Revista ARACÊ
ISSN: 2358-2472

A VULNERABILIDADE DOS DADOS NOS PROCESSOS JUDICIAIS ELETRÔNICOS: ANÁLISE DOS GOLPES DIGITAIS E DA RESPONSABILIDADE DO ESTADO NA PROTEÇÃO DAS INFORMAÇÕES PROCESSUAIS

THE VULNERABILITY OF DATA IN ELECTRONIC JUDICIAL PROCESSES: AN ANALYSIS OF DIGITAL FRAUD AND THE STATE'S RESPONSIBILITY IN PROTECTING PROCEDURAL INFORMATION

LA VULNERABILIDAD DE LOS DATOS EN LOS PROCESOS JUDICIALES ELECTRÓNICOS: UN ANÁLISIS DEL FRAUDE DIGITAL Y LA RESPONSABILIDAD DEL ESTADO EN LA PROTECCIÓN DE LA INFORMACIÓN PROCESAL

https://doi.org/10.56238/arev8n3-134

Data de submissão: 26/02/2026 **Data de publicação:** 26/03/2026

Wendelson Pereira Pessoa
Pós-doutor em direito
Instituição: Universidade Federal do Maranhão (UFMA)
Lattes: http://lattes.cnpq.br/5521933521924841

Arlen José Silva de Souza
Doutor em Ciências Políticas
Lattes: https://lattes.cnpq.br/4354433259831808

Flávio Henrique de Melo
Doutor em Ciências Juridicas
Lattes: https://lattes.cnpq.br/4820756680473316

Tiago Takashi Tomal
Pós Graduado Esp. em Direito Tributário
Lattes: https://lattes.cnpq.br/9474718933176863

Luiza Helena Galvão
Mestranda em Direito
Lattes: https://lattes.cnpq.br/9072962533044770

Lucas Rocha Andrade
Mestre em Direito
Lattes: https://lattes.cnpq.br/8977851086022955

Lucas Azevedo Santos
Graduando em direito
Lattes: http://lattes.cnpq.br/4175506811330707

Revista ARACÊ
ISSN: 2358-2472

Ozemar Lopes Ferreira
Pós-Graduado em MBA Executivo em Consultoria Empresarial, Pós-Graduado em Direito Penal e Processual Penal
Instituição: Faculdade Unyleya, AVM Faculdade Integrada
Lattes: http://lattes.cnpq.br/8065196802142147

RESUMO
A digitalização do sistema de justiça brasileiro expõe dados processuais a riscos que o ordenamento jurídico vigente ainda não endereça com precisão suficiente. Este estudo analisa a vulnerabilidade dos dados nos processos judiciais eletrônicos, examinando os mecanismos pelos quais golpes digitais exploram informações processuais públicas e os fundamentos da responsabilidade estatal pela proteção dessas informações. A pesquisa adota abordagem qualitativa, de natureza bibliográfica e documental, com levantamento sistemático da literatura publicada entre 2020 e 2026 nas bases Scielo, Google Acadêmico e Portal de Periódicos da CAPES. Os resultados indicam que a vulnerabilidade dos dados processuais decorre de uma combinação de lacunas normativas, defasagem tecnológica e tensão não resolvida entre publicidade processual e privacidade dos dados das partes. O estudo conclui que a efetividade da Lei Geral de Proteção de Dados no ambiente processual depende de mecanismos de enforcement específicos para o setor público e da adoção do princípio de privacy by design nos sistemas de processo eletrônico, sem os quais a responsabilidade estatal pelos danos causados por fraudes digitais permanece juridicamente indefinida.

Palavras-chave: Processo Judicial Eletrônico. Proteção de Dados. Golpes Digitais. Responsabilidade do Estado.

ABSTRACT
The digitalization of the Brazilian justice system exposes procedural data to risks that the current legal framework has not yet addressed with sufficient precision. This study analyzes data vulnerability in electronic judicial proceedings, examining the mechanisms by which digital scams exploit public procedural information and the legal foundations of state responsibility for protecting such information. The research adopts a qualitative approach, of a bibliographic and documentary nature, with a systematic survey of literature published between 2020 and 2026 in the Scielo, Google Scholar, and CAPES Periodicals Portal databases. The results indicate that the vulnerability of procedural data stems from a combination of normative gaps, technological lag, and an unresolved tension between procedural publicity and the privacy of the parties' data. The study concludes that the effectiveness of the General Data Protection Law (Lei Geral de Proteção de Dados — LGPD) in the procedural environment depends on specific enforcement mechanisms for the public sector and on the adoption of the privacy by design principle in electronic process systems, without which state responsibility for damages caused by digital fraud remains legally undefined. The findings reinforce that the protection of procedural data is not a technical problem with a technical solution; it is an institutional design problem that requires coordinated responses from legislators, court administrators, and legal practitioners. Future research should prioritize empirical studies analyzing judicial proceedings involving digital fraud and the regulatory role of the National Data Protection Authority (Autoridade Nacional de Proteção de Dados — ANPD) in relation to the Judiciary.

