www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 158, 2026 | DOI: 10.69849/g3vz5r98

Fraude processual na era da inteligência artificial: desafios jurídicos, éticos e tecnológicos para a justiça brasileira

Procedural fraud in the age of artificial intelligence: legal, ethical and technological challenges for brazilian justice

Paulo Afonso Bento[1]

Aline de Assis Rodrigues do Amaral Muniz[2]

Marina Teodoro[3]

RESUMO

O presente estudo tem como objetivo analisar os limites do regime jurídico brasileiro no enfrentamento da fraude processual mediada por inteligência artificial, identificando seus fundamentos normativos, suas lacunas e seus mecanismos possíveis de prevenção. Parte-se do problema de que o regime jurídico tradicional, estruturado para reprimir falsificações documentais e condutas desleais perceptíveis, tornou-se parcialmente insuficiente diante de provas digitais e conteúdos sintéticos produzidos por inteligência artificial generativa. A metodologia adotada é bibliográfica, descritiva e qualitativa, com exame do Código Penal, do Código de Processo Civil, da legislação sobre processo eletrônico, internet e proteção de dados, além de atos normativos do Conselho Nacional de Justiça, recomendações profissionais e precedentes sobre prova digital. Os resultados indicam que a boa-fé, a cooperação, a cadeia de custódia e as sanções por litigância de má-fé continuam essenciais, mas precisam ser complementadas por deveres específicos de rastreabilidade, verificação humana, preservação técnica, auditabilidade e responsabilização pelo uso abusivo de IA em juízo. Conclui-se que a resposta adequada não consiste em negar a utilidade da tecnologia, mas em construir uma

[1]Discente do Curso Superior de Direito da Instituição Universidade Evangélica de Goiás Campus Ceres – Ceres – Goiás – Brasil. E-mail: bento8765@gmail.com

[2]Universidade Evangélica de Goiás Campus Ceres – Ceres - Goiás – Brasil. ORCID: https://orcid.org/0000-0002-2280-163X

[3]Universidade Evangélica de Goiás Campus Ceres – Ceres - Goiás – Brasil. ORCID: https://orcid.org/0009-0004-4001-2900

governança processual da prova digital sintética, capaz de proteger o contraditório, a segurança jurídica e a confiança pública no Poder Judiciário.
Palavras-chave: fraude processual; inteligência artificial; prova digital; cadeia de custódia; segurança jurídica.

ABSTRACT

This study aims to analyze the limitations of the Brazilian legal system in addressing procedural fraud mediated by artificial intelligence, identifying its normative foundations, gaps, and possible prevention mechanisms. The research addresses the insufficiency of a traditional legal framework designed mainly to repress documentary forgery and visibly disloyal conduct when confronted with digital evidence and synthetic content produced by generative artificial intelligence. The methodology is qualitative, bibliographic and documentary, based on the Brazilian Criminal Code, the Code of Civil Procedure, legislation on electronic proceedings, internet governance and data protection, as well as regulations issued by the National Council of Justice, professional guidelines and case law concerning digital evidence. The findings show that good faith, cooperation, chain of custody and sanctions for bad-faith litigation remain indispensable, but they must be supplemented by specific duties of traceability, human verification, technical preservation, auditability and liability for abusive AI use in litigation. The article concludes that the appropriate response is not to reject technology, but to develop procedural governance for synthetic digital evidence, protecting adversarial proceedings, legal certainty and public trust in the Judiciary.
Keywords: procedural fraud; artificial intelligence; digital evidence; chain of custody; legal certainty.

1 INTRODUÇÃO

A fraude processual sempre teve um lugar delicado no sistema judiciário, uamvez que se destina somente à parte contrária. Ao alterar de forma artificial o estado de lugar, coisa, pessoa, documento, narrativa ou prova, o agente está atacando a própria função jurisdicional, pois desvia o processo de sua finalidade constitucional de reconstruir de maneira racional os fatos em disputa. Destaca-se que nos dias atuais, contudo,registros a digitalização do processo alterou o centro da confiança probatória: a solidez do papel foi maximizada pela confiança em metadados, registros de acesso, logs, assinaturas eletrônicas, arquivos digitais e ambientes de armazenamento

(Brasil,logs , assinaturas eletrônicas, arquivos digitais e ambientes de armazenamento (Brasil, 2015; Didier Júnior, 2018) . 2015; Didier Júnior, 2018).

Na concepção de Russell e Norvig (2021), a inteligência artificial generativa leva isso a outro nível.esses sistemas têm a capacidade de criar documentos e conteúdos, como textos, imagens e áudios, que parecem extremamente reais. Apesar de a tecnologia poder auxiliar na gestão processual e na identificação de erros, seu uso inadequado levanta questões jurídicas. Instrumentos geradores podem provocar equívocos judiciais, ocultar a autoria e enfraquecer o contraditório, apresentando aparências de verdade que não são passíveis de verificação. O dilema é encontrar o equilíbrio entre a inovação tecnológica e a integridade do processo judicial (Chesney; Citron, 2019).

O tema assume relevância prática porque o Judiciário brasileiro já se encontra inserido em ambiente de intensa digitalização. A informatização do processo judicial, prevista pela Lei n. 11.419/2006, a tramitação eletrônica, o uso de documentos digitais, o peticionamento remoto e a ampliação de sistemas de apoio à decisão modificaram profundamente o modo de produzir, apresentar e controlar a prova. Ao mesmo tempo, a Resolução CNJ n. 332/2020 e, posteriormente, a Resolução Conselho Nacional de Justiça (CNJ) n. 615/2025 consolidaram diretrizes de ética, transparência, governança, auditoria, supervisão humana e gestão de riscos para soluções de IA no Poder Judiciário (Brasil, 2006; CNJ, 2020; CNJ, 2025).

Este tema se justifica na medida que o rápido desenvolvimento da inteligência artificial (IA) afeta diretamente o sistema judicial, tanto no Brasil quanto em outros países, permitindo a emergência de novas formas de ilícitos processuais. Entre as diversas modalidades, sobressai a fraude processual cometida por meio de tecnologias que simulam identidades, forjam provas ou modificam documentos. Esse ponto de vista questiona a confiabilidade do sistema judicial e destaca as falhas na legislaçãoe nas O tema, investigado de forma interdisciplinar, permite uma compreensão mais ampla das implicações jurídicas, éticas e tecnológicas da questão, especificamente como base para aprimorar as normas e a atuação do Judiciário em face das inovações digitais.

Por conseguinte, a questão problema establelecida é a seguinte: o ordenamento jurídico brasileiro já dispõe de mecanismos adequados para prevenir, identificar e punir fraudes processuais realizadas com o auxíliode inteligência artificial, ou é necessário um aprimoramento normativo e técnico mais específico? Assim, a hipótese levantada é que o sistema possui

fundamentos importantes, como boa fé objetiva, cooperação, deveres processuais, tipos penais, cadeia de custódia, proteção de dados e atos normativos do CNJ, mas esses fundamentos ainda funcionam de maneira fragmentada e reativa em relação à prova digital sintética.

