Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

# A PROVA SINTÉTICA: DEEPFAKES DOCUMENTAIS E O FUTURO DA VERDADE NO PROCESSO BRASILEIRO[138]

## *SYNTHETIC EVIDENCE: DOCUMENTARY DEEPFAKES AND THE FUTURE OF TRUTH IN BRAZILIAN LEGAL PROCEEDINGS*

**Antonio Lopo Martinez**

Doutor em Direito pela Universidade de Coimbra e pela Universidade de Salamanca. Pós-doutor na Faculdade de Direito da Universidade de Lisboa. Doutor em Contabilidade pela Universidade de São Paulo. Bolsista de Produtividade em Pesquisa do CNPq. Auditor Fiscal da Receita Federal. E-mail: almartinez@fd.uc.pt. ORCID: https://orcid.org/0000-0001-9624-7646

**RESUMO:** O artigo demonstra que *deepfakes* documentais deslocam a fraude da adulteração *ex post* para a falsidade originária, produzindo contratos, recibos, laudos e comunicações oficiais com aparência impecável à inspeção ocular. O artigo objetiva mapear essas vulnerabilidades no ordenamento processual brasileiro e propor uma arquitetura probatória e procedimental capaz de enfrentá-las. A partir de casos recentes, mapeiam-se vulnerabilidades do processo brasileiro: métodos de autenticação centrados na cadeia de custódia da coleta não alcançam a verificação de proveniência; princípios como verdade material, contraditório e paridade de armas sofrem abalos; e o dividendo do mentiroso permite desacreditar provas autênticas. Com base em uma leitura semiótica de Peirce, explica-se a persuasão sintética pela convergência de iconicidade, indexicalidade e simbolicidade, que constrói uma "realidade documental" compatível com as expectativas cognitivas do julgador. Propõe-se uma arquitetura probatória em duas camadas: autenticidade na origem (registro de *hash* na criação e marca d'água frágil institucional) e perícia algorítmica multimodal e explicável para valoração *ex post*. No plano procedimental, recomenda-se a criação de incidente de falsidade sintética, a distribuição dinâmica do ônus da prova (art. 429 do CPC) quando houver suspeita plausível, o reconhecimento da perda de uma chance probatória diante de arquivos sem trilha auditável e a padronização de formatos e metadados nos sistemas judiciais eletrônicos, acompanhadas de protocolos de verificação e capacitação contínua. Conclui-se pela urgência de um paradigma proativo, no qual o parecer autêntico cede lugar ao ser tecnicamente autêntico,

[138] Artigo recebido em 11/03/2026 e aprovado em 09/04/2026.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

restaurando a prova digital como vestígio confiável.

**PALAVRAS-CHAVE:** Deepfakes documentais; Prova digital; Autenticidade documental; Inteligência artificial generativa; Direito probatório.

**ABSTRACT:** This paper argues that documentary deepfakes shift fraud from *ex post* tampering to original falsity, producing contracts, receipts, expert reports, and official communications that look flawless to visual inspection. Drawing on recent cases, it maps systemic vulnerabilities in Brazilian procedure: authentication methods focused on the chain of custody at collection fail to establish provenance; core principles, material truth, adversarial parity, and the right to a defense, are strained; and the liar's dividend enables bad-faith challenges to genuine evidence. A Peircean semiotic lens explains synthetic persuasion through the convergence of iconic, indexical, and symbolic cues that build a "documentary reality" aligned with judicial expectations. The paper proposes a two-layer evidentiary architecture: origin authenticity (creation-time *hash* registration and fragile digital watermarking by issuing institutions) and algorithmic forensics, multimodal and explainable, for *ex post* assessment. Procedurally, it recommends a dedicated synthetic falsity incident, dynamic allocation of the burden of proof (CPC art. 429) when plausible suspicion arises, recognition of a lost chance of proof where files lack an auditable trail, and standardization of formats and metadata in e-court systems, coupled with verification protocols and continuous training. The conclusion calls for a proactive paradigm in which the appearance of authenticity yields to technically demonstrable authenticity, thereby restoring digital evidence as a reliable trace in adjudication.

**KEYWORDS:** Documentary deepfakes; Digital evidence; Document authenticity; Generative artificial intelligence; Law of evidence.

## INTRODUÇÃO – A NOVA FRONTEIRA DA FALSIDADE PROBATÓRIA

A integridade do sistema de justiça repousa sobre um pilar fundamental: a confiabilidade da prova. É por meio da análise de documentos, testemunhos e perícias que o Estado-juiz busca reconstruir a verdade dos fatos para, então, aplicar o direito. Contudo, o advento da inteligência artificial (IA) generativa inaugura uma crise existencial no direito probatório, deslocando a falsificação do campo da adulteração artesanal para a esfera da produção sintética em massa.

A tecnologia *deepfake*, definida como a manipulação ou síntese de mídias por meio de IA, representa a vanguarda dessa nova fronteira da falsidade. O termo, uma fusão de *deep learning* e *fake*, aponta para a capacidade de redes neurais profundas de criar imitações quase

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

perfeitas da realidade.[139] Não por acaso, estudiosos do processo penal já enfatizavam a importância da autenticidade e da veracidade das provas muito antes dessa tecnologia – sem provas confiáveis, não há processo penal válido, o que evidencia a gravidade do desafio atual.[140]

Enquanto o debate público e a preocupação legislativa se concentraram predominantemente em deepfakes de vídeos e áudios, geralmente associados à desinformação política ou a ataques à honra, uma ameaça mais insidiosa e subestimada emergiu nos bastidores: o deepfake documental. Trata-se da capacidade de gerar, a partir do zero, documentos sintéticos (faturas, contratos, extratos bancários, laudos periciais, comunicações oficiais etc.) visualmente indistinguíveis de documentos autênticos. Essa possibilidade inédita representa um desafio de magnitude sem precedentes à integridade dos processos.

