Revista SICEx

ISSN: 3086-4275 (online)

O GOLPE DO FALSO ADVOGADO EM MATO GROSSO: limites da publicidade processual, proteção de dados e engenharia social

Roger de Jesus Ventura[1]
Anna Carolina Miranda Bellini de Freitas[2]

RESUMO: Este artigo examina o golpe do falso advogado no contexto do Estado de Mato Grosso, com ênfase na tensão entre a publicidade dos atos processuais, a proteção de dados pessoais e o emprego de técnicas de engenharia social. O problema de pesquisa consiste em determinar em que medida a disponibilização digital de informações processuais pode ampliar a capacidade de convencimento dos fraudadores e quais respostas jurídicas e institucionais são compatíveis com a transparência do Poder Judiciário. A investigação utiliza abordagem qualitativa, de caráter exploratório e documental, acrescida de método estatístico descritivo para sistematizar dados secundários sobre ocorrências registradas no Estado. O estudo analisa a Constituição Federal, o Código de Processo Civil, a Lei Geral de Proteção de Dados Pessoais, a legislação penal, atos do Conselho Nacional de Justiça, precedentes do Superior Tribunal de Justiça e materiais institucionais. A contribuição de Daniel Kahneman é empregada para compreender como urgência, coerência narrativa, ancoragem e aversão à perda interferem na tomada de decisão da vítima. Conclui-se que a publicidade processual não deve ser eliminada, mas estruturada de forma proporcional e diferenciada, com minimização de dados, controles de acesso, rastreabilidade, autenticação multifator, protocolos de confirmação e educação digital. A responsabilização de terceiros exige demonstração do dever jurídico violado, do dano e do nexo causal, não sendo legítima a atribuição automática do prejuízo à vítima ou a qualquer instituição.

PALAVRAS-CHAVE: golpe do falso advogado. publicidade processual. proteção de dados. engenharia social. Mato Grosso.

INTRODUÇÃO

A digitalização das relações sociais e dos serviços públicos alterou profundamente a forma como as pessoas se comunicam, realizam pagamentos e acompanham processos judiciais. A mesma infraestrutura que ampliou o acesso à Justiça também favoreceu novas modalidades de fraude, nas quais dados verdadeiros são combinados com identidades falsas, documentos adulterados e pedidos urgentes de pagamento.

Entre essas práticas está o denominado golpe do falso advogado. O fraudador utiliza o nome, a fotografia e o número de inscrição de profissional regularmente inscrito na Ordem dos Advogados do Brasil (OAB), associa tais elementos a informações reais de uma ação judicial e estabelece contato com a parte por aplicativo de mensagens. Em seguida, afirma existir alvará, precatório, indenização ou benefício prestes a ser liberado e condiciona o recebimento ao pagamento imediato de supostas custas, impostos ou honorários, normalmente por Pix ou transferência bancária.

A gravidade do fenômeno não se limita ao prejuízo patrimonial. A fraude atinge a confiança entre advogado e cliente, compromete a credibilidade do Poder Judiciário e explora pessoas que aguardam, muitas vezes por anos, a concretização de um direito. Em Mato Grosso, notícia baseada em dados do Observatório de Segurança Pública

[1] rogerventura2005@gmail.com
[2] 100104655@professor.uniasselvi.com.br

ISSN: 3086-4275 (online)

da Secretaria de Estado de Segurança Pública de Mato Grosso (Sesp-MT) informou 2.933 queixas relacionadas ao golpe entre janeiro e agosto de 2025, equivalentes a 12% dos registros de estelionato no período (Diário de Cuiabá, 2025).

Diante desse cenário, formula-se o seguinte problema de pesquisa: até que ponto a publicidade dos atos processuais facilita o golpe do falso advogado e quais medidas jurídicas e institucionais podem proteger as partes sem comprometer a transparência do Poder Judiciário?