Keywords: Electronic Judicial Proceedings. Data Protection. Digital Scams. State Responsibility.

RESUMEN
La digitalización del sistema judicial brasileño expone los datos procesales a riesgos que el marco jurídico actual aún no aborda con suficiente precisión. Este estudio analiza la vulnerabilidad de los

Revista ARACÊ
ISSN: 2358-2472

datos en los procesos judiciales electrónicos, examinando los mecanismos mediante los cuales las estafas digitales explotan la información procesal pública y los fundamentos de la responsabilidad del Estado en la protección de dicha información. La investigación adopta un enfoque cualitativo, de carácter bibliográfico y documental, con una revisión sistemática de la literatura publicada entre 2020 y 2026 en las bases de datos SciELO, Google Scholar y CAPES Periodicals Portal. Los resultados indican que la vulnerabilidad de los datos procesales se deriva de una combinación de lagunas normativas, retraso tecnológico y una tensión no resuelta entre la publicidad procesal y la privacidad de los datos de las partes. El estudio concluye que la efectividad de la Ley General de Protección de Datos en el ámbito procesal depende de mecanismos de aplicación específicos para el sector público y de la adopción del principio de privacidad desde el diseño en los sistemas de procesos electrónicos, sin el cual la responsabilidad del Estado por los daños causados por el fraude digital permanece jurídicamente indefinida.

Palabras clave: Proceso Judicial Electrónico. Protección de Datos. Fraude Digital. Responsabilidad del Estado.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

A digitalização do sistema de justiça brasileiro produziu uma transformação que vai além da substituição do papel pelo arquivo eletrônico. O processo judicial eletrônico, consolidado pelo sistema PJe e por plataformas correlatas, reorganizou a arquitetura do acesso à justiça, mas também criou uma superfície de ataque que criminosos digitais exploram com crescente sofisticação. Quando um processo tramita em ambiente digital, cada peça processual, cada decisão, cada dado das partes e de seus representantes legais passa a existir em um espaço que, por definição, é acessível por rede. Essa acessibilidade, que é a virtude do sistema, é também sua vulnerabilidade mais exposta. A pergunta que organiza este estudo não é se os dados processuais podem ser comprometidos, mas quem responde juridicamente quando esse comprometimento ocorre e quais mecanismos o Estado dispõe para preveni-lo.

O contexto regulatório brasileiro oferece um ponto de partida normativo que, por si só, não resolve o problema. A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018 e em vigor desde 2020, estabelece princípios e obrigações para o tratamento de dados pessoais, mas sua aplicação ao ambiente processual enfrenta tensões com o princípio da publicidade dos atos judiciais, previsto no artigo 5.º, inciso LX, da Constituição Federal. Alves (2026, p. 270) observa que o "panorama regulatório sobre proteção de dados" revela assimetrias entre diferentes contextos normativos que afetam diretamente a capacidade de proteção dos titulares, o que se aplica com precisão ao ambiente processual, onde a publicidade e a privacidade coexistem em tensão permanente e sem critérios de resolução plenamente definidos.

A concentração do poder tecnológico nas mãos de poucos atores, sejam eles empresas privadas ou estruturas estatais centralizadas, acrescenta uma dimensão geopolítica ao problema. Beuron e Cristóvam (2025, p. 4) argumentam que a trajetória "do coronelismo eletrônico ao colonialismo digital" representa "perspectivas históricas de concentração hegemônica de poder tecnológico e os riscos à soberania digital", o que interpela diretamente a dependência do Poder Judiciário brasileiro de infraestruturas tecnológicas cujo controle efetivo não reside no Estado. Quando os servidores que hospedam processos judiciais operam sob lógicas de mercado que o Estado não regula com plenitude, a soberania sobre os dados processuais torna-se uma ficção normativa.

Os golpes digitais que exploram informações processuais públicas constituem o fenômeno mais concreto e imediato dessa vulnerabilidade. O chamado "golpe do falso advogado" exemplifica com precisão a cadeia de exploração: o criminoso acessa dados processuais disponíveis publicamente, identifica partes em litígio, simula ser o advogado constituído e solicita transferências financeiras ou informações sensíveis. Esse tipo de fraude não exige invasão de sistemas; ele se alimenta da

Revista ARACÊ
ISSN: 2358-2472

publicidade processual que o próprio ordenamento jurídico garante. A questão que se impõe é se o Estado, ao tornar esses dados acessíveis sem mecanismos de autenticação robustos, assume corresponsabilidade pelos danos que essa acessibilidade produz.