Importa frisar que não se trata de uma ameaça meramente teórica ou futura; ela já é real e atual. No setor financeiro, análogo direto do ambiente probatório judicial pela dependência de documentos, registram-se perdas massivas decorrentes de fraudes documentais baseadas em IA. Estimativas indicam que golpes alimentados por IA generativa poderão causar US$ 40 bilhões em danos apenas nos Estados Unidos até 2027, em um crescimento exponencial que evidencia a escala e sofisticação dos ataques.[141]

A relevância dessa discussão transcende o interesse acadêmico, pois atinge o cerne da função jurisdicional. Como adverte Carrão, os sistemas de IA, por sua autonomia e capacidade de aprendizado e de ação, geram riscos significativos aos direitos fundamentais, especialmente no contexto da justiça criminal.[142] Quando a prova, alicerce sobre o qual se constroem acusações e defesas, pode ser *fabricada* com perfeição digital, os paradigmas atuais de verificação, baseados na presunção de autenticidade e na análise visual, tornam-se não apenas obsoletos, mas também perigosamente ingênuos.

O problema se agrava porque a ameaça já não reside na simples falsificação de um documento pré-existente, mas na criação de uma realidade documental inteiramente nova e plausível. A questão jurídica desloca-se de indagações como “Este

[139] BLOCK, Matthias. *Deepfakes und Recht: Einführung in den deutschen Rechtsrahmen für synthetische Medien*. Wiesbaden: Springer, 2023, p. 5–6.

[140] ALBERGARIA, Pedro Soares et al. *Comentário Judiciário do Código de Processo Penal*, t. II. Coimbra: Almedina, 2019, n.p.; VALENTE, Manuel Monteiro Guedes. *Processo Penal*, tomo I, 4. ed. Coimbra: Almedina, 2020, n.p.

[141] KENNEY, Andrew. “How CPAs can combat the rising threat of deepfake fraud.” *Journal of Accountancy*, 2025, n.p.; OPIAH, Abigail. “Deepfake financial fraud to surge over the next 12 months, Deloitte reveals.” *Biometric Update*, 19 set. 2024, n.p.

[142] CARRÃO, Maria do Céu Cunha. *Artificial Intelligence in Criminal Proceedings: The admissibility of AI-generated evidence*. Dissertação (Mestrado) — Nova School of Law, 2022, p. 1–5

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

documento foi alterado?" para uma muito mais complexa e desestabilizadora: "O evento representado por este documento – apesar da aparência perfeitamente autêntica, realmente aconteceu?". Essa mudança fundamental mostra que a crise instaurada pelos deepfakes não é apenas pericial, mas também epistemológica, afetando a própria capacidade do julgador de reconstruir, com fidelidade, a verdade dos fatos.

Diante desse cenário, o presente artigo propõe-se a analisar como os deepfakes documentais constituem uma ameaça real e crescente ao sistema de justiça brasileiro, comprometendo princípios processuais essenciais como a busca pela verdade material, o direito de defesa e o contraditório. A abordagem adotada é interdisciplinar, combinando os aspectos técnicos da IA generativa, as vulnerabilidades do ordenamento jurídico-processual pátrio e as contramedidas tecnológicas e jurídicas disponíveis. Busca-se demonstrar que a preservação da busca pela verdade e pela justiça na era digital exige uma resposta coordenada e urgente dos operadores do direito. Estudos internacionais já destacam as implicações das tecnologias digitais avançadas no âmbito criminal, reforçando que apenas uma atuação imediata e multidisciplinar será capaz de resguardar a integridade do processo na era da prova sintética.

## 1. A ANATOMIA DA AMEAÇA: TECNOLOGIA, TÁTICAS E A MATERIALIZAÇÃO DO RISCO

Para compreender a profundidade do desafio imposto pelos deepfakes documentais, é preciso articular três camadas: (i) a mecânica técnica de geração; (ii) as táticas de ataque já testadas em fraudes reais de alto impacto; e (iii) os mecanismos psicocognitivos que tornam tais falsificações altamente persuasivas. A ameaça é sociotécnica: combina sofisticação computacional, exploração de vulnerabilidades humanas e democratização de ferramentas de fraude.

### 1.1 A MECÂNICA DA FALSIFICAÇÃO: DE GANS A MODELOS AUTOREGRESSIVOS

Em essência, deepfakes utilizam modelos de aprendizado de máquina para sintetizar conteúdo. O paradigma clássico é o das Redes Adversariais Generativas (GANs): um gerador cria amostras falsas e um discriminador procura distingui-las das reais; o ciclo competitivo se repete até que o gerador atinja um grau de realismo que leve o discriminador a falhar com frequência.[143] Embora inicialmente associadas à manipulação de áudio e vídeo, essas técnicas migraram para todo tipo de mídia digital, inclusive para documentos, com replicação fidedigna

[143] BLOCK, Matthias. *Deepfakes und Recht*... Wiesbaden: Springer, 2023, p. 13–14.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

de layout, fontes, marcas e convenções gráficas.[144]

Paralelamente, difundiram-se modelos autorregressivos aplicados à imagem, capazes de gerar conteúdo pixel a pixel. Essa abordagem permite controlar nuances como textura de papel, padrão de iluminação e microimperfeições típicas de um documento escaneado, isto é, sua "materialidade percebida"; nessa chave, a análise visual humana tende a perder eficácia, sobretudo quando não acompanhada de verificação técnica.[145] Ao mesmo tempo, o custo de insumo desabou: hoje, segundos de áudio bastam para clones de voz convincentes, ampliando o vetor de ataque multimodal e barateando a operação criminosa.[146] Em consequência, produzir documentos falsos com qualidade "profissional" deixou de ser prerrogativa de Estados ou grandes organizações e passou a estar ao alcance de litigantes individuais mal-intencionados, com ferramentas acessíveis e instruções públicas.