A hipótese é que a publicidade processual, embora indispensável ao controle democrático da jurisdição, pode aumentar o risco de fraude quando dados pessoais, fases processuais e expectativas de recebimento são disponibilizados de modo excessivo, facilmente indexável ou sem controles proporcionais. A resposta adequada não é o sigilo generalizado, mas a construção de uma publicidade responsável, baseada em necessidade, segurança, rastreabilidade e diferenciação dos níveis de acesso.

O objetivo geral é analisar o golpe do falso advogado como fenômeno jurídico e social relacionado à publicidade processual, à proteção de dados e à engenharia social. Especificamente, pretende-se: examinar os limites constitucionais e legais da publicidade; explicar o funcionamento psicológico da fraude; sistematizar dados e iniciativas de Mato Grosso; avaliar a vulnerabilidade das vítimas; identificar medidas preventivas; e delimitar os pressupostos de responsabilização criminal e civil.

A pesquisa adota abordagem qualitativa, de caráter exploratório e documental. O método estatístico descritivo é empregado exclusivamente para organizar dados secundários divulgados por fontes institucionais e jornalísticas, sem pretensão de inferência para além do universo informado. O referencial normativo é composto pela Constituição Federal, pelo Código de Processo Civil, pela Lei Geral de Proteção de Dados Pessoais, pelo Código Penal e por atos do Conselho Nacional de Justiça. Também são examinados precedentes do Superior Tribunal de Justiça, obras doutrinárias e materiais da OAB, do Tribunal de Justiça de Mato Grosso e da Polícia Civil. Não são utilizados relatos pessoais, entrevistas ou dados identificáveis de vítimas.

1 Publicidade processual, acesso à informação e proteção de dados

A publicidade dos atos processuais constitui garantia do Estado Democrático de Direito. Ela viabiliza o controle social da atividade jurisdicional, reduz espaços de arbitrariedade e assegura que decisões públicas possam ser conhecidas e criticadas. Contudo, a Constituição da República não trata a publicidade como valor absoluto. O artigo 5º, inciso LX, admite sua restrição quando a defesa da intimidade ou o interesse social o exigirem; o inciso X protege a intimidade, a vida privada, a honra e a imagem; e o inciso LXXIX reconhece a proteção de dados pessoais como direito fundamental (Brasil, 1988).

O Código de Processo Civil confirma essa arquitetura. Embora o artigo 189 estabeleça a publicidade como regra, o dispositivo prevê segredo de justiça quando houver interesse público ou social, quando a controvérsia envolver determinadas relações familiares ou quando os autos contiverem dados protegidos pelo direito constitucional à intimidade (Brasil, 2015). A existência dessas exceções demonstra que transparência e privacidade devem ser harmonizadas, e não tratadas como princípios mutuamente excludentes.

A Lei Geral de Proteção de Dados Pessoais (LGPD) acrescenta critérios próprios para o tratamento de informações pessoais. Seus princípios de finalidade, adequação, necessidade, segurança, prevenção e responsabilização exigem que a exposição de dados seja compatível com a finalidade pública perseguida. Para os órgãos públicos, o artigo 23 condiciona o tratamento ao atendimento da finalidade pública e do interesse público, enquanto o artigo 46 impõe medidas técnicas e administrativas aptas a prevenir acessos não autorizados e tratamentos ilícitos (Brasil, 2018).

ISSN: 3086-4275 (online)

O exercício regular de direitos em processo judicial é uma base jurídica legítima para o tratamento de dados, mas não converte todo conteúdo dos autos em informação irrestritamente reutilizável. Petições iniciais, contestações e documentos probatórios frequentemente reúnem nome completo, Cadastro de Pessoas Físicas (CPF), endereço, telefone, dados bancários, informações de saúde, vínculos familiares e expectativas econômicas. A publicidade do processo não autoriza que esses elementos sejam coletados em massa ou desviados para finalidade criminosa.

Rodotà (2008) descreve a proteção da privacidade contemporânea como poder de controle sobre a circulação das próprias informações. Doneda (2006), por sua vez, demonstra que a proteção de dados ultrapassa a noção clássica de isolamento e se volta à disciplina do tratamento informacional. Aplicada ao processo eletrônico, essa compreensão impede que o ingresso em juízo seja interpretado como renúncia geral à autodeterminação informativa.