A responsabilidade civil do Estado por falhas na proteção de dados processuais é um campo jurídico ainda em construção no Brasil. A teoria da responsabilidade objetiva do Estado, prevista no artigo 37, § 6.º, da Constituição Federal, estabelece que o poder público responde pelos danos que seus agentes causarem a terceiros, independentemente de culpa. Transposta para o ambiente digital, essa regra levanta uma questão que a jurisprudência ainda não respondeu com uniformidade: a omissão do Estado na adoção de medidas de segurança da informação adequadas configura ato omissivo que gera responsabilidade objetiva ou subjetiva? A resposta a essa pergunta tem consequências práticas para milhares de jurisdicionados que já foram vítimas de fraudes alimentadas por dados processuais.

Este estudo analisa a vulnerabilidade dos dados nos processos judiciais eletrônicos, examinando os mecanismos pelos quais golpes digitais exploram informações processuais e os fundamentos jurídicos da responsabilidade estatal pela proteção dessas informações. O objetivo geral é avaliar em que medida o Estado brasileiro cumpre seu dever de proteção dos dados processuais e quais lacunas normativas e operacionais expõem os jurisdicionados a fraudes digitais. Os objetivos específicos são: (a) caracterizar a arquitetura de vulnerabilidade dos sistemas de processo eletrônico no Brasil; (b) analisar os principais tipos de golpes digitais que exploram dados processuais públicos; (c) examinar os fundamentos da responsabilidade civil do Estado por falhas na proteção de informações processuais; (d) discutir as implicações da LGPD para o ambiente processual e as lacunas regulatórias que persistem.

O trabalho organiza-se em cinco seções. A seção 2 desenvolve o referencial teórico, articulando os conceitos de soberania digital, proteção de dados, publicidade processual e responsabilidade estatal. A seção 3 descreve os procedimentos metodológicos adotados. A seção 4 apresenta e discute os resultados à luz da literatura especializada. A seção 5 expõe as considerações finais, com síntese dos achados, limitações do estudo e perspectivas para investigações futuras.

2 METODOLOGIA

Esta pesquisa adota abordagem qualitativa, de natureza aplicada, com objetivo descritivo e analítico. A escolha pela abordagem qualitativa justifica-se pela natureza do objeto investigado: a vulnerabilidade dos dados nos processos judiciais eletrônicos envolve dimensões normativas, tecnológicas e institucionais que não se reduzem à quantificação estatística, mas exigem interpretação

Revista ARACÊ
ISSN: 2358-2472

contextualizada de fenômenos jurídicos e digitais que operam em múltiplas escalas. A pesquisa classifica-se, quanto aos procedimentos técnicos, como bibliográfica e documental, com levantamento sistemático da literatura científica e jurídica publicada entre 2020 e 2026 nas áreas de direito digital, proteção de dados, segurança da informação e responsabilidade civil do Estado.

A coleta de dados bibliográficos foi realizada nas bases Scielo, Google Acadêmico, Portal de Periódicos da CAPES, Repositório do Conselho Nacional de Justiça (CNJ) e bases de dados jurídicas especializadas, com os descritores: "processo judicial eletrônico", "proteção de dados processuais", "LGPD e processo", "golpe digital", "responsabilidade do Estado", "soberania digital" e suas combinações em português e inglês. Os critérios de inclusão abrangeram artigos originais, estudos de caso, revisões bibliográficas e documentos normativos publicados em periódicos com avaliação Qualis, disponíveis na íntegra e com aderência temática ao objeto de estudo. Gomes, Pinto e Silva (2023) demonstram que o levantamento de processos judiciais em perspectiva panorâmica exige a definição precisa de critérios de inclusão e exclusão para garantir a representatividade e a comparabilidade dos dados entre diferentes contextos institucionais, argumento que orienta a delimitação metodológica adotada neste estudo.

Os dados coletados foram submetidos à análise de conteúdo temática, com organização em quatro eixos analíticos: (a) arquitetura de vulnerabilidade dos sistemas de processo eletrônico; (b) tipologia dos golpes digitais que exploram dados processuais; (c) fundamentos jurídicos da responsabilidade estatal por falhas na proteção de dados; (d) lacunas regulatórias entre a LGPD e o ambiente processual. Essa categorização permitiu o tratamento sistemático do material e a identificação de convergências e divergências entre os estudos analisados. Gontijo (2025) sustenta que a análise jurídico-constitucional da soberania digital no Brasil exige uma abordagem que articule o plano normativo com o plano das práticas institucionais concretas, raciocínio que orienta a organização analítica adotada neste estudo.

A validade interna da pesquisa foi assegurada pela triangulação de fontes, com consulta a estudos de diferentes abordagens metodológicas sobre o mesmo fenômeno, e pela rastreabilidade das decisões analíticas, documentadas ao longo do processo de coleta e categorização. Os aspectos éticos foram observados mediante citação rigorosa das fontes, vedação ao plágio e à deturpação das ideias dos autores referenciados, e transparência quanto às limitações metodológicas do estudo. A principal limitação reside no caráter bibliográfico da pesquisa, que não permite a análise direta dos sistemas de processo eletrônico nem a coleta de dados primários junto aos tribunais ou às vítimas de golpes digitais. Estudos futuros poderão suprir essa lacuna por meio de pesquisa de campo com análise de

Revista ARACÊ
ISSN: 2358-2472

processos judiciais envolvendo fraudes digitais e entrevistas com operadores do direito e especialistas em segurança da informação.