## 1.2 CASOS GLOBAIS E ESCALA DO RISCO: A FRAUDE CORPORATIVA COMO PRECURSORA DA FRAUDE PROCESSUAL

Os principais incidentes corporativos de 2023–2025 servem como provas de conceito do que pode ingressar, sem fricção, no contencioso judicial. Em janeiro de 2024, um funcionário da Arup, em Hong Kong, foi induzido a transferir US$ 25,6 milhões após uma videoconferência com supostos executivos, na realidade, avatares deepfake articulados a e-mails de phishing e a clonagem de voz em tempo real; tratou-se de um ataque multimodal, desenhado para explorar relações de confiança hierárquicas.[147] Outras ocorrências revelam personalização cirúrgica: tentativas de se passar pelo CEO da Ferrari, Benedetto Vigna, e pelo CEO do grupo WPP, Mark Read, por meio de combinações de *voice cloning* e imagens públicas.[148]

A escala do problema é alarmante: entre 2022 e 2023, as fraudes com deepfake na América do Norte cresceram 1.740%, e mais de um quarto dos executivos reportou ao menos um ataque no último ano.[149] Em dimensão diretamente relacionada à prova documental, análises de *due diligence* indicam que cerca de 17% dos extratos bancários digitais submetidos a pedidos de empréstimo estavam adulterados, o que sinaliza a

[144] BLOCK, Matthias. *Deepfakes und Recht*... 2023, p. 35–36.
[145] BURKE, Ronan. "This receipt was made by AI. Can you tell?" *Inscribe Blog*, 2025, n.p.
[146] KENNEY, Andrew. "How CPAs can combat the rising threat of deepfake fraud." *Journal of Accountancy*, 2025, n.p.
[147] INCODE. "Top 5 Cases of AI Deepfake Fraud from 2024 Exposed." 2024, n.p.
[148] INCODE. "Top 5 Cases...", 2024, n.p.
[149] COLMAN, Ben. "Why detecting dangerous AI is key to keeping trust alive." *World Economic Forum*, 2025, n.p.; SUMSUB. "Deepfake fraud worldwide increased by more than 10 times from 2022 to 2023." *Security.org*, 2024, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

disseminação de manipulação documental de alto nível.[150]

O ambiente corporativo, impulsionado por fortes incentivos financeiros, acelera o refinamento dessas táticas; o mesmo arranjo tecnológico, apto a liberar US$ 25 milhões, pode fabricar um contrato, um recibo ou uma cadeia de e-mails probatórios com a mesma eficiência, transbordando para processos cíveis e penais.

## 1.3. DA QUANTIDADE À QUALIDADE: SALTO TÉCNICO E APLICAÇÕES JURÍDICAS

O salto atual não é apenas quantitativo (produção mais rápida e barata), mas também qualitativo. Sai-se do terreno da "adulteração" de um original para a falsidade originária: documentos que nascem digitais, "perfeitos" e plausíveis. A literatura especializada alerta que, em breve, será extremamente difícil distinguir materiais genuínos de falsificações, inclusive para peritos experientes.[151] Some-se a isso a corrida armamentista entre geradores e detectores: aperfeiçoamentos em modelos de detecção retroalimentam técnicas de evasão e reduzem a acurácia "fora de laboratório", em condições reais.[152]

À medida que a próxima geração de modelos elimina "erros de principiante", deslizes tipográficos, incoerências de formatação, sombras e *kerning* atípicos, a inspeção meramente visual tende a se tornar inócua, exigindo validação técnica e trilhas de proveniência desde a origem.[153] As aplicações maliciosas desse salto qualitativo já são conhecidas e têm impacto direto no processo. A construção de identidades sintéticas completas — passaportes, documentos de identidade, históricos financeiros e ocupacionais — tem sido utilizada para burlar rotinas de *KYC* e *background checks*, criando perfis sólidos o suficientes para enganar bancos, *fintechs* e autoridades.[154]

A fabricação de evidências processuais — contratos, recibos, faturas, cadeias de e-mails — pode vir acompanhada de metadados "plausíveis" e trilhas falsas de transmissão, exigindo do oponente processual um ônus probatório diabólico para infirmá-las.[155] Há ainda a manipulação de registros médicos,

---

[150] U.S. DEPARTMENT OF HOMELAND SECURITY. *Impact of Artificial Intelligence on Criminal and Illicit Activities*, 2024, p. 23.

[151] SHERMAN, A. "A Feast of Fraud: How International Hesitations to Regulate Deepfakes Are Creating a Buffet for Financial Crime." *Journal of Financial Crime*, 2025, p. 95–96.

[152] MASOOD, M.; NAWAZ, M. "Deepfakes generation and detection: open challenges and way forward." *Applied Intelligence*, 2023, passim; TURNER, L.; BEYK, S. "A systematic literature review of deepfake detection." *Journal of Cyber Security Technology*, 2023, passim; ZHANG, Y. "A survey on deepfake techniques: generation, detection and applications." *Multimedia Tools and Applications*, 2022, passim.

