processuais públicas forneceu aos criminosos, material suficiente para personalizar contatos fraudulentos. Nesse cenário, torna-se necessário repensar a aplicação da publicidade processual, pois, embora seja fundamental para a transparência e o controle social, a exposição indiscriminada de dados pessoais em processos eletrônicos aumentou significativamente as oportunidades de exploração criminosa.

Verificou-se que fragilidades relacionadas à proteção de dados no âmbito do Judiciário e a tardia implementação de medidas, propiciaram a sofisticação e aumento no número de golpes e vítimas, sendo as partes interessadas em determinado auto processual e os advogados vinculados ao mesmo. O golpe do falso advogado, ganhou material validado com associações de dados vazados e processos judiciais públicos, e com base nisso, vê-se que é necessário repensar a aplicação do princípio da publicidade processual, vale destacar que ela é indispensável para assegurar transparência e controle social, a exposição indiscriminada de dados pessoais em processos eletrônicos ampliou significativamente as oportunidades de exploração criminosa. Os documentos analisados demonstraram que a disponibilização irrestrita de informações sensíveis, somada à facilidade de acesso aos portais judiciais, contribuiu para a personalização de contatos fraudulentos observados nas ocorrências recentes.

Os resultados também indicam que instituições como o Conselho Nacional de Justiça, a Autoridade Nacional de Proteção de Dados, a Ordem dos Advogados do Brasil e tribunais federais têm adotado medidas preventivas, como autenticação em dois fatores, políticas de governança de dados e campanhas de verificação de identidade profissional. Apesar desses avanços, constatou-se que a principal vulnerabilidade permanece sendo estrutural: a ampla exposição de dados das partes em processos públicos. Relatórios, decisões judiciais e reportagens recentes demonstram o crescimento expressivo das fraudes eletrônicas e o surgimento de organizações criminosas especializadas em explorar essas brechas informacionais.

Por fim, os resultados indicam que o conflito entre os princípios da publicidade processual e da proteção de dados exige reavaliação criteriosa pelos órgãos superiores do Judiciário. A literatura e os documentos institucionais convergem no sentido de que é necessário mitigar a publicidade de dados sensíveis, especialmente aqueles que possam ser utilizados para simular comunicações oficiais. Assim, o estudo confirma que a prevenção efetiva do estelionato digital depende da

harmonização entre transparência judicial e segurança informacional, o que requer revisão das práticas de divulgação, implementação de controles de acesso mais rígidos e fortalecimento das barreiras institucionais de proteção de dados, garantindo a preservação dos direitos fundamentais dos jurisdicionados.

4. Considerações Finais

Em síntese, os resultados mostram que o golpe do falso advogado se firmou como uma forma específica de estelionato digital, fortalecida principalmente pela grande exposição de dados pessoais e processuais nos sistemas eletrônicos da Justiça. A migração para o processo digital modernizou o Judiciário, mas não veio acompanhada de medidas suficientes para impedir que essas informações fossem usadas por golpistas, o que facilitou a criação de contatos fraudulentos extremamente convincentes.

À luz dessa constatação, torna-se evidente que a solução para o problema exige uma revisão criteriosa da forma como a publicidade processual vem sendo aplicada no ambiente digital. A transparência judicial permanece essencial para a legitimidade democrática, mas sua execução deve observar os limites impostos pela proteção de dados pessoais, agora reconhecida como direito fundamental. Ajustes como anonimização, limitação de acesso a determinados dados e ocultação de informações sensíveis surgem como caminhos adequados para reduzir riscos sem eliminar a transparência.

Além disso, instituições como o CNJ, a ANPD, os tribunais e a própria OAB desempenham papel essencial nessa revisão. A advocacia organizada, por exemplo, já tem contribuído com ferramentas de verificação de identidade profissional e campanhas educativas, o que ajuda a população a identificar comunicações legítimas. A atuação integrada dessas instituições é indispensável para diminuir o espaço de atuação dos golpistas.

Também iniciativas como a proposta apresentada pela OAB de Marabá para a criação de delegacias especializadas em crimes virtuais devem ser seguidas por outros municípios. A concentração das ocorrências e o trabalho de equipes preparadas para lidar com fraudes digitais podem fortalecer a capacidade de investigação do Estado e melhorar o combate não apenas ao golpe do falso advogado, mas a outros crimes que se apoiam nas brechas do mundo digital, como anonimato.

Por fim, a solução desse problema exige um esforço coordenado e contínuo, que una medidas normativas, tecnológicas, educativas e institucionais. A harmonização entre publicidade processual e proteção de dados precisa ser acompanhada de perto pelos tribunais superiores, responsáveis por definir os limites e a correta ponderação entre esses princípios. Somente com esse alinhamento será possível reduzir a vulnerabilidade digital dos cidadãos e construir um ambiente processual mais seguro e confiável.