A metodologia adotada para este estudo foi a revisaod e literatura bibliográfica, descritiva e abordagem qualitativa..conforme Marcno e Lakatos (2017), a pesquisa bibliográfica inclui todo o material já publicado a respeito do tema em questão, como artigos científicos, monografias, dissertações e teses, e foi realizada uma análise do Código Penal, do Código de Processo Civil, da legislação pertinente ao processo eletrônico, à internete à proteção de dados, assim como dos atos normativos do Conselho Nacional de Justiça, das orientações profissionais e dos precedentes que tratam da prova digital.

Logo, a pesquisa descritiva tem como objetivo caracterizar um objeto, população ou especificidade , sem a manipulação de variáveis, apenas observando e analisando dados para obter um retrato detalhado do comportamento ou das características de um grupo ou situação (Gil, 2017). Já a abordagem qualitativa, é uma estratégia metodológica comum em várias disciplinas, permite investigar o fundo das nuances de uma característica, sem recorrer à estatística (Lunetta; Guerra, 2024).

2 REVISÃO DA LITERATURA

Inicialmente, discorre-se que a revisão teórica deste estudo baseia -se em três eixos interconectados. O primeiro é dogmático-processual, centrado na fraude processual enquanto viola à boa-fé, à cooperação, à verdade processual admissível e à segurança jurídica. O segundo é tecnológico-probatório, diz respeito à conversão do suporte documental em prova digital, à cadeia de custódia e ao surgimento de conteúdos sintéticos. O terceiro é de natureza regulatória, englobando tanto as normas brasileiras quanto as internacionais que tratam de IA, proteção de dados, governança, responsabilidade e transparência. Assim, esses eixos consistem em ser considerados em conjunto, uma vez que a fraude por IA não se limita a ser um crime, um incidente processual ou uma falha técnica: ela emerge na interseção entre a tecnologia, a ética profissional e a legitimidade da decisão judicial.

2.1 A Fraude Processual No Ordenamento Jurídico

A fraude processual é expressamente prevista no art. 347 do Código Penal (CP), que pune a inovação artificiosa, na pendência de processo civil ou administrativo, do estado de lugar, coisa ou pessoa, com a finalidade de induzir a erro o juiz ou o perito. O parágrafo único agrava a resposta quando a inovação se destina a produzir efeito em processo penal. Embora a redação do tipo tenha sido construída em contexto anterior à massificação digital, sua estrutura revela um núcleo ainda atual: a manipulação artificial do estado probatório com finalidade de engano jurisdicional (Brasil, 1940).

No plano processual civil, a fraude não se limita ao crime do art. 347. O Código de Processo Civil de 2015 impõe a todos os participantes do processo o dever de agir conforme a boa-fé, estabelece a cooperação entre os sujeitos processuais e prevê deveres de lealdade, veracidade e não criação de embaraços à efetivação das decisões judiciais. A litigância de má-fé, a alteração da verdade dos fatos, a resistência injustificada e o uso do processo para objetivo ilegal revelam que a fraude também pode ser enfrentada por sanções processuais e por medidas de correção da conduta abusiva (Brasil, 2015; Didier Júnior, 2018).

A boa-fé objetiva, nesse contexto, não depende apenas da intenção íntima do agente. Ela funciona como padrão normativo de conduta, exigindo comportamento leal, transparente e compatível com a confiança que sustenta o processo. Didier Júnior (2018) observa que a boa-fé processual possui fundamento constitucional e não pode ser reduzida a fórmula retórica: ela incide sobre partes, advogados, magistrados, auxiliares e todos os que participam da atividade jurisdicional. Essa leitura é decisiva para a fraude por IA, pois a submissão de documento sintético sem verificação adequada pode ser juridicamente censurável ainda que o usuário alegue ignorância técnica.

Neves (2025) observa que nesse novo cenário, as fraudes eletrônicas se tornaram mais complexas de serem identificadas, uma vez que as evidências deixaram de ser concretas, como na falsificação de documentos físicos. Em vez disso, os fraudadores passaram a usar softwares avançados para criar ou editar documentos digitais, permitindo uma manipulação mais rápida e menos detectável. A fraude eletrônica abrange, entre outras coisas, a utilização de assinaturas digitais falsificadas, a falsificação de e-mails, a alteração de registros bancários e a manipulação de dados em sistemas eletrônicos de tramitação processual.

Ainda Neves (2025) acrescenta que a Lei 12.965/2014, o Marco Civil da Internet, estabelece normas sobre a utilização da internet no Brasil, e embora tenha sido um avanço em

termos de proteção da privacidade, também trouxe desafios no combate a fraudes eletrônicas, uma vez que os fraudadores passaram a utilizar essas novas ferramentas para ampliar suas ações ilegais.

No atual processo civil, o enfrentamento à fraude processual não se limita às sanções impostas após uma fraude consumada, entretanto à existência de deveres estruturantes de conduta que sirvam para prevenir e orientar o comportamento dos sujeitos processuais. Nesse sentido, a boa-fé objetiva, a cooperação e o dever de lealdade são peças centrais, na medida em que se tornam referências normativas da integridade processual, cobrando das partes, dos advogados e do próprio juiz uma postura que seja condizente com a transparência, a honestidade e a confiabilidade do procedimento (Maia, 2025).

A boa-fé objetiva e a cooperação no processo permanecem como pilares do sistema, no entanto, passam a atuar em um debate crescente frente a fraudes cada vez mais sofisticadas, automatizadas e de difícil percepção (Ferreira; Scremin Neto, 2024). No ponto de vista de Theodoro Junior (2017), o princípio da boa-fé processual é um dos pilares que sustentam o sistema de justiça civil brasileiro. A boa-fé processual impõe um dever de lealdade entre todos os sujeitos do processo, incluindo as partes, os advogados, os juízes e os auxiliares da justiça.

Segundo Coêlho (2019), o artigo 6º do CPC, foi estabelecido o princípio da cooperação, que institui que todos os particpantes do processo devem colaborar entre si para alcançar uma decisão justa e eficaz em tempo razoável. O princípio da cooperação processual permite que as partes dialoguem com embasamento nas necessidades de interação em todas as etapas do conflito funciona como um instrumento que possibilita a visualização integral da atividade processual e assim, favorece a gestão eficiente da relação processual.