[153] BURKE, Ronan. "This receipt was made by AI...", 2025, n.p.

[154] U.S. DEPARTMENT OF HOMELAND SECURITY. *Impact of AI on Criminal and Illicit Activities*, 2024, n.p.

[155] RESISTANT.AI. "Document Fraud Analysis" In: U.S. DHS. *Impact of AI on Criminal and Illicit Activities*, 2024, p. 23.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

com adição ou remoção de achados em tomografias e ressonâncias, o que desloca o problema para o coração da perícia e da valoração probatória.[156]

Em seguros e saúde, fotografias e vídeos "perfeitos demais" alimentam pedidos e defesas com aparência de autenticidade irretocável, mas lastreadas em síntese algorítmica.[157] Nesse quadro, um sistema de justiça que permaneça ancorado em presunções de autenticidade e em inspeções oculares reage tarde e mal: a resposta adequada requer protocolos de autenticidade na origem e uma gramática pericial compatível com o estado da arte tecnológica — temas que serão desenvolvidos nos capítulos seguintes.

## 2. O ORDENAMENTO JURÍDICO BRASILEIRO SOB TENSÃO: VULNERABILIDADES SISTÊMICAS

A introdução de provas sintéticas no ecossistema jurídico brasileiro não encontra um sistema resiliente, mas um conjunto de doutrinas, jurisprudência e regras processuais forjado em era pré-IA, com forte confiança na materialidade do documento e em rotinas de verificação que pressupõem a existência de "vestígios tradicionais" de adulteração. Esse desenho mostra-se insuficiente para enfrentar a falsidade originária típica dos deepfakes documentais, isto é, artefatos que já nascem digitalmente perfeitos e plausíveis.

### 2.1 PROVA DIGITAL NA JURISPRUDÊNCIA DO STJ: O LIMITE DA CADEIA DE CUSTÓDIA

Nos últimos anos, o Superior Tribunal de Justiça (STJ) consolidou diretrizes relevantes sobre admissibilidade de prova digital, com ênfase na cadeia de custódia e na rejeição de *prints* extraídos sem metodologia forense adequada.[158] A orientação de que capturas de tela de aplicativos, como o WhatsApp, são insuficientes quando desacompanhadas de procedimentos que assegurem idoneidade, integridade e rastreabilidade significou um avanço contra manipulações *ex post*.[159]

Todavia, essa resposta, voltada a preservar a coleta e a custódia, não enfrenta o núcleo do problema dos deepfakes: a origem. Se um contrato em PDF, um recibo em imagem ou um extrato bancário for gerado por IA e inserido no fluxo comunicacional antes de qualquer intervenção estatal, todo protocolo de extração, *de hashing e de* documentação preservará, com rigor, a integridade de uma fabricação.[160]

---

[156] SHERMAN, A. "A Feast of Fraud...", 2025, p. 95–96

[157] COLMAN, Ben. *WEF*, 2025, n.p.; INCODE. "Top 5 Cases...", 2024, n.p.

[158] BARCHI, G. "STJ: provas digitais e a importância da metodologia adequada na extração de dados." MFBD Advogados, 2024, n.p.; LOPES, V. H. "STJ inviabiliza uso de prints de WhatsApp como meio de prova..." Migalhas, 2024, n.p.; STJ. "Quinta Turma não aceita como provas prints de celular extraídos sem metodologia adequada." 2024, n.p.

[159] STJ. "Quinta Turma não aceita como provas prints..." 2024, n.p.

[160] STJ. "Quinta Turma não aceita como provas prints..." 2024, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

A jurisprudência atual, centrada na "falsidade procedimental" (vícios na extração e no manuseio), carece de instrumentos para a "falsidade originária" (conteúdo nativo sintético). A fragilidade aumenta quando se admite, corretamente, para fins de desburocratização, a validade de assinaturas eletrônicas fora do ICP-Brasil, sem exigir contrapartidas técnicas mínimas de autenticação e de trilha de auditoria, o que amplia a superfície de ataque se não vier acompanhada de verificações mais robustas.[161] O resultado é um paradoxo probatório: protege-se o percurso do arquivo, mas, de partida, não se questiona o que esse arquivo é.

A insuficiência dos métodos tradicionais de autenticação manifesta-se, ao menos, em três frentes interligadas. Em primeiro lugar, a presunção de autenticidade que acompanha documentos oficiais ou financeiros converte-se em vulnerabilidade explorável: faturas e contratos são recebidos como verdadeiros até prova em contrário, invertendo, na prática, o ceticismo necessário em ambiente de síntese algorítmica. Em segundo lugar, a própria cadeia de custódia digital perde sua função heurística quando qualquer etapa anterior à coleta pode ter sido contaminada por IA; não basta provar que nada se alterou *depois* se o arquivo já era falso *desde sempre*. Em terceiro lugar, o princípio da imediação resta esvaziado: a percepção direta do julgador sobre um documento "perfeito demais" não oferece um antídoto cognitivo suficiente contra a verossimilhança sintética, exigindo protocolos técnicos que ultrapassem a inspeção ocular.[162]

## 2.2 O COLAPSO DE PRINCÍPIOS PROCESSUAIS FUNDAMENTAIS

A entrada de provas sintéticas desencadeia um efeito dominó nos pilares do processo. A começar pela busca da verdade material: se a prova, que deveria funcionar como vestígio do passado, pode ser construída no presente com aparência de passado, a própria reconstrução histórica dos fatos se fragiliza.[163] A consequência é sistêmica: mais do que dificultar, *deepfakes* podem inviabilizar a verdade processual, deslocando o debate para narrativas ficcionais, com potencial para gerar decisões baseadas em eventos inexistentes.