O conflito, portanto, não está entre processo público e processo secreto, mas entre formas distintas de publicidade. Uma consulta individual destinada ao acompanhamento legítimo da jurisdição não produz o mesmo risco que a indexação automatizada, o download em massa ou o cruzamento de dados processuais com redes sociais. A proporcionalidade exige que o desenho dos sistemas considere volume, finalidade, sensibilidade, possibilidade de reidentificação e risco previsível de uso abusivo.

2 Engenharia social, vieses cognitivos e funcionamento do golpe

Engenharia social é o conjunto de estratégias de manipulação empregadas para induzir alguém a revelar informações, executar comandos ou realizar pagamentos. O golpe do falso advogado não depende necessariamente de invasão sofisticada do sistema judicial. Sua eficiência decorre da combinação entre dados autênticos, aparência institucional, autoridade simulada e pressão temporal.

O Tribunal de Justiça do Estado de Mato Grosso (TJMT), na campanha “Justiça Segura – Não Caia no Golpe”, descreveu um padrão recorrente: coleta de informações em sites públicos, criação de perfil falso com nome e fotografia de advogado real, envio de documentos forjados, alegação de prazo curto e solicitação de pagamento por Pix ou transferência. O Tribunal ressalta que não exige depósito antecipado para liberar alvarás, precatórios ou verbas judiciais (Mato Grosso, 2025b).

A contribuição de Kahneman permite compreender por que a abordagem pode convencer pessoas instruídas e familiarizadas com o próprio processo. O autor distingue um modo de pensamento rápido, intuitivo e emocional, denominado Sistema 1, de outro mais lento, deliberativo e analítico, denominado Sistema 2. Situações de urgência, esperança e medo favorecem respostas automáticas e reduzem o tempo disponível para verificação crítica (Kahneman, 2012).

Os dados verdadeiros do processo produzem coerência narrativa e conforto cognitivo: quando o interlocutor conhece o nome do advogado, a natureza da ação e a expectativa de recebimento, a mensagem parece internamente consistente. A indicação de um valor supostamente liberado atua como âncora, enquanto a ameaça de perder a oportunidade caso o pagamento não seja imediato mobiliza a aversão à perda. A fraude, assim, transforma informações fragmentadas em uma história plausível e emocionalmente carregada.

Essa análise não autoriza culpar a vítima. Vieses cognitivos são características ordinárias do julgamento humano, e os criminosos estruturam deliberadamente a comunicação para explorá-los. A resposta preventiva deve reduzir a assimetria informacional, interromper a urgência artificial e criar procedimentos de confirmação simples, acessíveis e conhecidos pela população.

ISSN: 3086-4275 (online)

3 O golpe do falso advogado no contexto de Mato Grosso

Em Mato Grosso, o crescimento das denúncias mobilizou a OAB, a Polícia Civil e o Poder Judiciário. Conforme notícia que reproduziu dados do Observatório de Segurança Pública da Sesp-MT, foram formalizadas 2.933 queixas entre janeiro e agosto de 2025. A modalidade ocupou o terceiro lugar entre os estelionatos no Estado, com participação de 12% no total das ocorrências. A mesma fonte registrou aumento de 13% nos estelionatos virtuais, com elevação da média diária de 90 vítimas em 2024 para 102 em 2025 (Diário de Cuiabá, 2025).

Quadro 1 – Indicadores divulgados sobre o golpe do falso advogado e estelionatos virtuais em Mato Grosso

Indicador	**Dado informado**
Vítimas do golpe do falso advogado em Mato Grosso	2.933
Período analisado	janeiro a agosto de 2025
Posição no ranking de estelionatos	3º lugar
Participação no total de ocorrências	12%
Média diária de vítimas de estelionatos virtuais em 2024	90 vítimas por dia
Média diária de vítimas de estelionatos virtuais em 2025	102 vítimas por dia
Crescimento dos estelionatos virtuais em Mato Grosso	13%

Fonte: elaborado pelo autor com base em Diário de Cuiabá (2025), que reproduz dados do Observatório de Segurança Pública da Sesp-MT.