A cooperação não é exclusivamente texto legal, porém norma jurídica real, dotada de densidade semântica e transversalidade epistemológica. Destarte, a cooperação processual, constitui padrões morais de racionalidade jurídica a aperfeiçoar os comportamentos das partes, exigindo-lhes ética, honestidade e decoro (Ferreira; Scremin Neto, 2024). O princípio cooperativo passa a ser um instrumento de suma importância para a materialização das garantias constitucionais do devido processo legal e contraditório, na medida que proporciona meios para a sua concretização no processo, em compensação a outros modelos processuais nos quais essas garantias eram somente normas formais (Maia, 2025).

A fraude processual constitui uma das mais graves ameaças à segurança jurídica, pois compromete a integridade dos atos processuais, fragiliza a confiabilidade do sistema de justiça e interfere diretamente na formação do convencimento judicial (Trento, 2022). Em seguida, Silva (2020) discorre que a segurança jurídica, por sua vez, constitui valor essencial ao Estado de Direito, pois assegura previsibilidade, estabilidade e confiança nas relações jurídicas. Sob essa perspectiva, o processo judicial deve desenvolver-se sobre bases probatórias íntegras, verificáveis e submetidas ao contraditório, de modo que a decisão jurisdicional decorra de elementos confiáveis e juridicamente controláveis.

2.2 Inteligência Artificial E Suas Implicações No Judiciário

O capítulo anterior demonstrou que a fraude processual deixou de se limitar à falsificação material de documentos e passou a incorporar formas digitais de adulteração, ocultação, simulação e distorção informacional. A tese defendida neste capítulo é que o ordenamento jurídico brasileiro possui instrumentos relevantes para regular o uso institucional da inteligência artificial no Poder Judiciário e para controlar a admissibilidade de determinadas provas digitais.

Entretanto, tais instrumentos ainda não oferecem resposta suficientemente específica, preventiva e sistemática para a fraude processual praticada por meio de documentos artificiais, deepfakes, petições automatizadas, alucinações argumentativas, bots e campanhas coordenadas de manipulação reputacional. A insuficiência, portanto, não está na ausência absoluta de normas, mas na inadequação parcial das categorias tradicionais diante de uma fraude que atua sobre a própria aparência de realidade da prova.

A digitalização do processo judicial ampliou a eficiência administrativa, mas também deslocou o centro da confiança probatória. No processo físico, a falsificação incidia principalmente sobre suporte material, assinatura, rasura ou documento impresso. No processo eletrônico, a confiabilidade passa a depender de metadados, registros de acesso, cadeia de custódia, logs, integridade de arquivo, rastreabilidade de autoria e documentação técnica da coleta (Brasil, 2015). De acordo com Superior Tribunal de Justiça (STJ) (2024), essa mudança é decisiva porque a fraude processual com IA não apenas adultera documentos: ela pode criar uma realidade probatória plausível, sem correspondente factual, explorando a confiança do sistema em peças formalmente bem redigidas e arquivos visualmente convincentes.

A IA generativa aprofunda esse deslocamento porque opera por modelos capazes de produzir linguagem natural, código, imagens, sons e vídeos a partir de comandos simples. O problema jurídico não está na tecnologia em si, mas na sua aptidão para gerar conteúdo falso com alto grau de verossimilhança, inclusive citações jurisprudenciais inexistentes, narrativas probatórias coerentes e documentos aparentemente consistentes. A cartilha oficial sobre IA generativa no serviço público reconhece a utilidade desses sistemas, mas também alerta para limitações, erros e riscos de uso acrítico, enquanto o Instituto Nacional de Padrões e Tecnologia - EUA (NIST) enfatiza que sistemas generativos demandam gestão de risco, documentação e controle humano proporcional ao contexto de uso (Ministério da Gestão e da Inovação em Serviços Públicos, 2025; National Institute Of Standards And Technology - NIST, 2023).

Portanto, a tese ao demonstrar que a questão não é mais narrar o nascimento da internet, e sim compreender como a digitalização criou o ambiente no qual a IA generativa pode contaminar a prova e a argumentação judicial. A suficiência jurídica, portanto, não pode ser medida pela existência genérica de normas sobre processo eletrônico, mas pela capacidade específica de controlar autoria, autenticidade, integridade e rastreabilidade de conteúdos sintéticos (Brasil, 2015; STJ, 2026).

A evolução histórica da fraude processual acompanha a evolução dos suportes de informação. Em um primeiro momento, o foco recaía sobre documentos físicos, rasuras, assinaturas falsificadas, declarações montadas, alteração de objetos e manipulações materiais perceptíveis por exame grafotécnico, inspeção, confronto de documentos e perícia tradicional. Esse modelo não desapareceu, mas perdeu exclusividade. A digitalização ampliou a velocidade de circulação dos documentos, reduziu a dependência do suporte físico e deslocou o controle da autenticidade para elementos técnicos invisíveis ao observador comum, como metadados, hashes, registros de acesso, certificados, trilhas de auditoria e integridade de arquivos.

A Lei n. 11.419/2006 representou marco relevante ao admitir a informatização do processo judicial, a prática de atos eletrônicos e o uso de assinaturas digitais. Esse avanço trouxe ganhos de eficiência e acesso, mas também criou novos riscos: credenciais podem ser indevidamente utilizadas, arquivos podem ser adulterados antes da assinatura, sistemas podem ser explorados e documentos podem ostentar aparência formal regular sem corresponder a conteúdo verdadeiro. A assinatura eletrônica, por exemplo, comprova vínculo técnico entre signatário e

arquivo, mas não garante, isoladamente, a veracidade material do conteúdo assinado (Brasil, 2006).

O Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD) Lei nº 13.709/2018, ampliam o repertório normativo para lidar com registros, responsabilização, privacidade, proteção de dados e governança informacional. Ainda assim, tais diplomas não foram concebidos especificamente para disciplinar a admissibilidade, impugnação e perícia de prova sintética em juízo. Eles auxiliam na preservação de registros, na identificação de responsabilidades e na proteção de dados pessoais, mas não substituem um regime processual de controle da autenticidade de documentos produzidos ou manipulados por IA (Brasil, 2014; Brasil, 2018).

A noção de prova digital já exige metodologia de coleta e preservação. O STJ tem reforçado a inadmissibilidade ou fragilidade de provas extraídas sem documentação técnica adequada, especialmente quando não há garantia de integridade, autenticidade e confiabilidade dos elementos informáticos. Essa orientação é coerente com a cadeia de custódia, pois a prova digital é facilmente replicável, editável e descontextualizável. No ambiente de IA generativa, a exigência se torna mais intensa: não basta preservar o arquivo apresentado; é necessário discutir origem, autoria, contexto, ferramenta utilizada, metadados, STJ, 2021; STJ, 2024).

A passagem da prova digital para a prova sintética é o ponto central do problema. A prova digital pode consistir em dado verdadeiro produzido em ambiente eletrônico; a prova sintética, por sua vez, pode ser criada artificialmente para simular documento, fala, rosto, decisão, conversa ou evento que nunca ocorreu. Essa distinção não é meramente terminológica. Ela altera a lógica do contraditório, pois a parte impugnante não enfrenta apenas a dificuldade de demonstrar adulteração posterior, mas a possibilidade de que o próprio conteúdo tenha sido gerado do zero por sistema automatizado (STJ, 2021).