A paridade de armas também se rompe. Quem apresenta um documento sintético de alta qualidade impõe ao adversário o ônus probatório

[161] CLICKSIGN. "STJ reafirma os entendimentos acerca da validade jurídica das assinaturas eletrônicas." 2024, n.p.; MIGALHAS. "STJ valida assinatura eletrônica fora do sistema ICP-Brasil." 2024, n.p.; STJ. REsp 2.159.442/PR, 2024, n.p.; TJDFT. Acórdão 1750473, 2023, n.p.

[162] RAMALHO, D. S. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017, p. 258.

[163] SILVEIRA, S. S.; SILVEIRA, R. R. "A prova eletrônica no processo penal." *Rev. Fac. Dir. UFG*, 2015, passim; FONTENELE LEMOS, D.; HOMSI CAVALCANTE, L.; GONÇALVES MOTA, R. "A prova digital no processo..." *Rev. Acad. ESMP-CE*, 2021, passim.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

diabólico de provar o negativo, a inexistência do que parece impecavelmente autêntico, pressionando recursos periciais caros e escassos.[164] Forma-se, assim, uma assimetria processual na qual a tecnologia atua como arma de desequilíbrio, favorecendo quem pode produzir a síntese (ou arcar com sua detecção).

Por fim, dissemina-se o "dividendo do mentiroso" (*liar's dividend*): a consciência pública sobre *deepfakes* permite que litigantes de má-fé desacreditem provas autênticas com um simples rótulo de falsidade, mesmo sem base técnica.[165] O dano aqui é difuso: a corrosão da confiança epistêmica no acervo probatório pode paralisar a decisão ou conduzi-la pela via da dúvida sistemática, inclusive contra material genuíno. A literatura técnica, ademais, indica que distinguir materiais genuínos de falsificações tende a tornar-se extremamente difícil, inclusive para peritos, o que agrava o ceticismo generalizado.[166]

### 2.2.1 Verdade material

O processo penal brasileiro assenta-se na reconstrução fiel dos fatos. Se documentos podem ser gerados com perfeição fotorrealista, a coluna mestra da verdade material sofre abalo direto: a prova deixa de ser "rastro" e passa a ser "projeto", com impacto na legitimidade de qualquer conclusão fática.[167]

### 2.2.2 Direito de defesa e contraditório

O direito de impugnar evidências pressupõe condições materiais para o exercício. Em ambiente de síntese algorítmica, a defesa frequentemente não dispõe de meios técnicos para demonstrar a falsidade de um documento "perfeito", sobretudo quando a trilha de auditoria é inexistente ou deficiente. A paridade de armas, corolário do contraditório, fica comprometida de forma qualitativa.[168]

### 2.2.3 Confiança no sistema de justiça

A confiança social na adjudicação é capital institucional. Com deepfakes, torna-se plausível impugnar tudo e provar quase nada: a retórica da dúvida ganha força enquanto os métodos de autenticação não acompanham o estado da arte tecnológico.[169] A resposta há de ser estrutural, sob pena de erosão

[164] LOPES JÚNIOR, A. *Direito Processual Penal*, 18. ed., São Paulo: Saraiva, 2021, n.p.
[165] SCHIFF, K. J.; SCHIFF, D. S.; BUENO, N. S. "The Liar's Dividend...", 2022, passim.
[166] SHERMAN, A. "A Feast of Fraud...", 2025, p. 95–96.
[167] FIGUEIREDO DIAS, J. *Direito Processual Penal*, v. I, Coimbra: Coimbra Editora, 1974, n.p.; LOPES JÚNIOR, A. *Direito Processual Penal*, 2021, n.p
[168] GOMES FILHO, A. M. *Direito à prova no processo penal*. São Paulo: RT, 1997, n.p.; PRADO, G. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2014, n.p.; SILVEIRA; SILVEIRA, 2015, passim.
[169] SCHIFF; SCHIFF; BUENO, 2022, passim; SHERMAN, 2025, p. 95–96.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

generalizada da autoridade das decisões.

## 2.3 ÔNUS PROBATÓRIO EM XEQUE: ART. 429 DO CPC E A NECESSIDADE DE INVERSÃO DINÂMICA

O art. 429 do CPC disciplina a distribuição do ônus em hipóteses de arguição de falsidade documental (inc. I) e de impugnação da autenticidade (inc. II), atribuindo, respectivamente, a quem alega a falsidade o dever de prová-la e, a quem produziu o documento, o dever de provar sua autenticidade.[170] Esse desenho, concebido para o universo físico (ou para cópias cuja fidelidade possa ser cotejada), não captura a natureza dos documentos nativamente digitais e sintéticos. Em tais casos, impor à parte impugnante o encargo de demonstrar que um arquivo "perfeito" é uma criação algorítmica equivale a institucionalizar a assimetria.