Os números devem ser interpretados com cautela, pois correspondem às ocorrências formalizadas e divulgadas pela fonte, não necessariamente ao total real de tentativas ou prejuízos. A vergonha, a culpa e a dificuldade de identificar o autor podem favorecer subnotificação.

A Operação Rábula, deflagrada pela Polícia Civil em julho de 2025, evidencia a gravidade concreta de fraudes baseadas em autoridade jurídica simulada. A investigação alcançou grupo que se apresentava como prestador de serviços previdenciários, utilizava trajes sociais e linguagem técnica e obtinha acesso a contas de pessoas idosas. Houve bloqueio aproximado de R$ 300 mil, e a apuração identificou empréstimos entre R$ 18 mil e R$ 24 mil, parcelados em até 96 vezes (Mato Grosso, 2025a). Embora o modo de execução não seja idêntico ao contato digital por dados processuais, o caso revela a força persuasiva da falsa identidade profissional e a especial exposição de pessoas vulneráveis.

A Ordem dos Advogados do Brasil – Seccional Mato Grosso (OAB-MT) informou que as denúncias passaram a ocorrer com maior frequência a partir de agosto de 2020 e criou canal específico para receber relatos, encaminhá-los à Polícia Civil e orientar advogados e jurisdicionados (Ordem dos Advogados do Brasil, 2025). A atuação coordenada é relevante porque a fraude atinge simultaneamente patrimônio, identidade profissional e confiança institucional.

4 Vulnerabilidade da vítima e danos produzidos

A vítima do golpe costuma estar em situação de expectativa jurídica e econômica. Ela pode aguardar benefício previdenciário, indenização, verba trabalhista, precatório ou quantia necessária à manutenção familiar. O fraudador converte essa expectativa em instrumento de pressão: apresenta uma oportunidade aparentemente concreta e afirma que a perda será inevitável caso a exigência financeira não seja cumprida de imediato.

ISSN: 3086-4275 (online)

A vulnerabilidade não se reduz à idade ou ao grau de escolaridade. Ela pode decorrer da baixa familiaridade com sistemas digitais, da confiança depositada no advogado, da linguagem técnica empregada, da urgência artificial, da necessidade financeira, de deficiência, de enfermidade ou da própria assimetria de informações sobre o procedimento judicial. Crianças e adolescentes também podem ser atingidos indiretamente por meio de seus representantes legais.

Pessoas idosas merecem proteção reforçada porque podem enfrentar barreiras tecnológicas e porque o artigo 171, § 4º, do Código Penal prevê aumento de pena quando o estelionato é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso (Brasil, 1940). Essa tutela penal, entretanto, não dispensa medidas preventivas acessíveis, como confirmação por ligação para número previamente conhecido, atendimento presencial e mensagens institucionais em linguagem simples.

Os danos podem ultrapassar a perda financeira. A vítima pode desenvolver ansiedade, vergonha, sentimento de culpa, medo de novos contatos e desconfiança em relação ao advogado verdadeiro e ao próprio Judiciário. A prevenção, por isso, deve ser orientada pela dignidade e evitar discursos que tratem o engano como simples descuido individual.

5 Respostas institucionais e segurança dos sistemas judiciais

O Conselho Federal da OAB lançou, em abril de 2025, a plataforma ConfirmADV, integrada ao Cadastro Nacional dos Advogados, para permitir a verificação da identidade profissional. O usuário informa o número de inscrição, a seccional e o e-mail apresentado pelo suposto advogado; o profissional recebe solicitação de confirmação em endereço previamente cadastrado. Em abril de 2026, a OAB informou que a plataforma havia registrado 32.318 solicitações, das quais 22.685 foram confirmadas e 9.633 não foram validadas ou concluídas (Conselho Federal da Ordem dos Advogados do Brasil, 2026).