Dessa forma, o enfrentamento desse crime exige uma atuação coordenada, contínua e institucionalizada, capaz de equilibrar o acesso à informação com a preservação da segurança, da dignidade e da privacidade das partes envolvidas em processos judiciais. Somente com a conjugação de esforços normativos, tecnológicos, investigativos e educacionais será possível reduzir a incidência de fraudes digitais e construir um ambiente processual mais seguro para os cidadãos brasileiros.

Referências

AGÊNCIA LUPA. Golpes nas redes: Brasil registrou 281 mil casos de estelionato digital em 2024. Rio de Janeiro: Lupa, 24 jul. 2025. Disponível em: https://lupa.uol.com.br/jornalismo/2025/07/24/golpes-nas-redes-brasil-registrou-281-mil-casos-de-estelionato-digital-em-2024. Acesso em: 18 nov. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Balanço de 4 anos da ANPD. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view. Acesso em: 18 nov. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Relatório do ciclo de monitoramento – 2023. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf. Acesso em: 18 nov. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (Brasil). Resolução CD/ANPD nº 15, de 24 de abril de 2024: aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-o-regulamento-de-comunicacao-de-incidente-de-seguranca. Acesso em: 18 nov. 2025.

BANCO CENTRAL DO BRASIL. Manual de Segurança do Pix. Brasília, DF: BCB, 2024. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual_de_Seguranca_PIX.pdf. Acesso em: 18 nov. 2025.

BOBBIO, Noberto. O futuro da democracia.6.ed. Rio de Janeiro: Paz e Terra, 1997.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 18 nov. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 nov. 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), quanto ao estelionato cometido por meios eletrônicos. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 18 nov. 2025.

BRASIL. Constituição (1988). Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 18 nov. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, RJ, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 18 nov. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 nov. 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), quanto ao estelionato cometido por meios eletrônicos. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 18 nov. 2025.

CNN BRASIL. Manual do crime: grupo criou cartilha para aplicar golpe do falso advogado. São Paulo: CNN Brasil, 15 jul. 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/sp/manual-do-crime-grupo-criou-cartilha-para-aplicar-golpe-do-falso-advogado/. Acesso em: 18 nov. 2025.

CNN BRASIL. Vazamento expõe bilhões de senhas do Google, Apple e Meta, diz site. São Paulo: CNN Brasil, 20 jun. 2025. Disponível em: https://www.cnnbrasil.com.br/tecnologia/vazamento-expoe-bilhoes-de-senhas-do-google-apple-e-meta-diz-site/. Acesso em: 18 nov. 2025.

CONSELHO DA JUSTIÇA FEDERAL (Brasil). Segurança da informação no CJF e Justiça Federal. Brasília, DF: CJF, 2024. Disponível em: https://www.cjf.jus.br/cjf/unidades/tecnologia-da-informacao/politica-de-seguranca-da-informacao. Acesso em: 18 nov. 2025.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). Resolução nº 363, de 12 de janeiro de 2021. Estabelece medidas para adequação dos tribunais à LGPD. Brasília, DF: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/files/original181204202101196007 20f42c02e.pdf. Acesso em: 18 nov. 2025.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). Resolução nº 435, de 28 de outubro de 2021. Dispõe sobre a política e o sistema nacional de segurança do Poder Judiciário. Brasília, DF: CNJ, 2021. Disponível em:

https://atos.cnj.jus.br/files/original152110202111036182a8e64e88e.pdf. Acesso em: 18 nov. 2025.

CORREIO BRAZILIENSE. Golpe do falso advogado usa dados de processos para enganar vítimas. Brasília, DF: Correio Braziliense, 27 maio 2025. Disponível em: https://www.correiobraziliense.com.br/direito-e-justica/2025/05/7158575-golpe-do-falso-advogado-usa-dados-de-processos-para-enganar-vitimas.html. Acesso em: 18 nov. 2025.

CORREIO BRAZILIENSE. Suspeitos de aplicar golpe do falso advogado são alvo de operação. Brasília, DF: Correio Braziliense, 17 jul. 2025. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2025/07/7190540-suspeitos-de-aplicar-golpe-do-falso-advogado-sao-alvo-de-operacao.html. Acesso em: 18 nov. 2025.

EUROPOL. Internet Organised Crime Threat Assessment (IOCTA) 2023. The Hague: Europol, 2023. Disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf. Acesso em: 18 nov. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública. Ano 18: 2024. São Paulo: FBSP, 2024. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2024/07/anuario-2024.pdf. Acesso em: 18 nov. 2025.

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: 18 nov. 2025.

G1. Vazamento de dados expõe 1,6 bilhão de senhas de Apple, Google e Facebook. Rio de Janeiro: G1, 20 jun. 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/06/20/vazamento-de-dados-expoe-16-bilhoes-de-senhas-da-apple-google-e-facebook.ghtml. Acesso em: 18 nov. 2025.
GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2017.