Mostra-se, pois, adequado recorrer à distribuição dinâmica do ônus da prova: uma vez suscitada suspeita plausível de síntese (com elementos mínimos), o encargo de comprovar a autenticidade e a proveniência — *inclusive* por meio de trilha de auditoria técnica (arquivos nativos, metadados íntegros, cadeia de transmissão, registros) — deve recair sobre quem juntou o documento aos autos, por ser quem melhor pode produzi-lo. A lógica encontra paralelo na tese firmada no Tema Repetitivo 1.061, que impõe às instituições financeiras o ônus de comprovar a autenticidade de assinaturas impugnadas, dada sua posição técnica privilegiada.[171]

## 2.4 A "PERDA DE UMA CHANCE PROBATÓRIA" COMO ESTRATÉGIA DEFENSIVA

Outra via dogmática útil é a perda de uma chance probatória. Transposta da responsabilidade civil para o processo, a tese reconhece que a conduta da parte pode suprimir a possibilidade real de a contraparte produzir contraprova essencial.[172] Se, na era da prova sintética, alguém apresenta um arquivo digital desprovido de trilha verificável de origem e integridade — por exemplo, sem arquivo nativo, sem metadados preservados, sem registro técnico (marca d'água, *hash* depositado, *logs* de transmissão) —, cria-se um déficit de auditabilidade que impede a defesa de reconstruir a gênese do documento.

Nessa hipótese, está-se diante de falha de diligência probatória, cuja consequência pode ir da inutilização da prova à valoração severamente desfavorável a quem a produziu, com impacto, a depender do conjunto probatório, até mesmo na absolvição

[170] BRASIL. Lei 13.105/2015 (CPC), art. 429, n.p.; SILVA, J. A. R. O. "A prova digital...", *Rev. TST*, v. 88(2), 2022, n.p.

[171] STJ. Tema Repetitivo 1.061 (Notícia STJ, 04 fev. 2022), n.p.

[172] LOPES, A. B.; TATSUO, E. P. "Teoria da perda da chance probatória." *Boletim IBCCRIM*, 2022, n.p.; STJ. Tema 1.061, 2022, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

por insuficiência de elementos confiáveis.

Em síntese, o arcabouço atual — útil contra adulterações tardias — não basta para enfrentar a falsidade originária. A adaptação do sistema requer, simultaneamente, (i) recalibrar as presunções sobre documentos digitais, (ii) redistribuir dinamicamente o ônus quando houver uma *plausible claim* de síntese e (iii) exigir trilhas técnicas de proveniência compatíveis com o estado da arte, sob pena de inutilidade epistêmica da prova em juízo.[173]

## 3. CONSTRUINDO A RESILIÊNCIA PROBATÓRIA: CONTRAMEDIDAS TECNOLÓGICAS E FORENSES

A batalha contra a prova sintética não se resolve apenas com dogmática processual; ela se decide, em grande medida, na arena tecnológica. A resposta adequada exige uma abordagem multifacetada, que articule medidas reativas de detecção com mecanismos proativos de autenticidade na origem, de modo que o sistema não fique condenado a "correr atrás" do falsificador, mas estabeleça, desde a criação do documento, condições objetivas de verificabilidade.

### 3.1 A DETECÇÃO POR IA: ANÁLISE FORENSE DE ARTEFATOS, METADADOS E INCONSISTÊNCIAS

Paradoxalmente, a mesma IA que possibilita *deepfakes* é hoje a principal ferramenta para identificá-los. A perícia digital emprega modelos de aprendizado de máquina para captar "impressões digitais" de síntese — inconsistências de iluminação, sombras e bordas, ruído de pixels não naturais, padrões de artefatos de compressão — que escapam à inspeção humana.[174] Em vídeos, algoritmos detectam anomalias fisiológicas sutis (como o piscar, a microdinâmica facial e variações pulsáteis na coloração da pele), enquanto a análise de metadados revela softwares de edição, *timestamps* improváveis e a ausência de dados esperados de captura.[175]

Apesar dos avanços, a detecção enfrenta dois obstáculos estruturais. O primeiro é a corrida armamentista: cada ganho do detector retroalimenta o treinamento de geradores para contornar assinaturas conhecidas, tornando o alvo mais móvel.[176] O segundo é a generalização: modelos que performam bem em *benchmarks* controlados perdem acurácia no "mundo selvagem", após recompressões, redimensionamentos e transcodificações típicas de arquivos

[173] ROSA, A. M. *Guia do processo penal conforme a teoria dos jogos*. Florianópolis: Empório do Direito, 2017, n.p.; KELLNER, C. "The End of Reality? How to combat deepfakes...", *ABA Journal*, 10 mar. 2025, n.p.

[174] BURKE, Ronan. "This receipt was made by AI. Can you tell?" *Inscribe Blog*, 2025, n.p.

[175] NGUYEN, T. D. et al. "Forensic Self-Descriptions Are All You Need for Zero-Shot Detection...", *arXiv*, 2025, n.p.

[176] MASOOD, M.; NAWAZ, M. "Deepfakes generation and detection: open challenges and way forward." *Applied Intelligence*, 2023, passim.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

que circulam na internet ou em aplicativos.[177]

Por isso, a pesquisa recente avança para detectores multimodais e explicáveis, capazes não só de classificar, mas também de explicar por que algo foi marcado como sintético, o que aumenta a auditabilidade judicial do laudo.[178]

Em termos processuais, o ponto é claro: a checagem visual e os ritos de documentação da coleta são insuficientes; é indispensável incorporar rotinas periciais algorítmicas que deem lastro técnico à valoração probatória.[179]

## 3.2 IMUTABILIDADE COMO GARANTIA: BLOCKCHAIN APLICADO À AUTENTICIDADE DOCUMENTAL

Para além da detecção *ex post*, é decisivo estabelecer a origem dos documentos. A tecnologia blockchain oferece uma trilha de auditoria imutável e distribuída: na criação do arquivo relevante (por exemplo, assinatura eletrônica de contrato ou emissão de laudo), gera-se um *hash*[180] criptográfico (como SHA-256) e registra-se essa "impressão digital" em rede pública ou permissionada, com *timestamp*.[181] No futuro, a verificação reproduz o algoritmo: se o *hash* do arquivo apresentado coincide com o registrado, preserva-se a integridade; se diverge, há evidência objetiva de alteração.