Quadro 1 –Referências Acadêmicas e Suas Contribuições para a Pesquisa

Autor	Título	Ano	Contribuições
Perez, O.; Souza, B.	Do público ao privado: representações sociais de associações acerca da responsabilidade com a questão socioambiental	2022	Discute como associações percebem sua responsabilidade socioambiental, oferecendo base teórica sobre responsabilidade social que pode dialogar com deveres de proteção de dados e de governança digital pelas organizações.
Reis, R.; Saikali, L.; Freitas, C.	POLÍTICAS REGULATÓRIAS PARA A PROTEÇÃO DE DADOS NO BRASIL E A APLICABILIDADE DO MODELO DE REGULAÇÃO PELA ARQUITETURA DE CÓDIGO OU PRIVACY BY DESIGN	2022	Analisa políticas regulatórias de proteção de dados no Brasil e a ideia de "privacy by design", contribuindo para compreender modelos regulatórios que integram tecnologia, arquitetura de código e proteção de dados pessoais.
Gomes, M.; Pinto, P.; Silva, R.	Procedimentos odontológicos e processos judiciais: um panorama do Estado do Rio de Janeiro	2023	Apresenta panorama de processos judiciais envolvendo procedimentos odontológicos, trazendo reflexões sobre responsabilização profissional, registros e, indiretamente, sobre a importância da gestão adequada de dados em saúde.
Silveira, M.; Lima, M.	ANÁLISE DA MOROSIDADE PROCESSUAL NAS COMPRAS PÚBLICAS E SEUS IMPACTOS NA EFICÁCIA DO ATENDIMENTO À SAÚDE PÚBLICA	2023	Analisa a morosidade em compras públicas e seus reflexos na saúde, permitindo dialogar com a necessidade de processos mais eficientes, inclusive digitais, sem comprometer transparência, controle e proteção de dados sensíveis.
Machado, K.; Preta, K.; Pungirum, J.	SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS NO BRASIL	2024	Discute segurança da informação no contexto empresarial brasileiro, abordando riscos, medidas técnicas e organizacionais, e criando base para implementação de políticas de proteção de dados alinhadas à LGPD.
Beuron, B.	Do coronelismo eletrônico ao colonialismo digital	2025	Problematiza a concentração de poder tecnológico e o "colonialismo digital", discutindo riscos à soberania digital e à autonomia regulatória do Estado frente a grandes plataformas e infraestruturas digitais.
Corrêa, G.; Frota, V.	Hipervulnerabilidade do idoso na contratação de empréstimos por meios digitais no Estado do Amazonas	2025	Analisa a hipervulnerabilidade de idosos em contratações digitais, contribuindo para debates sobre proteção de dados, consentimento, fraude e tutela jurídica de grupos vulneráveis em ambientes digitais.
Filho, A.	PROVAS DIGITAIS NO PROCESSO PENAL: NULIDADES E A AUSÊNCIA DE REGULAMENTAÇÃO ESPECÍFICA	2025	Examina provas digitais no processo penal, destacando nulidades e lacunas normativas, o que é central para discutir admissibilidade, cadeia de custódia e confiabilidade de evidências em ambiente digital.
Gontijo, A.	O JOGO DE DADOS ENTRE O ESTADO E AS BIG TECHS: UMA ANÁLISE JURÍDICO-CONSTITUCIONAL DA SOBERANIA DIGITAL NO BRASIL	2025	Aborda a disputa por dados entre Estado e Big Techs, discutindo soberania digital, limites do poder público e impactos na proteção de direitos fundamentais em um cenário de forte assimetria informacional.