Para os fins desta tese, não basta conceituar inteligência artificial como sistema computacional capaz de executar tarefas associadas à inteligência humana. O conceito relevante é operacional: trata-se de um conjunto de sistemas baseados em dados e modelos capazes de classificar, prever, recomendar ou produzir conteúdo, com graus variáveis de autonomia e opacidade (Silva; Rocha, 2025). Essa definição é importante porque a fraude processual mediada por IA nasce justamente do uso externo desses sistemas para criar documentos, simular fatos,

automatizar petições ou produzir conteúdo audiovisual falso, e não apenas do uso institucional da tecnologia pelos tribunais (Russell; Norvig, 2021; CNJ, 2025).

Inteligência artificial pode ser compreendida, em sentido amplo, como o conjunto de sistemas computacionais capazes de executar tarefas associadas à percepção, classificação, predição, recomendação, geração de conteúdo e tomada de decisão apoiada por dados. Para a análise jurídica, porém, importa uma delimitação operacional. Há diferença entre IA analítica, empregada para triagem, classificação e apoio administrativo, e IA generativa, capaz de produzir texto, imagem, áudio, vídeo e código com aparência de autoria humana. A primeira suscita debates sobre viés, explicabilidade e supervisão; a segunda acrescenta o risco específico de fabricação de conteúdo probatório ou argumentativo (Russell; Norvig, 2021).

O Poder Judiciário brasileiro já incorporou tecnologias de apoio à gestão processual e à racionalização de fluxos. A Resolução CNJ n. 332/2020 estabeleceu parâmetros de ética, transparência e governança para a produção e uso de IA no Judiciário. A Resolução CNJ n. 615/2025 aprofundou esse regime ao disciplinar desenvolvimento, governança, auditoria, monitoramento e uso responsável de soluções de IA, com preocupação expressa com segurança da informação, proteção de dados, robustez, confiabilidade, prevenção de vieses e supervisão humana (CNJ, 2020; CNJ, 2025).

Para Valero et al (2024), esses atos normativos são importantes, mas seu foco predominante é a IA adotada institucionalmente pelos órgãos judiciais. A fraude processual por IA frequentemente ocorre fora da infraestrutura do Judiciário, quando uma parte cria um documento falso, um advogado submete precedente inexistente, um terceiro produz áudio manipulado ou uma campanha automatizada tenta pressionar a reputação de magistrados, testemunhas ou partes. A governança institucional, portanto, não equivale automaticamente a governança da prova sintética apresentada por usuários externos.

A Ordem dos Advogados do Brasil (OAB) também reconheceu a necessidade de orientar a advocacia quanto ao uso responsável da IA generativa. A Recomendação n. 001/2024 aponta a importância de conformidade com o Estatuto da Advocacia, o Código de Ética, o sigilo profissional, a revisão humana e a responsabilidade técnica do advogado. Esse parâmetro é indispensável: a IA pode auxiliar pesquisa e redação, mas não transfere ao software a responsabilidade pelo conteúdo submetido ao juízo. Quando uma petição contém jurisprudência

inventada, dados sigilosos indevidamente inseridos em ferramenta aberta ou narrativa probatória artificial, o dever de conferência profissional permanece íntegro (OAB, 2024).

No plano internacional, instrumentos como a Recomendação da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) sobre Ética da IA, os Princípios da Cooperação e Desenvolvimento Econômico (OCDE), e o NIST AI Risk Management Framework (AI RMF), reforçam diretrizes de transparência, governança de riscos, supervisão humana, equidade, segurança, documentação e responsabilidade. Esses documentos não resolvem diretamente a disciplina processual brasileira, mas oferecem vocabulário técnico-normativo útil para formular padrões de auditabilidade, rastreabilidade e contestabilidade de sistemas e conteúdos gerados por IA (Unesco, 2021; NIST, 2023).

A seguir discorre-se sobre as modalidades de fraude processual com uso de IA. A primeira modalidade é a produção de documentos falsos por IA generativa. A Inteligência Artificial Generativa (IAG) tem se consolidado como um dos maiores avanços tecnológicos da atualidade, especialmente no campo da modelagem computacional, que utiliza algoritmos avançados para aprender padrões a partir de vastos volumes de dados. Soares (2025) relata que o progresso da IAG tem tornado a criação de documentos falsos com uma precisão visual jamais vista,Ferramentas de texto e imagem podem criar contratos, recibos, declarações, certidões, relatórios, conversas, e-mails, laudos aparentes e trechos de decisões com linguagem formal convincente.

Ainda Soares (2025), a gravidade está na combinação entre aparência técnica, coerência narrativa e inexistência de lastro factual. O documento pode ingressar no processo como anexo, transcrição, print, ata, prova emprestada ou simples fundamento argumentativo, produzindo efeito persuasivo antes mesmo de ser submetido a controle pericial.

A segunda modalidade envolve manipulação de provas digitais (deepfakes de áudio, vídeo e imagem). Deepfakes são conteúdos sintéticos ou manipulados que simulam a fala, o rosto, a presença ou o comportamento de pessoa real. No processo judicial, esse tipo de conteúdo pode afetar reconhecimento de autoria, confissão, ameaça, injúria, negociação, consentimento, presença em local, prova de contato ou integridade de depoimento (Guimarães, 2025). Chesney e Citron (2019) já advertiam que deepfakes desafiam privacidade, reputação, democracia e segurança, e a esfera processual adiciona problema específico: a aparência audiovisual tende a

exercer forte impacto cognitivo sobre julgadores e partes, mesmo quando tecnicamente contestável.

A terceira modalidade é criação de petições automáticas fraudulentas em massa, jurisprudência, doutrina ou fundamentação inexistente. Soares (2025) menciona que a petição automatizada reflete a integração entre o trabalho jurídico tradicional e as ferramentas tecnológicas, que tornam o processo mais ágil e eficientModelos generativos podem produzir respostas formalmente elegantes, mas juridicamente falsas, fenômeno conhecido como alucinação.

Segundo Almeida (2024), no processo, a alucinação deixa de ser mero erro tecnológico quando se converte em fundamento de petição, parecer, decisão ou recurso. O dever de verificação humana é indispensável, pois o sistema judicial depende de fontes oficiais e rastreáveis. A citação de precedente inexistente compromete a boa-fé, desperdiça recursos jurisdicionais e pode configurar litigância de má-fé, além de gerar responsabilidade profissional.