A ferramenta acrescenta uma camada de segurança, mas não substitui outros cuidados. A ausência de confirmação deve interromper qualquer pagamento, e a confirmação, isoladamente, não dispensa a checagem do conteúdo da cobrança e da titularidade da conta destinatária. O cidadão deve utilizar canais já conhecidos, e não números ou links fornecidos pelo próprio interlocutor suspeito.

No plano regional, a OAB-MT mantém canal de denúncias e o TJMT divulga orientações para que a população desconfie de mensagens inesperadas, não realize pagamentos antecipados, não clique em links suspeitos e confirme a informação com o advogado constituído ou pelos canais oficiais do Tribunal (Ordem dos Advogados do Brasil, 2025; Mato Grosso, 2025b).

O Conselho Nacional de Justiça (CNJ) estabeleceu, pela Resolução nº 363/2021, medidas de adequação dos tribunais à LGPD, incluindo governança, transparência e proteção contra acessos não autorizados (Conselho Nacional de Justiça, 2021). Posteriormente, a Portaria nº 140/2024 tornou obrigatória a autenticação multifator (MFA) para usuários internos e externos de sistemas judiciais sensíveis, entre eles os sistemas de processo eletrônico (Conselho Nacional de Justiça, 2024). Em novembro de 2025, a autenticação em duas etapas passou a ser exigida para usuários externos do Processo Judicial Eletrônico (PJe), do Jus.br e da Plataforma Digital do Poder Judiciário (Conselho Nacional de Justiça, 2025).

A autenticação multifator reduz o risco de invasão de credenciais, mas não elimina dados obtidos em consultas públicas, diários oficiais, bases antigas ou dispositivos comprometidos. Também não impede que informações legítimas sejam copiadas por usuários autorizados e posteriormente desviadas. Por isso, a segurança deve combinar autenticação, registro de consultas, detecção de acessos anômalos, limitação de extração em massa, revisão periódica de permissões e resposta rápida a incidentes.

ISSN: 3086-4275 (online)

6 Responsabilização penal, civil e proteção jurídica

No âmbito penal, a conduta pode configurar estelionato e, conforme o meio empregado, fraude eletrônica. A Lei nº 14.155/2021 introduziu o § 2º-A no artigo 171 do Código Penal, estabelecendo pena de reclusão de quatro a oito anos e multa para a fraude praticada com informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos, correio eletrônico fraudulento ou meio análogo. Posteriormente, a Lei nº 15.397/2026 manteve a pena e ampliou a redação do dispositivo para mencionar expressamente a duplicação de dispositivo eletrônico e a aplicação de internet. A utilização de perfis falsos, mensagens instantâneas e dados processuais para induzir pagamentos pode, em tese, enquadrar-se nessa estrutura típica, observadas as circunstâncias concretas, a autoria e o dolo.

A responsabilidade civil deve ser examinada por núcleos distintos. O primeiro responsável é o autor da fraude, obrigado a reparar integralmente o prejuízo. A dificuldade prática de identificação e recuperação do numerário, contudo, leva à análise do comportamento de instituições financeiras, plataformas e agentes de tratamento de dados.

Quanto às instituições financeiras, a Súmula 479 do Superior Tribunal de Justiça (STJ) estabelece responsabilidade objetiva pelos danos decorrentes de fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias (Superior Tribunal de Justiça, 2012). Isso não significa responsabilidade automática em todo pagamento voluntariamente realizado. É necessário verificar se houve falha do serviço, transação incompatível com o perfil, deficiência na abertura ou manutenção da conta recebedora, demora injustificada no bloqueio ou ausência de mecanismos de prevenção.

Essa distinção foi reafirmada no AgInt no REsp 2.221.112-SC. A Quarta Turma do STJ considerou que a falha no monitoramento de transações atípicas e na mitigação do dano pode transformar fraude por engenharia social em fortuito interno, especialmente quando a comunicação do golpe é imediata e a instituição não adota providências tempestivas (Superior Tribunal de Justiça, 2026). O precedente oferece fundamento concreto para a responsabilização bancária, mas preserva a análise das circunstâncias de cada caso.