Revista ARACÊ
ISSN: 2358-2472

Jabur, A.	COMPARAÇÃO ENTRE A LEI DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD) E A LEGISLAÇÃO DE PROTEÇÃO DE DADOS DOS ESTADOS UNIDOS: ANÁLISE COM ENFOQUE NOS ESTUDOS DE DANILO DONEDA, BRUNO BIONI E PERSPECTIVAS ATUAIS	2025	Compara a LGPD com a legislação norte-americana, destacando diferenças estruturais e influências doutrinárias, útil para compreender modelos de proteção de dados e seus reflexos na prática regulatória e empresarial.
Oliveira, B.	UMA ANÁLISE DA EVOLUÇÃO DOS CASOS DE ESTELIONATO VIRTUAL APÓS A PROMULGAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	2025	Analisa a evolução de casos de estelionato virtual após a LGPD, permitindo avaliar se o marco regulatório impactou a criminalidade digital e quais lacunas permanecem na proteção de dados dos usuários.
Rodrigues, F.	Golpe do falso advogado: estelionato digital, publicidade processual e proteção de dados no sistema de justiça brasileiro	2025	Estuda o "golpe do falso advogado" e relaciona estelionato digital com publicidade processual e proteção de dados, evidenciando vulnerabilidades do sistema de justiça e a necessidade de maior controle sobre informações judiciais.
Alves, L.	Panorama regulatório sobre proteção de dados de crianças e adolescentes: Norte e Sul Global em perspectiva	2026	Traça panorama comparado da proteção de dados de crianças e adolescentes entre Norte e Sul Global, fundamental para debates sobre proteção reforçada, consentimento parental e risco de exploração de dados de menores.
Cossaros, B.	COMPLIANCE NAS CLÍNICAS ODONTOLÓGICAS: NECESSIDADE, CRITÉRIOS E MODELOS DE IMPLEMENTAÇÃO	2026	Discute modelos de compliance em clínicas odontológicas, incluindo governança, responsabilidade e proteção de dados de pacientes, sugerindo critérios práticos de implementação de programas de conformidade.
Perez, O.; Souza, B.	Do público ao privado: representações sociais de associações acerca da responsabilidade com a questão socioambiental	2022	Discute como associações percebem sua responsabilidade socioambiental, oferecendo base teórica sobre responsabilidade social que pode dialogar com deveres de proteção de dados e de governança digital pelas organizações.
Reis, R.; Saikali, L.; Freitas, C.	POLÍTICAS REGULATÓRIAS PARA A PROTEÇÃO DE DADOS NO BRASIL E A APLICABILIDADE DO MODELO DE REGULAÇÃO PELA ARQUITETURA DE CÓDIGO OU PRIVACY BY DESIGN	2022	Analisa políticas regulatórias de proteção de dados no Brasil e a ideia de "privacy by design", contribuindo para compreender modelos regulatórios que integram tecnologia, arquitetura de código e proteção de dados pessoais.

Fonte: Elaboração do próprio autor (2026)

O quadro evidencia, em sequência temporal, como a produção recente vem aprofundando temas centrais do direito digital: proteção de dados, segurança da informação, soberania digital, vulnerabilidade de grupos específicos, provas digitais e compliance. Em conjunto, as obras permitem ao pesquisador construir uma análise robusta e crítica sobre os desafios jurídicos e regulatórios da sociedade de dados, articulando teoria, comparações internacionais, estudos de caso e implicações práticas para o sistema de justiça, empresas e cidadãos.

Revista ARACÊ
ISSN: 2358-2472

3 REFERENCIAL TEÓRICO

A proteção de dados pessoais no ambiente digital não é uma questão técnica com solução técnica; ela é uma questão de poder, de quem controla a informação e de quais consequências esse controle produz sobre os direitos dos indivíduos. No contexto dos processos judiciais eletrônicos, essa dimensão política da proteção de dados se manifesta com particular intensidade, porque o Estado ocupa simultaneamente a posição de guardião dos dados e de potencial responsável por sua exposição indevida. Compreender essa dualidade exige que se parta de um conceito de soberania digital que vá além da retórica institucional e que examine as condições concretas em que o poder público exerce, ou deixa de exercer, controle efetivo sobre as informações que processa.

O conceito de *compliance* digital emerge, nesse contexto, como ferramenta de governança que as instituições públicas ainda incorporam de forma incipiente. Cossaros (2026, p. 3) argumenta que o *compliance* representa "necessidade, critérios e modelos de implementação" que transcendem o setor privado e se aplicam a qualquer organização que trate dados sensíveis, o que inclui, com evidência, os tribunais e os sistemas de processo eletrônico. A ausência de programas estruturados de conformidade digital no Poder Judiciário não é uma omissão neutra; ela configura uma escolha institucional que expõe os jurisdicionados a riscos que poderiam ser mitigados por protocolos já disponíveis na literatura especializada.

A hipervulnerabilidade de determinados grupos no ambiente digital acrescenta uma camada de análise que o debate sobre processo eletrônico frequentemente ignora. Corrêa e Frota (2025, p. 4) demonstram que a "hipervulnerabilidade do idoso na contratação de empréstimos por meios digitais" revela padrões de exploração que se replicam em outros contextos de interação digital assimétrica, incluindo o ambiente processual. Partes em litígio que não dominam os mecanismos de autenticação digital, que não reconhecem tentativas de *phishing* e que confiam em comunicações que simulam ser do sistema de justiça constituem um grupo de vítimas potenciais cujo perfil o Estado precisa considerar ao desenhar a arquitetura de segurança dos seus sistemas.

A questão das provas digitais no processo penal revela uma lacuna normativa que se estende para além do campo probatório. Filho, Castro e Ugalde (2025, p. 58) sustentam que as "provas digitais no processo penal" enfrentam "nulidades e a ausência de regulamentação específica", o que evidencia que o ordenamento jurídico brasileiro ainda não produziu um marco normativo capaz de acompanhar a velocidade com que o ambiente digital transforma as práticas processuais. Essa lacuna não afeta apenas a validade das provas; ela compromete a integridade de todo o ecossistema processual digital, porque um sistema sem regras claras sobre a cadeia de custódia digital é um sistema que não consegue garantir a autenticidade das informações que processa.