Contudo, a automação de peças não é, por si, ilícita. Ela pode padronizar demandas repetitivas legítimas, reduzir custos e ampliar acesso à justiça. O abuso surge quando a automação gera litigância em massa sem controle individualizado, multiplica alegações genéricas, oculta informações relevantes, reproduz teses sabidamente improcedentes ou cria assimetria processual pela escala artificial. Nesses casos, a IA não apenas auxilia o advogado; ela passa a industrializar o uso estratégico do processo, tensionando a boa-fé, a cooperação e a duração razoável do processo (Brasil, 2015).

A quinta modalidade envolve bots, desinformação processual e ataques reputacionais em rede. Sistemas automatizados podem disseminar narrativas falsas sobre processos, partes, testemunhas, peritos ou magistrados, buscando influenciar o ambiente externo do julgamento, intimidar sujeitos processuais ou fragilizar a confiança pública no Judiciário (Dias; Silva, 2023). Embora nem todo ataque reputacional constitua fraude processual em sentido estrito, ele pode integrar estratégia de manipulação do processo quando vinculado a provas fabricadas, campanhas coordenadas ou tentativa de constranger a atividade jurisdicional (Rosa, 2025).

A sexta modalidade é a manipulação de metadados e rastros digitais. A prova eletrônica não se limita ao conteúdo visível: datas, autoria, localização, histórico de edição, registros de criação, logs de acesso e hashes podem ser decisivos para atestar integridade. A IA pode facilitar alterações, simulações ou reconstruções plausíveis de contexto. A impugnação passa a exigir

capacidade técnica, preservação do arquivo original, comparação de versões e perícia computacional. Sem isso, o contraditório se torna formal, porque a parte pode não dispor de meios efetivos para demonstrar a artificialidade do elemento apresentado.

Em relação a jurisprudência, prova digial e insuficiência atuais. A análise jurisprudencial é indispensável para verificar se os tribunais brasileiros já conseguem responder aos riscos de fraude processual mediados por IA. Como ainda são escassos os julgados especificamente voltados a deepfakes probatórias ou documentos sintéticos gerados por IA, a investigação deve partir dos precedentes sobre prova digital, cadeia de custódia, autenticidade, integridade e metodologia de extração. Esses precedentes não resolvem integralmente o problema da IA generativa, mas indicam o padrão jurídico que tende a orientar sua aplicação futura.

O primeiro padrão identificado é o da desconfiança técnica diante de provas digitais sem preservação adequada. O STJ, no RHC 99.735/SC, considerou inválida a prova obtida por espelhamento de conversas via WhatsApp Web, destacando que a ferramenta permite acesso amplo a conversas pretéritas e possibilidade de interferência ativa, inclusive com envio e exclusão de mensagens. A relevância desse julgado para a presente tese está em reconhecer que a prova digital não pode ser tratada como reprodução neutra da realidade quando o meio de obtenção permite alteração, supressão ou interferência sem rastros confiáveis.

O segundo padrão aparece em julgados posteriores do STJ sobre extração de dados de aparelho celular. No AgRg no HC 828.054/RN, a Quinta Turma entendeu que prints e dados extraídos sem metodologia adequada são inadmissíveis no processo penal quando não houver procedimentos capazes de assegurar idoneidade, integridade e confiabilidade. O critério decisório não foi apenas formal; foi técnico-probatório. A prova digital exige documentação do modo de coleta, preservação, extração e tratamento. Sem esse percurso verificável, o contraditório fica esvaziado, porque a parte adversa não consegue reproduzir ou auditar o material apresentado (SSTJ, 2024).

Esse entendimento é decisivo para a tese porque demonstra que a autenticidade digital não pode ser presumida pelo simples fato de o conteúdo ter sido apresentado em juízo. A lógica adotada pelo STJ desloca o centro da discussão da aparência do arquivo para a metodologia de coleta, preservação, documentação e controle técnico, aproximando a prova digital da exigência de rastreabilidade própria da cadeia de custódia. (STJ, 2024; NIST, 2006).

O terceiro padrão foi reforçado no AgRg no HC 1.014.212/ES, em que a Sexta Turma do STJ afirmou que, havendo dúvida razoável sobre a integridade e a autenticidade da prova digital, é necessária a realização de exame pericial para assegurar a confiabilidade do material e o exercício do contraditório. Esse julgamento aprofunda a ideia de que a prova digital possui vulnerabilidades próprias e que a autorização judicial ou a identificação do agente responsável pela obtenção do dado não suprem, por si só, a ausência de documentação técnica adequada (STJ, 2021).

A consequência jurídica desse padrão é relevante: os tribunais já reconhecem que a prova digital exige metodologia, mas ainda não há disciplina legislativa suficientemente detalhada para prova sintética gerada por IA. Se prints e dados extraídos de celular já exigem cautela técnica, com maior razão deepfakes, áudios clonados, imagens artificiais e documentos produzidos por modelos generativos devem exigir critérios reforçados de origem, integridade, metadados, hash, logs, perícia e contraditório técnico. (STJ, 2026; Chesney; Citron, 2019).

Esses julgados permitem construir uma linha jurisprudencial: a autenticidade da prova digital não deve ser presumida quando o modo de coleta, preservação ou apresentação do conteúdo compromete auditabilidade, reprodutibilidade e rastreabilidade. O tribunal não exige perícia em todo e qualquer arquivo digital, mas exige rigor quando há risco concreto de alteração, ausência de cadeia de custódia, fragilidade metodológica ou dúvida razoável sobre a integridade. Esse padrão é diretamente aplicável à prova sintética produzida por IA, pois deepfakes e documentos generativos elevam o grau de dúvida técnica sobre origem, autoria e correspondência com a realidade.

O quarto padrão, de natureza setorial, vem da Justiça Eleitoral. A Resolução Tribunal Superior Eleitoral (TSE) nº 23.732/2024 não é precedente judicial em sentido estrito, mas expressa resposta normativa especializada a riscos já identificados pelo próprio sistema de justiça: conteúdo sintético, deepfake, uso de IA, chatbots e manipulação informacional. O TSE adotou lógica preventiva ao exigir informação explícita sobre conteúdo fabricado ou manipulado por IA e ao proibir deepfake com potencial de afetar a integridade do processo eleitoral.

Essa resposta revela que, quando o risco de manipulação do ambiente decisório é reconhecido, o direito brasileiro admite deveres de transparência, rotulagem, remoção e responsabilização mais específicos. A importância desse exemplo está em mostrar que respostas setoriais são possíveis, mas também evidenciar que o processo civil e penal comum ainda não

contam com disciplina equivalente para litígios judiciais ordinários. (TSE, 2024; Chesney; Citron, 2019).

A comparação entre STJ e TSE evidencia dois modelos de resposta. O STJ tem desenvolvido resposta predominantemente probatória e reativa, centrada em cadeia de custódia, perícia, integridade e inadmissibilidade da prova digital quando o método de obtenção é frágil. O TSE, por sua vez, adotou resposta mais preventiva e regulatória, com deveres de rotulagem e proibição expressa de deepfake em contexto eleitoral. Para a tese, essa diferença é essencial: o processo judicial comum ainda depende de categorias gerais e precedentes sobre prova digital, enquanto o campo eleitoral já possui regras mais específicas para conteúdo sintético.