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/estelionatarios-com-cartilha-para-ensinar-golpe-do-falso-advogado-sao-alvo-da-policia-em-sp cmd4d8pmt004b014m6u5gpau0.html. Acesso em: 23 nov. 2025.

INTERPOL. Annual Report 2023. Lyon: INTERPOL, 2024. Disponível em: https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf. Acesso em: 18 nov. 2025. NIC.br; CETIC.br. TIC Domicílios 2023: pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros. São Paulo: NIC.br, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20241104102822/tic_domicilios_2023_livro

_eletronico.pdf. Acesso em: 18 nov. 2025. NIC.br. Relatório de atividades 2023 do NIC.br/CERT.br. São Paulo: NIC.br, 2024. Disponível em: https://www.nic.br/media/docs/publicacoes/9/20250213171737/relatorio-de-atividades-2023.pdf. Acesso em: 18 nov. 2025.

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/oab-lanca-campanha-nacional-e-plataforma-de-verificacao-contra-golpe-do-falso-advogado. Acesso em: 18 nov. 2025.

ORDEM DOS ADVOGADOS DO BRASIL – SEÇÃO CEARÁ. Cartilha: Golpe do Falso Advogado. Fortaleza: OAB-CE, 2025. Disponível em: https://oabce.org.br/wp-content/uploads/2025/07/CARTILHA-FALSO-ADVOGADO-compressed.pdf. Acesso em: 18 nov. 2025.

ORDEM DOS ADVOGADOS DO BRASIL – SEÇÃO RIO DE JANEIRO. Cartilha de combate ao golpe do falso advogado. Rio de Janeiro: OAB-RJ, 2025. Disponível em: https://www.oabrj.org.br/sites/default/files/cartilha_de_combate_ao_golpe_do_falso_advogado.pdf. Acesso em: 18 nov. 2025.

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: 18 nov. 2025.

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: Jornal da Advocacia (OAB-SP), 25 jul. 2025. Disponível em: https://www.oabsp.org.br/jornaldaadvocacia/25-07-25-1632-forca-tarefa-contra-o-golpe-do-falso-advogado-da-oab-sp-cria-novo-mecanismo-para-prevencao-de-crimes. Acesso em: 18 nov. 2025.

RÁDIO SENADO (Brasil). Aumentam casos de estelionato digital. Brasília, DF: Senado Federal, 12 ago. 2025. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2025/08/12/aumentam-casos-de-estelionato-digital. Acesso em: 18 nov. 2025.

SAFERNET BRASIL. Central Nacional de Denúncias – Relatório 2024. São Paulo: SaferNet, 2024. Disponível em: https://new.safernet.org.br/sites/default/files/content_files/safernet_central_nacional_de_denuncias_2024.pdf. Acesso em: 18 nov. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (Brasil). Citação por aplicativo de mensagem pode ser válida se der ciência inequívoca da ação judicial. Brasília, DF: STJ, 22 ago. 2023. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/22082023Citacao-por-aplicativo-de-mensagem-pode-ser-valida-se-der-ciencia-inequivoca-da-acao-judicial.aspx. Acesso em: 18 nov. 2025.

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO. Autenticação em dois fatores para acesso ao PJe começou nessa segunda-feira (3). Salvador: SJBA/TRF1, 3 nov. 2025. Disponível em: https://www.trf1.jus.br/sjba/noticias/autenticacao-em-dois-fatores-para-acesso-ao-pje-comecou-nessa-segunda-feira-3. Acesso em: 18 nov. 2025.

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO. Em combate ao golpe do falso advogado, CNJ inicia autenticação em dois fatores para usuários do PJe. Teresina: SJPI/TRF1, 3 nov. 2025. Disponível em: https://www.trf1.jus.br/sjpi/noticias/em-combate-ao-golpe-do-falso-advogado-cnj-inicia-autenticacao-em-dois-fatores-para-usuarios-do-pje-. Acesso em: 18 nov. 2025.

TRIBUNAL REGIONAL FEDERAL DA 1ª 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. 2025. Disponível em: https://www.trf1.jus.br/sjpi/noticias/trf1-alerta-sobre-golpe-do-falso-advogado-entenda-como-funciona-a-fraude-que-usa-dados-reais-para-enganar-vitimas. Acesso em: 18 nov. 2025.

TRIBUNAL REGIONAL FEDERAL DA 3ª 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: 18 nov. 2025.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime: compilation of conclusions and recommendations (UNODC/CCPCJ/EG.4/2021/CRP.1). Vienna: UNODC, 2021. Disponível em: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf. Acesso em: 18 nov. 2025.

VEJA. Violação de dados expõe senhas de Apple, Google e Facebook e outras empresas. São Paulo: Veja, 20 jun. 2025. Disponível em: https://veja.abril.com.br/tecnologia/violacao-de-dados-expoe-senhas-de-apple-google-e-facebook-e-outras-empresas/. Acesso em: 18 nov. 2025.