Revista ARACÊ
ISSN: 2358-2472

A teoria da responsabilidade civil do Estado por omissão digital encontra na doutrina constitucional contemporânea fundamentos que a jurisprudência ainda não consolidou. O dever de proteção (*Schutzpflicht*), desenvolvido pela dogmática constitucional alemã e incorporado ao pensamento jurídico brasileiro, postula que o Estado não apenas deve abster-se de violar direitos fundamentais, mas tem a obrigação positiva de protegê-los contra ameaças de terceiros. Quando o Estado disponibiliza dados processuais em plataformas digitais sem adotar medidas de segurança proporcionais ao risco que essa disponibilização cria, ele falha no cumprimento desse dever de proteção, o que abre espaço para a responsabilização por danos decorrentes de fraudes que a omissão estatal tornou possíveis. O referencial teórico aqui construído articula, portanto, as dimensões normativa, tecnológica e constitucional da vulnerabilidade dos dados processuais, fornecendo a base conceitual para a análise desenvolvida nas seções seguintes.

4 RESULTADOS E DISCUSSÃO

A análise da literatura selecionada revelou que a vulnerabilidade dos dados nos processos judiciais eletrônicos brasileiros não decorre de uma falha técnica isolada, mas de uma combinação de fatores estruturais que se reforçam mutuamente: a ausência de um marco normativo específico para a proteção de dados processuais, a dependência de infraestruturas tecnológicas com governança fragmentada, e a tensão não resolvida entre publicidade processual e privacidade dos dados das partes. Os estudos examinados convergiram para a identificação de um padrão recorrente: o Estado cria sistemas digitais de acesso à justiça sem projetar, desde a concepção, os mecanismos de segurança proporcionais ao risco que esses sistemas geram.

Rodrigues, Martins e Amorim (2025) analisaram o "golpe do falso advogado" e demonstraram que o estelionato digital, a publicidade processual e a proteção de dados no sistema de justiça brasileiro formam um triângulo de vulnerabilidade em que cada vértice potencializa os outros dois. O criminoso não precisa invadir nenhum sistema; ele utiliza dados que o próprio Estado disponibiliza publicamente para construir uma narrativa fraudulenta convincente. Esse achado questiona a premissa de que a segurança dos dados processuais é um problema de cibersegurança; ela é, antes de tudo, um problema de desenho institucional.

Oliveira (2025) demonstrou que a evolução dos casos de estelionato virtual após a promulgação da LGPD não apresentou a redução esperada pelos defensores da lei, o que indica que a norma, por si só, não produziu o efeito dissuasório sobre as fraudes digitais que seu texto prometia. Esse resultado não invalida a LGPD; ele revela que a efetividade de uma lei de proteção de dados depende de mecanismos de enforcement que o Brasil ainda não consolidou, especialmente no

Revista ARACÊ
ISSN: 2358-2472

ambiente processual, onde a Autoridade Nacional de Proteção de Dados (ANPD) ainda não definiu com clareza sua competência regulatória.

Jabur (2025, p. 7282) identificou, ao comparar a LGPD com a legislação norte-americana de proteção de dados, que o modelo brasileiro apresenta lacunas na definição de responsabilidades para o setor público que a legislação comparada já endereçou com maior precisão. Essa assimetria regulatória tem consequências diretas para o ambiente processual: enquanto o setor privado enfrenta sanções da ANPD por violações da LGPD, o Poder Judiciário opera em uma zona de relativa impunidade regulatória, sem que haja mecanismo claro de responsabilização por falhas na proteção dos dados que processa.

Machado, Preta e Pungirum (2024) demonstraram que a segurança da informação para organizações no Brasil ainda se concentra em soluções reativas, adotadas após a ocorrência de incidentes, em vez de estratégias preventivas baseadas em análise de risco. Esse padrão, documentado no setor privado, reproduz-se com ainda maior intensidade no setor público, onde os ciclos de atualização tecnológica são mais lentos e os investimentos em segurança da informação competem com demandas orçamentárias de outras áreas. O resultado é um sistema de processo eletrônico que opera com defasagem tecnológica em relação às ameaças que enfrenta.

Reis, Saikali e Freitas (2022, p. 365) argumentam que as "políticas regulatórias para a proteção de dados no Brasil" precisam incorporar o modelo de "*privacy by design*", segundo o qual a proteção da privacidade deve ser projetada desde a concepção dos sistemas, e não adicionada como camada posterior. Aplicado ao processo eletrônico, esse princípio exigiria que os sistemas de consulta processual fossem desenhados com mecanismos de autenticação que distinguissem o acesso legítimo do acesso fraudulento, sem comprometer a publicidade dos atos judiciais que a Constituição garante.