Portanto, a jurisprudência brasileira já oferece critérios relevantes, mas ainda não responde plenamente ao problema da fraude processual por IA generativa. Os tribunais conseguem reagir quando há ausência de cadeia de custódia, dúvida sobre autenticidade ou metodologia inadequada. Todavia, ainda falta uma matriz jurisprudencial consolidada sobre documentos inteiramente sintéticos, deepfakes de alta qualidade, petições com precedentes inventados e campanhas coordenadas de manipulação reputacional. O padrão atual é promissor, mas insuficiente: protege a integridade da prova digital em casos específicos, sem ainda formar um regime completo para a prova artificial

2.3 Fraude Processual Na Era Da Inteligência Artificial: Respostas Jurídicas, Insuficiências Normativas E Mecanismos De Prevenção

O Código Penal, o Código de Processo Civil, a LGPD, o Marco Civil da Internet e as resoluções do CNJ oferecem instrumentos relevantes, porém nenhum deles estrutura, de modo específico e sistemático, um regime de prevenção, identificação, autenticação e responsabilização para provas sintéticas produzidas por inteligência artificial generativa (Brasil, 1940; Brasil, 2015).

Essa distinção é decisiva para a tese, porque a existência de normas aplicáveis não se confunde com suficiência normativa. A fraude processual tradicional pressupõe a alteração artificiosa de coisa, pessoa, lugar, documento ou informação; já a fraude processual por IA pode criar uma aparência integral de realidade, mediante texto, imagem, voz, vídeo, metadado ou jurisprudência inexistente, reduzindo a capacidade do juiz e das partes de perceberem a falsidade sem apoio técnico especializado (Goodfellow et al., 2014). O art. 347 do Código Penal continua

sendo relevante ao punir a inovação artificiosa destinada a induzir juiz ou perito a erro, assim como os tipos de falsidade documental e estelionato podem alcançar determinadas condutas fraudulentas praticadas com apoio tecnológico (Chesney; Citron, 2019).

A LGPD contribui ao exigir finalidade, adequação, necessidade, segurança, prevenção, responsabilização e possibilidade de revisão de decisões automatizadas, sobretudo quando dados pessoais ou sensíveis são tratados no ambiente judicial. Contudo, a LGPD não foi concebida como estatuto probatório da inteligência artificial, razão pela qual protege dados e titulares, mas não define, com precisão processual, critérios de admissibilidade, impugnação e perícia de provas geradas ou adulteradas por IA (Brasil, 2018; CNJ, 2025). A Recomendação nº 001/2024 do Conselho Federal também contribui ao reconhecer que a IA generativa pode auxiliar a prática jurídica, desde que submetida a supervisão humana.

A jurisprudência brasileira já oferece sinais relevantes sobre a forma como os tribunais estão reagindo à prova digital e ao uso indevido da inteligência artificial, mas ainda não formou um regime decisório completo para a fraude processual algorítmica. O padrão que emerge é de respostas pontuais: ora os tribunais exigem cadeia de custódia e metodologia técnica, ora aplicam sanções por litigância de má-fé diante de precedentes inexistentes, ora tratam a manipulação sintética em áreas específicas, como a propaganda eleitoral. (STJ, 2024; TJPR, 2025).

O eixo jurisprudencial envolve o uso de IA generativa para criação de jurisprudência inexistente. No Recurso em Sentido Estrito nº 0002062-61.2025.8.16.0019, o Tribunal de Justiça do Paraná não conheceu recurso cujas razões continham quarenta e três julgados inexistentes, criados por inteligência artificial, destacando a impossibilidade de separar alegações verdadeiras de referências fabricadas e reafirmando que apenas o advogado possui capacidade postulatória e dever de revisão técnica (TJPR, 2025; OAB, 2024).

Na Justiça do Trabalho, decisões recentes também passaram a aplicar multa por litigância de má-fé quando partes apresentam julgados ou fundamentos inexistentes produzidos por IA, inclusive com comunicação à OAB para apuração disciplinar. O padrão decisório é convergente: o uso de IA não afasta a responsabilidade do advogado ou da parte, pois a assinatura da peça implica dever de conferência, diligência, veracidade e supervisão humana. (TRT2, 2025; OAB, 2024).

O terceiro eixo aparece no campo eleitoral, em que o TSE proibiu deepfakes e disciplinou o uso de inteligência artificial em conteúdos político-eleitorais, reconhecendo que a manipulação

sintética pode distorcer a deliberação pública e afetar a integridade de processos decisórios. Embora a norma eleitoral não regule diretamente o processo civil ou penal comum, ela revela que o ordenamento já admite resposta específica quando a IA ameaça ambientes institucionais sensíveis. (TSE, 2024; UNESCO, 2021).

Portanto, a jurisprudência confirma a tese, porque demonstra que os tribunais já percebem os riscos da prova digital e da IA generativa, mas respondem por decisões isoladas, sem um protocolo nacional e sistemático. Assim, a jurisprudência resolve casos concretos, mas ainda não resolve o problema estrutural da fraude processual algorítmica, que exige regras uniformes sobre autenticidade, cadeia de custódia, perícia, dever de revelação, responsabilidade profissional e sanção. (STJ, 2026; CNJ, 2025).

Na concepção de Araujo (2023), a cadeia de custódia digital deve ocupar posição central no enfrentamento da fraude por IA. Inspirada na documentação do vestígio desde o reconhecimento até o descarte, ela deve registrar origem, coleta, ferramenta empregada, responsável, data, ambiente técnico, hash criptográfico, armazenamento, transferências e eventuais conversões do arquivo. Em conteúdos suspeitos de geração sintética, a cadeia deve incluir preservação do arquivo original, metadados, logs, histórico de edição e informações sobre a fonte de obtenção, sempre que possível (Brasil, 1941; STJ, 2024).

Costa (2019) descreve que a certificação digital e a assinatura eletrônica qualificada continuam relevantes para autoria formal, integridade do arquivo e não repúdio. Todavia, não devem ser tratadas como selo absoluto de verdade. Um documento assinado digitalmente pode conter fato falso, citação inexistente, imagem manipulada ou texto gerado por IA sem revisão. A certificação prova que determinado arquivo foi assinado por determinado certificado em determinado contexto; não elimina a necessidade de controle sobre conteúdo, origem, cadeia de formação e veracidade material (Brasil, 2006; Brasil, 2015).