No campo da proteção de dados, os artigos 42 a 44 da LGPD condicionam o dever de reparar à ocorrência de dano causado por tratamento realizado em violação à legislação e admitem excludentes quando não houver tratamento atribuível, violação normativa ou quando o dano decorrer exclusivamente do titular ou de terceiro (Brasil, 2018). No REsp 2.147.374-SP, o STJ destacou a responsabilidade proativa do agente de tratamento e afastou a simples invocação de ataque externo como justificativa suficiente, exigindo demonstração de medidas adequadas de segurança e de concretização dos direitos do titular (Superior Tribunal de Justiça, 2024).

A existência de vazamento, contudo, não gera automaticamente dano moral em qualquer hipótese. No AREsp 2.130.619-SP, o STJ decidiu que a exposição de dados pessoais comuns não produz dano moral presumido, exigindo comprovação do prejuízo concreto; a natureza dos dados e os efeitos do incidente permanecem relevantes para a solução (Superior Tribunal de Justiça, 2023). No golpe do falso advogado, pagamentos efetivamente realizados, empréstimos contratados, uso direcionado de dados ou abalo comprovado podem constituir danos materiais e morais individualizáveis.

Em relação a tribunais e demais órgãos públicos, não é juridicamente rigoroso afirmar que a mera existência de dados processuais usados por criminosos gera responsabilidade estatal. A análise deve partir do artigo 37, § 6º, da Constituição, das regras da LGPD aplicáveis ao Poder Público e das circunstâncias do incidente. É indispensável demonstrar conduta administrativa juridicamente relevante, falha de segurança ou exposição incompatível com a finalidade pública, dano e nexo causal. Quando os dados foram obtidos de fonte legitimamente pública, cruzados com outras bases ou extraídos por terceiro sem falha imputável ao órgão, a responsabilização

ISSN: 3086-4275 (online)

pode não se configurar. Quando houver deficiência comprovada de segurança, tratamento irregular ou omissão diante de risco conhecido, a reparação poderá ser discutida à luz do caso concreto.

7 Publicidade responsável: proposta de compatibilização

O problema investigado não recomenda a substituição da publicidade por sigilo indiscriminado. A solução juridicamente mais consistente é uma publicidade diferenciada, na qual o grau de acesso corresponda à finalidade e ao risco do dado. Metadados essenciais — órgão julgador, classe processual, movimentações e teor de decisões — podem permanecer públicos, enquanto documentos contendo endereços, telefones, dados bancários, documentos de identificação e informações sensíveis devem receber proteção reforçada.

Como proposta, os sistemas processuais podem adotar três níveis de acesso: publicidade aberta para informações indispensáveis ao controle social; acesso autenticado e rastreável para peças com dados pessoais necessários ao exercício profissional ou ao interesse jurídico; e acesso restrito para dados sensíveis ou elementos sem relevância pública imediata. Essa arquitetura não decorre de uma regra única já pronta, mas da aplicação conjunta da proporcionalidade, da minimização de dados e da segurança desde a concepção.

Medidas complementares incluem mascaramento parcial de CPF e endereço, bloqueio de indexação por mecanismos de busca quando juridicamente adequado, limitação de consultas automatizadas, alertas de extração anômala, histórico de acessos, revisão de perfis, autenticação multifator, proteção de arquivos para impedir cópia massiva e canais rápidos para comunicação de incidentes. A tecnologia deve ser acompanhada por protocolos humanos: escritórios podem informar previamente os números oficiais, proibir alteração de dados bancários por mensagem isolada e exigir dupla confirmação para cobranças extraordinárias.

A educação digital completa o modelo. Campanhas devem explicar que dados verdadeiros não provam a identidade do interlocutor, que a urgência é parte do método fraudulento e que pagamentos judiciais devem ser confirmados por canal independente. A informação precisa alcançar pessoas idosas, comunidades com menor acesso digital e representantes de beneficiários vulneráveis, com linguagem simples e alternativas presenciais.

A publicidade responsável preserva a transparência, mas rejeita a ideia de que todo dado acessível possa ser reutilizado sem limite. No ambiente digital, o dever de abertura institucional deve conviver com o dever de reduzir riscos previsíveis, especialmente quando a arquitetura informacional permite coleta em escala e abordagem dirigida de vítimas.