Perez e Souza (2022) demonstraram que a transição do público ao privado em contextos de responsabilidade socioambiental revela padrões de transferência de risco que se replicam no ambiente digital: o Estado cria sistemas que geram riscos para os cidadãos e, ao mesmo tempo, resiste a assumir a responsabilidade pelos danos que esses riscos produzem. Silveira e Lima (2023) acrescentam que a morosidade processual nas compras públicas e seus impactos na eficácia do atendimento revelam um padrão institucional de subestimação dos custos da ineficiência, padrão que se reproduz na gestão da segurança dos sistemas de processo eletrônico, onde os custos das falhas são externalizados para as vítimas das fraudes.

Revista ARACÊ
ISSN: 2358-2472

5 CONSIDERAÇÕES FINAIS

Este estudo analisou a vulnerabilidade dos dados nos processos judiciais eletrônicos brasileiros, examinando os mecanismos pelos quais golpes digitais exploram informações processuais públicas e os fundamentos jurídicos da responsabilidade estatal pela proteção dessas informações.

Os resultados obtidos demonstram que a vulnerabilidade dos dados processuais não é um problema técnico com solução técnica; ela é um problema de desenho institucional, de escolhas regulatórias e de uma cultura organizacional que ainda não incorporou a proteção de dados como valor operacional do sistema de justiça.

A análise dos golpes digitais que exploram dados processuais revelou que o criminoso não precisa invadir sistemas para causar dano; ele utiliza informações que o próprio Estado disponibiliza publicamente, o que desloca o debate da cibersegurança para o campo do desenho normativo e da responsabilidade institucional.

A tensão entre publicidade processual e proteção de dados pessoais constitui o nó central do problema e não encontra, na legislação brasileira vigente, uma solução que equilibre os dois princípios com precisão suficiente para orientar a prática dos tribunais.

A hipótese de que a LGPD, por si só, seria capaz de reduzir a incidência de fraudes digitais no ambiente processual não encontra respaldo nos estudos analisados, o que indica que a efetividade da norma depende de mecanismos de *enforcement* que o Brasil ainda não consolidou para o setor público.

A contribuição deste estudo para o campo do direito digital e da responsabilidade civil do Estado reside na articulação sistemática entre as dimensões normativa, tecnológica e constitucional da vulnerabilidade dos dados processuais, perspectiva que a literatura jurídica brasileira ainda aborda de forma fragmentada.

A principal limitação da pesquisa é o seu caráter bibliográfico, que não permite a análise direta dos sistemas de processo eletrônico nem a coleta de dados primários junto aos tribunais ou às vítimas de golpes digitais, o que restringe a capacidade de generalização dos achados para contextos institucionais específicos.

Estudos futuros devem investir em pesquisas de campo com análise de processos judiciais envolvendo fraudes digitais, entrevistas com operadores do direito e especialistas em segurança da informação, e levantamentos sobre a atuação da ANPD em relação ao Poder Judiciário.

A adoção do princípio de *privacy by design* nos sistemas de processo eletrônico representa uma agenda de reforma tecnológica e normativa que este estudo contribui para fundamentar, ao

Revista ARACÊ
ISSN: 2358-2472

demonstrar que a proteção de dados processuais precisa ser projetada desde a concepção dos sistemas, e não adicionada como resposta a incidentes já ocorridos.

A responsabilidade civil do Estado por falhas na proteção de dados processuais precisa ser objeto de regulamentação específica que defina com clareza os critérios de imputação, os mecanismos de reparação e os limites da responsabilidade objetiva em contextos de omissão digital.

A formação dos operadores do direito para o reconhecimento e o manejo de ameaças digitais no ambiente processual constitui uma lacuna formativa que as instituições de ensino jurídico e os programas de capacitação dos tribunais precisam endereçar com maior sistematicidade.

A soberania digital do Estado brasileiro sobre os dados que processa em seus sistemas de justiça é uma condição de legitimidade democrática que este estudo posiciona como problema de pesquisa e de política pública, convocando legisladores, gestores e juristas a uma resposta coordenada.

A relação entre concentração tecnológica, dependência de infraestruturas privadas e vulnerabilidade dos dados processuais constitui uma agenda de pesquisa que transcende o direito e exige diálogo com a ciência da computação, a ciência política e a economia digital.

O impacto deste trabalho reside na sua capacidade de articular evidências dispersas em uma narrativa coerente que posiciona a proteção dos dados processuais como problema de Estado, de direitos fundamentais e de confiança institucional, convocando o Poder Judiciário a assumir sua responsabilidade como guardião não apenas da justiça, mas das informações que a tornam possível.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

ALVES, L. Panorama regulatório sobre proteção de dados de crianças e adolescentes: Norte e Sul Global em perspectiva. Revista Rede de Direito Digital, Intelectual & Sociedade, v. 5, n. 10, p. 265-298, 2026. DOI: 10.5380/rrddis.v5i10.101840.