O blockchain pode contribuir para registrar hashes e eventos de custódia em estrutura resistente à alteração, criando trilha auditável. Sua utilidade está na preservação de integridade a partir do momento do registro. Entretanto, blockchain não transforma conteúdo falso em verdadeiro: se um deepfake for registrado de forma íntegra, a tecnologia apenas preservará aquele arquivo falso. Por isso, seu emprego deve ser associado à coleta adequada, identificação de responsáveis, validação pericial, interoperabilidade com sistemas judiciais e contraditório técnico (Malik et al, 2023).

A IA defensiva também pode auxiliar. Ferramentas de detecção de padrões sintéticos, análise de metadados, verificação automatizada de citações, comparação de petições, identificação de similaridades e alertas de inconsistência podem reduzir riscos. Contudo, o remédio não pode repetir o vício. Sistemas defensivos precisam ser auditáveis, documentados, supervisionados por humanos e sujeitos a contestação, sob pena de substituírem uma opacidade por outra. A detecção automatizada deve funcionar como indicativo técnico, não como prova absoluta (Mittelstadt, 2019; NIST, 2023).

No plano profissional, escritórios, órgãos públicos e departamentos jurídicos devem adotar rotinas internas: proibição de inserir dados sigilosos em ferramentas sem garantias, identificação de fontes oficiais, conferência manual de jurisprudência, registro de revisão humana, preservação de versões, treinamento contínuo e política de uso responsável de IA. No plano judicial, recomenda-se protocolo nacional para prova digital e sintética, com critérios de admissibilidade, impugnação, perícia, guarda de arquivos, dever de preservação e cooperação técnica entre Judiciário, advocacia, Ministério Público, Defensoria, perícia e plataformas digitais (OAB, 2024; CNJ, 2025).

Como limitação, reconhece-se que o tema está em rápida evolução normativa e técnica. Ferramentas generativas, métodos de detecção, padrões de perícia e atos regulatórios podem ser atualizados em curto intervalo. Por essa razão, o artigo não pretende oferecer resposta definitiva, mas estruturar um quadro teórico-jurídico consistente para demonstrar a necessidade de regime processual específico de integridade da prova digital sintética.

3 CONSIDERAÇÕES FINAIS

O estudo demonstrou que a fraude processual, tradicionalmente vinculada à falsificação documental e à manipulação perceptível de provas, sofreu profunda transformação com a digitalização do processo e com a ascensão da inteligência artificial generativa. O art. 347 do Código Penal, os deveres de boa-fé e cooperação previstos no Código de Processo Civil e as sanções por litigância de má-fé continuam relevantes, mas foram concebidos em lógica predominantemente reativa, voltada a condutas mais facilmente identificáveis. A prova sintética, ao contrário, pode nascer com aparência de autenticidade, coerência formal e alto potencial persuasivo, dificultando a percepção imediata da fraude.

Observa-se que o ordenamento jurídico brasileiro possui instrumentos importantes, mas ainda insuficientes em termos de unidade, prevenção e especificidade. A Resolução CNJ n. 615/2025 representa avanço no uso responsável de IA pelo Judiciário, mas não disciplina de forma completa a IA utilizada por litigantes e profissionais para criar, alterar ou apresentar conteúdos sintéticos. A jurisprudência do STJ sobre prova digital reforça a necessidade de metodologia e cadeia de custódia, mas ainda precisa ser complementada por parâmetros próprios para deepfakes, documentos gerados por IA, precedentes inexistentes e peticionamento automatizado abusivo.

Conclui-se que, a fraude processual na era da inteligência artificial exige mudança de paradigma: do controle centrado na aparência documental para o controle baseado em rastreabilidade, auditabilidade e contraditório técnico. Somente assim será possível preservar a segurança jurídica, a paridade de armas, a confiança pública e a legitimidade das decisões judiciais diante de um ambiente probatório cada vez mais automatizado, sintético e tecnicamente sofisticado.

REFERÊNCIAS

ALMEIDA, Marcela Zanelato. **Uso da inteligência artificial na era do crime digital**. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2024. Disponível em: https://sapientia.pucsp.br/bitstream/handle/43824/1/TCC%20Marcela%20Zanelato%20Almeida%20%281%29_Greice%20Patricia%20Full.pdf. Acesso em: 27 jan. 2026.

ARAÚJO, Matheus. Inteligência artificial, blockchain e a cadeia de custódia da prova no processo penal. **Revista da Universidade Federal de Minas Gerais**, Belo Horizonte, v. 30, e47605, 2023. Disponível em: https://periodicos.ufmg.br/index.php/revistadaufmg/article/view/47605/. Acesso em: 10 fev. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Institui o Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 abr. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Institui o Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 5 maio 2026.

BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial. Brasília, DF: Presidência da República, 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 1 maio 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 maio 2026.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Institui o 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: 9 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 3 maio 2026.

CHESNEY, Robert M.; CITRON, Danielle Keats. Deep fakes: a looming challenge for privacy, democracy, and national security. **California Law Review**, v. 107, p. 1753-1820, 2019. Disponível em: https://scholarship.law.bu.edu/faculty_scholarship/640/. Acesso em: 12 maio 2026.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 332, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429. Acesso em: 8 maio 2026.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 615, de 11 de março de 2025**. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas

com recursos de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2025. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6001. Acesso em: 12 maio 2026.

COSTA, Marília Siqueira. O princípio da boa-fé como fundamento jurídico da vedação ao abuso do direito de recorrer. **Civil Procedure Review**, v. 10, n. 1, jan./abr. 2019. Disponível em: https://www.civilprocedurereview.com/revista/article/download/182/170/340. Acesso em: 12 mar. 2026.

DIAS, Jefferson Aparecido; SILVA, Fabiano Fernando. Bots, fake news, fake faces, deepfakes e sua eventual influência no processo eleitoral democrático. **Revista da Advocacia do Poder Legislativo**, 2021. Disponível em: https://revista.anpal.org.br/wpcontent/uploads/2022/03/Artigo_02_Fabiano_Fernando_e_Jefferson_Aparecido-1.pdf. Acesso em: 29 jan. 2026.

DIDIER JÚNIOR, Fredie. Princípio da boa-fé processual no direito processual civil brasileiro e seu fundamento constitucional. **Revista do Ministério Público do Rio de Janeiro**, n. 70, p. 179-188, out./dez. 2018. Disponível em: https://www.mprj.mp.br/documents/20184/1183784/Fredie_Didier_Jr.pdf. Acesso em: 7 maio 2026.

FERREIRA, Jussara Suzi Assis Borges Nasser; SCREMIN NETO, Ferdinando. A reafirmação do princípio da cooperação processual à luz dos deveres anexos da boa-fé objetiva. **Revista de Ciências Jurídicas e Sociais da UNIPAR**, v. 27, n. 1, p. 17-41, 2024. Disponível em: https://revistas.unipar.br/index.php/juridica/article/view/11553. Acesso em: 10 dez. 2025.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. São Paulo: Atlas, 2018.