Não se trata de elucubração acadêmica: cadeias de suprimentos já se ancoram em blockchains para conformidade regulatória (Renault), rastreabilidade ética de insumos críticos (Ford/cobalto) e segurança alimentar (Walmart), demonstrando viabilidade operacional em larga escala.[182] No setor público, a Estônia estruturou a identidade digital e os serviços estatais com base descentralizada, ilustrando que infraestruturas de confiança podem ser políticas de Estado.[183] Transposta ao campo probatório, a mesma lógica evita que o Judiciário dependa exclusivamente de detecção reativa: documentos nascem verificáveis.

## 3.3 A ASSINATURA OCULTA: MARCAS D'ÁGUA DIGITAIS E VERIFICAÇÃO DE INTEGRIDADE

[177] TURNER, L.; BEYK, S. "A systematic literature review of deepfake detection." *Journal of Cyber Security Technology*, 2023, passim; ZHANG, Y. "A survey on deepfake techniques: generation, detection and applications." *Multimedia Tools and Applications*, 2022, passim.

[178] GOYAL, H. et al. "State-of-the-art AI-based Learning Approaches for Deepfake Generation and Detection...", *arXiv*, 2025, n.p.; NGUYEN, T. D. et al., 2025, n.p.

[179] NGUYEN, T. D. et al., 2025, n.p.

[180] *Hash* criptográfico: Função matemática que converte uma entrada de dados de tamanho variável em uma saída de tamanho fixo. Qualquer alteração na entrada resulta em um *hash* completamente diferente, garantindo a integridade dos dados.

[181] AIMULTIPLE. "27 Real-World Blockchain Case Studies & Applications in 2025." 2025, n.p.

[182] ULAM. "Blockchain Analysis in Action: Real-Life Use Cases and Insights." 2024, n.p.

[183] MOLDSTUD. "Blockchain for Digital Identity: Real-World Case Studies and Practical Applications." 2025, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

Outro pilar é a marca d'água digital. Para fins probatórios, interessam especialmente as frágeis: sinais embutidos de maneira imperceptível que se quebram com mínimas alterações do arquivo. Se instituições emissoras — bancos, cartórios, repartições — adotam marcas frágeis em extratos, certidões e ofícios, a verificação posterior reduz-se a aferir a integridade do selo: íntegro, documento autêntico; corrompido ou ausente, indício forte de adulteração.[184]

A literatura técnica já descreve aplicações específicas, inclusive para PDFs com *fragile watermarking* voltado à detecção de microedições,[185] e métodos modernos para imagens e documentos que alinham robustez prática e sensibilidade forense.[186] Em termos de política judiciária, o deslocamento de uma cultura de "detectar o falso" para "exigir autenticidade verificável" — por meio de marcas d'água e registros de *hash* — recalibra as presunções: não basta parecer autêntico; é preciso comprovar a linhagem técnica do arquivo.

## 3.4 O CONTEXTO BRASILEIRO: VULNERABILIDADES E LIMITES PERICIAIS

No Brasil, a alta dependência de documentos digitalizados no PJe e em rotinas administrativas, a escassez de especialistas em forense de IA e a presunção cultural de boa-fé em relação a documentos apresentados por advogados formam um terreno fértil para a inserção de artefatos sintéticos.

A perícia adequada é multimodal: coteja o conteúdo, os metadados, o percurso comunicacional e os sinais algorítmicos residuais.[187] Contudo, a infraestrutura disponível é heterogênea; faltam protocolos padronizados e acesso mais disseminado a ferramentas de ponta.[188] No setor privado e nos quadros oficiais, relatos indicam déficit de capacidade e custos elevados para análises complexas, o que agrava a assimetria entre quem produz a síntese e quem precisa infirmá-la.[189]

Em termos de desenho institucional, isso impõe um dever de diligência: a parte que pretende sustentar sua tese em arquivos digitais

[184] IJERT. "A Survey on Digital Watermarking for Image Authentication." *International Journal of Engineering Research and Technology*, v. 2, n. 11, 2013, n.p.; KHAN, A. et al. "A Digital Image Watermarking Application for Authentication of Official Documents." *Electronics*, v. 10, n. 14, 2021, p. 1744.

[185] LI, S.; ZHANG, X. "A new method for authenticating PDF documents based on fragile watermarking." In: *IIH-MSP 2006*, Pasadena, 2006, p. 351–354.

[186] ZEAR, A. et al. "A proposed method for digital image watermarking." *Journal of Physics: Conference Series*, v. 1530, 2020, 012048.

[187] CYBEREXPERTS. "Investigação Forense e Perícia Digital em Deep Fakes...", 2024, n.p.

[188] PIGÃO, L. "Deepfakes em provas judiciais: estamos prontos...", GSGA, 2024, n.p.

[189] REIS, Advocacia. "Golpes com Deepfake: Responsabilidade Civil e Indenização." 2024, n.p.; ROITMAN, M. "Deepfakes em provas judiciais: estamos preparados...", LexLegal, 2024, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

deve antecipar a auditabilidade, apresentar arquivo nativo, metadados preservados, logs de cadeia de transmissão e, sempre que possível, *hash* previamente ancorado ou marca d'água verificável. Sem esses elementos mínimos, a prova corre o risco de se tornar, do ponto de vista judicial, epistemicamente inútil.