CONCLUSÃO

A pesquisa confirma que o golpe do falso advogado é favorecido pela convergência de quatro elementos: disponibilidade de informações processuais verdadeiras, facilidade de reprodução de identidades, técnicas de engenharia social e meios de pagamento instantâneo. A publicidade processual não é a causa exclusiva da fraude, mas pode ampliar sua verossimilhança quando dados suficientes para individualizar a parte, o advogado e a expectativa econômica são acessíveis sem controles proporcionais.

A resposta ao problema de pesquisa é, portanto, negativa quanto ao sigilo generalizado e afirmativa quanto à necessidade de reestruturação da publicidade no ambiente digital. A Constituição exige transparência, mas também protege intimidade e dados pessoais. A compatibilização deve ocorrer mediante publicidade diferenciada, minimização dos dados expostos, acesso autenticado a documentos com maior risco, rastreabilidade e revisão contínua da arquitetura dos sistemas.

A incorporação de Kahneman demonstra que a prevenção não pode pressupor um usuário permanentemente racional e disponível para longas verificações. O fraudador produz urgência, coerência e medo de perda

ISSN: 3086-4275 (online)

justamente para impedir o pensamento deliberativo. Por isso, os mecanismos de proteção devem tornar a conduta segura mais simples que a conduta arriscada: confirmação por canal independente, bloqueio diante de identidade não validada e resposta bancária imediata após a comunicação.

No plano da responsabilização, a conclusão central é que não existem culpados institucionais automáticos. O criminoso responde pela fraude; bancos podem responder quando a falha do serviço integra o risco da atividade; agentes de tratamento podem responder por tratamento irregular ou segurança insuficiente; e órgãos públicos somente devem ser responsabilizados quando demonstrados dever violado, dano e nexo causal. A vítima, por sua vez, não deve ser convertida em responsável padrão por ter sido alvo de manipulação profissionalmente estruturada.

Como contribuição propositiva, sustenta-se a adoção de um modelo de publicidade processual em camadas. Os elementos indispensáveis ao controle social da atividade jurisdicional devem permanecer acessíveis, enquanto documentos que contenham dados pessoais, informações patrimoniais, endereços, contatos, dados bancários ou elementos relacionados à expectativa de recebimento de valores devem ser submetidos a autenticação, controle de acesso e mecanismos de rastreabilidade. Não se trata de restringir arbitrariamente a transparência, mas de impedir que ela seja desvirtuada e convertida em instrumento de exposição e fraude.

Conclui-se, portanto, que a efetividade da Justiça digital não pode ser medida apenas pela facilidade de acesso ao processo. Um sistema verdadeiramente acessível também deve ser seguro. O cidadão não pode entregar seus dados ao Estado para buscar a tutela de um direito e, no mesmo percurso, tornar-se vítima de uma fraude construída a partir dessas informações. Compatibilizar publicidade, proteção de dados e segurança tecnológica não representa enfraquecimento da transparência, mas condição para que ela permaneça legítima no ambiente digital.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 jul. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 jul. 2026.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 27 jul. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 27 jul. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal para tornar mais graves crimes cometidos de forma eletrônica ou pela internet. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 27 jul. 2026.

BRASIL. Lei nº 15.397, de 30 de abril de 2026. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar penas e tipificar novas condutas. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15397.htm. Acesso em: 27 jul. 2026.

ISSN: 3086-4275 (online)

CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL. Plataforma ConfirmADV completa um ano com mais de 32 mil verificações contra falsos advogados. Brasília, DF: OAB, 29 abr. 2026. Disponível em: https://www.oab.org.br/noticia/64127/plataforma-confirmadv-completa-um-ano-com-mais-de-32-mil-verificacoes-contra-falsos-advogados. Acesso em: 27 jul. 2026.

CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 363, de 12 de janeiro de 2021. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Brasília, DF: CNJ, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 27 jul. 2026.