GOODFELLOW, Ian J. *et al.* Generative adversarial nets. *In*: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 27., 2014, Montréal. **Proceedings** [...]. Montréal: NIPS, 2014. p. 2672-2680. Disponível em: https://papers.neurips.cc/paper/5423-generative-adversarial-nets.pdf. Acesso em: 5 maio 2026.

GUIMARÃES, Pablo Rafael da Cunha. Provas no processo judicial e a ameaça de conteúdos gerados por IA. **Revista PPC – Políticas Públicas e Cidades**, Curitiba, v. 14, n. 7, p. 1-20, 2025. Disponível em: https://journalppc.com/RPPC/article/view/2178/1543. Acesso em: 18 fev. 2026.

LUNETTA, A.; GUERRA, R. Metodologias e classificação das pesquisas científicas. **Recima21 – Revista Científica Multidisciplinar**, v. 5, n. 8, 2024. Disponível em: https://recima21.com.br/recima21/article/download/5584/3830/33469. Acesso em: 16 mar. 2026.

MAIA, Lívia. Princípio da boa-fé processual: importância e limitações da boa-fé no desenvolvimento do processo civil. **Jusbrasil**, 13 jan. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/principio-da-boa-fe-processual-importancia-e-limitacoes-da-boa-fe-no-desenvolvimento-do-processo-civil/2978840510. Acesso em: 10 dez. 2025.

MALIK, Anas *et al.* Blockchain-based digital chain of custody multimedia evidence preservation framework for IoT devices. **Forensic Science International: Digital Investigation**, v. 46, 301602, 2023. DOI: https://doi.org/10.1016/j.fsidi.2023.301602. Acesso em: 27 abr. 2026.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos da metodologia científica**. 8. ed. São Paulo: Atlas, 2020.

MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. **Nature Machine Intelligence**, v. 1, n. 11, p. 501-507, 2019. Disponível em: https://www.nature.com/articles/s42256-019-0114-4. Acesso em: 4 maio 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Artificial Intelligence Risk Management Framework (AI RMF 1.0)**. NIST AI 100-1. Gaithersburg: NIST, 2023. Disponível em: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. Acesso em: 1 maio 2026.

NEVES, Marcelo Alves. Fraude processual: análise jurídica do artigo 347 do Código Penal. **Jusbrasil**, 13 jan. 2025. Disponível em: https://www.jusbrasil.com.br/artigos/fraude-processual-analise-juridica-do-artigo-347-do-codigo-penal/2977368569. Acesso em: 29 nov. 2025.

ORDEM DOS ADVOGADOS DO BRASIL. **Recomendação nº 001/2024**. Apresenta diretrizes para orientar o uso de Inteligência Artificial generativa na prática jurídica. Brasília, DF: Conselho Federal da OAB, 2024. Disponível em: https://diario.oab.org.br/pages/materia/842347. Acesso em: 5 maio 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. **Recommendation on the ethics of artificial intelligence**. Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 12 maio 2026.

ROSA, Alexandre Morais. ChatGPT: 'Primeiro você alucina, inventa jurisprudência' ou 'não era julgado, era cilada'. **Consultor Jurídico**, 25 abr. 2025. Disponível em: https://www.conjur.com.br/2025-abr-25/chatgpt-primeiro-voce-alucina-inventa-jurisprudencia-ou-nao-era-julgado-era-cilada/. Acesso em: 27 fev. 2026.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**: uma abordagem moderna. 4. ed. São Paulo: Pearson, 2021.

SILVA, Fabiano Machado; ROCHA, Alexandre Almeida. Inteligência artificial: uso ético e inclusivo da IA no direito, suas aplicações no judiciário e seus impactos no acesso à justiça. **Revista Jurídica Gralha Azul**, v. 1, n. 28, 2025. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/191. Acesso em: 23 nov. 2025.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 43. ed., rev. e atual. São Paulo: Malheiros, 2020.

SOARES, Guilherme Gabriel Sousa *et al.* Os impactos da utilização da inteligência artificial no processo penal: desafios éticos à segurança jurídica das garantias fundamentais do réu. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 11, n. 11, nov. 2025. Disponível em: https://periodicorease.pro.br/rease/article/download/22608/13923/65037. Acesso em: 22 jan. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Sexta Turma reafirma invalidade de prova obtida pelo espelhamento de conversas via WhatsApp Web**. Brasília, DF: STJ, 9 mar. 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/09032021-Sexta-Turma-reafirma-invalidade-de-prova-obtida-pelo-espelhamento-de-conversas-via-WhatsApp-Web.aspx. Acesso em: 29 mar. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Quinta Turma não aceita como provas prints de celular extraídos sem metodologia adequada**. Brasília, DF: STJ, 2 maio 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/02052024-Quinta-Turma-nao-aceita-como-provas-prints-de-celular-extraidos-sem-metodologia-adequada.aspx. Acesso em: 2 maio 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Sexta Turma afasta prisão preventiva até conclusão de perícia sobre prints de WhatsApp usados como prova**. Brasília, DF: STJ, 9 mar. 2026. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=358337181&registro_numero=202502313413&peticao_numero=202500890257&publicacao_data=20260220&formato=PDF. Acesso em: 1 abr. 2026.

THEODORO JÚNIOR, Humberto. **Curso de direito processual civil**: teoria geral do direito processual civil, processo de conhecimento e procedimento comum. 58. ed., rev., atual. e ampl. Rio de Janeiro: Forense, 2017. v. 1.

TRENTO, Paulo Gustavo. Breves apontamentos sobre a fraude no processo e no direito material. **Research, Society and Development**, v. 11, n. 3, e39711326708, 2022. Disponível em: https://rsdjournal.org/rsd/article/download/26708/23367. Acesso em: 13 dez. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. **Recurso em Sentido Estrito nº 0002062-61.2025.8.16.0019**. Relator: Des. Gamaliel Seme Scaff. 1ª Câmara Criminal. Julgado em: 12 abr. 2025. Disponível em: https://portal.tjpr.jus.br/jurisprudencia/j/4100000031991241/Ac%C3%B3rd%C3%A3o-0002062-61.2025.8.16.0019. Acesso em: 12 mar. 2026.

TRIBUNAL SUPERIOR ELEITORAL. **TSE proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições**. Brasília, DF: TSE, 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes. Acesso em: 12 maio 2026.

VALERO, Vanessa França *et al.* Do processo jurídico usando ferramentas tecnológicas sob a perspectiva do Programa Justiça 4.0. *In*: FÓRUM DE INICIAÇÃO CIENTÍFICA DO UNIFUNEC, 14., 2024, Santa Fé do Sul. **Anais** [...]. Santa Fé do Sul: UNIFUNEC, 2024. Disponível em: https://seer.unifunec.edu.br/index.php/forum/article/view/6236. Acesso em: 14 mar. 2026.