BEURON, B. M. C. de B.; CRISTÓVAM, J. S. da S. Do coronelismo eletrônico ao colonialismo digital: perspectivas históricas de concentração hegemônica de poder tecnológico e os riscos à soberania digital. Revista do Curso de Direito do UNIFOR, v. 16, n. 3, e252415, 2025. DOI: 10.24862/rcdu.v16i3.2415.

Do coronelismo eletrônico ao colonialismo digital: perspectivas históricas de concentração hegemônica de poder tecnológico e os riscos à soberania digital | Revista do Curso de Direito do UNIFOR

CORRÊA, G.; FROTA, V. Hipervulnerabilidade do idoso na contratação de empréstimos por meios digitais no Estado do Amazonas. Delos – Desarrollo Local Sostenible, v. 18, n. 67, e4957, 2025. DOI: 10.55905/rdelosv18.n67-014.

COSSAROS, B. M. COMPLIANCE NAS CLÍNICAS ODONTOLÓGICAS: NECESSIDADE, CRITÉRIOS E MODELOS DE IMPLEMENTAÇÃO. Aracê, v. 8, n. 2, e12188, 2026. DOI: 10.56238/arev8n2-076.

FILHO, A. N. M.; CASTRO, A. T. S. B.; UGALDE, J. C. R. PROVAS DIGITAIS NO PROCESSO PENAL: NULIDADES E A AUSÊNCIA DE REGULAMENTAÇÃO ESPECÍFICA. Revista FT, v. 29, n. 151, p. 58-59, 2025. DOI: 10.69849/revistaft/ra10202510291258.

PROVAS DIGITAIS NO PROCESSO PENAL: NULIDADES E A AUSÊNCIA DE REGULAMENTAÇÃO ESPECÍFICA – ISSN 1678-0817 Qualis/DOI

GOMES, M. B. C.; PINTO, P. H. V.; SILVA, R. H. A. da. Procedimentos odontológicos e processos judiciais: um panorama do Estado do Rio de Janeiro. Revista de Direito Sanitário, v. 23, e0005, 2023. DOI: 10.11606/issn.2316-9044.rdisan.2023.190448.

Procedimentos odontológicos e processos judiciais: um panorama do Estado do Rio de Janeiro | Revista de Direito Sanitário

GONTIJO, A. N. O jogo de dados entre o Estado e as Big Techs: uma análise jurídico-constitucional da soberania digital no Brasil. Revista de Geopolítica, v. 16, n. 5, e1179, 2025. DOI: 10.56238/revgeov16n5-303.

JABUR, A. P. COMPARAÇÃO ENTRE A LEI DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD) E A LEGISLAÇÃO DE PROTEÇÃO DE DADOS DOS ESTADOS UNIDOS: ANÁLISE COM ENFOQUE NOS ESTUDOS DE DANILO DONEDA, BRUNO BIONI E PERSPECTIVAS ATUAIS. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 11, n. 12, p. 7280-7289, 2025. DOI: 10.51891/rease.v11i12.23524.

Revista ARACÊ
ISSN: 2358-2472

MACHADO, K. A. N.; PRETA, K. P. B.; PUNGIRUM, J. M. SEGURANÇA DA INFORMAÇÃO PARA EMPRESAS NO BRASIL. Revista Multidisciplinar do Nordeste Mineiro, v. 10, n. 1, 2024. DOI: 10.61164/rmnm.v10i1.2985.

OLIVEIRA, B. R. UMA ANÁLISE DA EVOLUÇÃO DOS CASOS DE ESTELIONATO VIRTUAL APÓS A PROMULGAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). 2025. DOI: 10.22456/feisc.2025.364.

PEREZ, O. M. S.; SOUZA, B. de. Do público ao privado: representações sociais de associações acerca da responsabilidade com a questão socioambiental. Novos Cadernos NAEA, v. 25, n. 1, 2022. DOI: 10.18542/ncn.v25i1.9202.

REIS, R. T. P.; SAIKALI, L. C.; FREITAS, C. M. D. POLÍTICAS REGULATÓRIAS PARA A PROTEÇÃO DE DADOS NO BRASIL E A APLICABILIDADE DO MODELO DE REGULAÇÃO PELA ARQUITETURA DE CÓDIGO OU PRIVACY BY DESIGN. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 46, p. 363-385, 2022. DOI: 10.30899/dfj.v16i46.1118.

RODRIGUES, F. S.; MARTINS, J. J.; AMORIM, I. C. D. Golpe do falso advogado: estelionato digital, publicidade processual e proteção de dados no sistema de justiça brasileiro. Revista JRG de Estudos Acadêmicos, v. 8, n. 19, e082796, 2025. DOI: 10.55892/jrg.v8i19.2796.

SILVEIRA, M. F.; LIMA, M. P. ANÁLISE DA MOROSIDADE PROCESSUAL NAS COMPRAS PÚBLICAS E SEUS IMPACTOS NA EFICÁCIA DO ATENDIMENTO À SAÚDE PÚBLICA. 2023. DOI: 10.18066/inic0146.23.