CONSELHO NACIONAL DE JUSTIÇA. Portaria nº 140, de 22 de abril de 2024. Determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação como requisito funcional para acesso a sistemas judiciais sensíveis. Brasília, DF: CNJ, 2024. Disponível em: https://atos.cnj.jus.br/atos/detalhar/5536. Acesso em: 27 jul. 2026.

CONSELHO NACIONAL DE JUSTIÇA. Em combate ao golpe do falso advogado, CNJ inicia autenticação em dois fatores para usuários do PJe. Brasília, DF: CNJ, 3 nov. 2025. Disponível em: https://www.cnj.jus.br/em-combate-ao-golpe-do-falso-advogado-cnj-inicia-autenticacao-em-dois-fatores-para-usuarios-do-pje/. Acesso em: 27 jul. 2026.

DIÁRIO DE CUIABÁ. Golpe do falso advogado já é 3º lugar no ranking de estelionatos. Cuiabá, 4 out. 2025. Disponível em: https://www.diariodecuiaba.com.br/cidades/golpe-do-falso-advogado-ja-e-3-lugar-no-ranking-de-estelionatos/719616. Acesso em: 27 jul. 2026.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

KAHNEMAN, Daniel. Rápido e devagar: duas formas de pensar. Tradução de Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2012.

MATO GROSSO. Polícia Civil. Polícia Civil cumpre mandados contra falso advogado e comparsas especializados em crimes de furto mediante fraude contra vítimas idosas. Cuiabá: Polícia Civil-MT, 24 jul. 2025a. Disponível em: https://www.secitec.mt.gov.br/web/pjc/w/pol%C3%ADcia-civil-cumpre-mandados-contra-falso-advogado-e-comparsas-especializados-em-crimes-de-furto-mediante-fraude-contra-v%C3%ADtimas-idosas. Acesso em: 12 maio 2026.

MATO GROSSO. Tribunal de Justiça. “Justiça Segura”: saiba como funciona o golpe do falso advogado e reforça alerta à população. Cuiabá: TJMT, 16 jul. 2025b. Disponível em: https://www.tjmt.jus.br/noticias/2025/7/justica-segura-saiba-como-funciona-o-golpe-falso-advogado-e-reforca-alerta-a-populacao. Acesso em: 12 maio 2026.

ORDEM DOS ADVOGADOS DO BRASIL. Seccional Mato Grosso. OAB-MT reforça campanha de orientação e combate a golpes e cria novo canal para receber denúncias. Cuiabá: OAB-MT, 16 abr. 2025. Disponível em: https://www.oabmt.org.br/noticia/22354/oab-mt-reforca-campanha-de-orientacao-e-combate-a-golpes-e-cria-novo-canal-para-receber-denuncias. Acesso em: 27 jul. 2026.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula nº 479. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Segunda Seção, julgado em 27 jun. 2012, DJe 1º ago. 2012. Disponível em: https://processo.stj.jus.br/SCON/sumstj/doc.jsp?sumula=479. Acesso em: 27 jul. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. AREsp 2.130.619-SP. Relator: Ministro Francisco Falcão. Segunda Turma, julgado em 7 mar. 2023, DJe 10 mar. 2023. Vazamento de dados pessoais comuns e necessidade de comprovação do dano moral. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicacao=informativo&livre=%40cnot%3D019794. Acesso em: 27 jul. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 2.147.374-SP. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma, julgado em 3 dez. 2024, DJEN 6 dez. 2024. Responsabilidade proativa do agente de tratamento em incidente de segurança. Disponível em:

ISSN: 3086-4275 (online)

https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicacao=informativo&livre=%40CNOT%3D%27021293%27. Acesso em: 27 jul. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. AgInt no REsp 2.221.112-SC. Relator: Ministro Raul Araújo. Quarta Turma, julgado em 18 maio 2026, DJEN 22 maio 2026. Fraude bancária por engenharia social, monitoramento de transações atípicas e dever de mitigação do dano. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicacao=informativo&livre=%22AgInt%20no%20REsp%202.221.112-SC%22. Acesso em: 27 jul. 2026.