Em síntese, a detecção reativa é necessária, mas insuficiente sem autenticidade na origem. Blockchain para imutabilidade, *watermarking* para integridade e perícia algorítmica explicável para valoração formam, em conjunto, um tripé capaz de reequilibrar o jogo probatório em face da falsidade originária.[190] Esse é o patamar mínimo para que a prova digital volte a desempenhar sua função de vestígio confiável no processo.

## 4. ANÁLISE SEMIÓTICA E RESPOSTA REGULATÓRIA: A MECÂNICA DA PERSUASÃO FALSIFICADA E O NOVO PARADIGMA NORMATIVO

### 4.1 A SEMIÓTICA DE PEIRCE APLICADA AOS DEEPFAKES DOCUMENTAIS

Para explicar por que deepfakes documentais exercem um poder persuasivo tão elevado no foro, adotamos a semiótica de Charles S. Peirce. Todo signo opera na relação entre *representamen* (a forma sensível do signo), objeto (o fato representado) e interpretante (o efeito de sentido produzido no destinatário).[191] Em documentos sintéticos, o *representamen* é deliberadamente lapidado para produzir um interpretante de autenticidade a respeito de um objeto inexistente.

Esse efeito decorre da convergência de três regimes de significação:[192]

- **Iconicidade (semelhança)**: o arquivo "tem cara de documento", com layout verossímil, tipografia compatível, fórmulas e jargões padronizados, padrões de paginação e de organização visual típicos de contratos, laudos e comunicações oficiais.
- **Indexicalidade (traços de origem)**: sinais que parecem apontar para um evento real de emissão/assinatura, como carimbos, rubricas, numeração, *timestamps*, metadados "plausíveis", "ruído" de scanner e microimperfeições que encenam um histórico de vida do arquivo.
- **Simbolicidade (convenções)**: logotipos, brasões, códigos, expressões rituais de abertura/fecho e demais marcas normativas que comunicam pertencimento institucional e validade jurídica.

[190] IJERT, 2013, n.p.; KHAN et al., 2021, p. 1744.
[191] PEIRCE, C. S. *Collected Papers*. Cambridge: Harvard University Press, 1931–1958, passim.
[192] Os três regimes de significação — ícone, índice e símbolo — foram propostos por Charles S. Peirce. Ver a formulação clássica em Peirce, *Collected Papers*, CP 2.247–2.249; 2.274–2.279; 2.291–2.307.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

Quando esses três registros são simulados de modo coordenado, forma-se uma "realidade documental" coerente com as expectativas cognitivas do julgador, fazendo com que a aparência de autenticidade suplante o exame meramente ocular. Nesse cenário, a inspeção visual e as presunções tradicionais deixam de ser filtros adequados: a verificabilidade técnica da procedência (arquivos nativos, metadados íntegros, trilhas de transmissão, selos frágeis, *hash* ancorado) e a perícia algorítmica explicável tornam-se requisitos centrais para a valoração.

## 4.2 A EXPLORAÇÃO DAS CONVENÇÕES DOCUMENTAIS E A CONSTRUÇÃO DE UMA "REALIDADE SINTÉTICA"

A eficácia dos *deepfakes* documentais decorre do aproveitamento estratégico das convenções de redação, diagramação e circulação de papéis oficiais. Elementos simbólicos — brasões, marcas institucionais, rubricas, fórmulas de abertura e fecho — comunicam pertencimento a um universo legítimo; elementos indexicais — dobras, carimbos de tempo, numeração sequencial "plausível", metadados de suposta captura — encenam um histórico de vida do arquivo. Somados à iconicidade do gênero documental (um contrato que "parece" contrato; um laudo que "parece" laudo), esses traços constroem uma realidade documental sintética, perfeitamente alinhada às expectativas cognitivas de magistrados e partes.

O avanço recente de modelos autorregressivos voltados à "materialidade percebida" do arquivo (texturas, iluminação, microimperfeições) reduz ainda mais a utilidade da inspeção ocular como mecanismo de filtragem, fazendo com que o parecer autêntico suplante o ser autêntico.[193]

## 4.3 RESPOSTA REGULATÓRIA: ENTRE LACUNAS NORMATIVAS E DIRETRIZES EMERGENTES

A velocidade da IA generativa ultrapassa o ritmo legislativo. No Brasil, a resposta tem sido fragmentada e predominantemente voltada à desinformação em massa e a crimes contra a honra, com pouca incidência direta sobre a fraude processual documental. O PL 2.338/2023, eixo do futuro marco de IA, propõe classificação de risco, proibições a sistemas de risco excessivo e deveres de transparência e governança para alto risco, mas não estabelece mecanismos processuais específicos para provas sintéticas em juízo.[194]

[193] BURKE, R. "This receipt was made by AI. Can you tell?" *Inscribe Blog*, 2025, n.p.

[194] BRASIL. Projeto de Lei nº 2.338, de 2023 (Marco de IA), 2023, n.p.; CÂMARA DOS DEPUTADOS. "Projeto que regulamenta uso da inteligência artificial no Brasil." 2025, n.p.; DATA PRIVACY BRASIL. "Senado aprova PL que regulamenta IA...", 2024, n.p.; GFT. "Pontos-chaves do projeto de lei sobre uso de IA...", 2024, n.p.; PACHECO, R. "Senado Federal aprova marco regulatório da IA." 2023, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

O PL 2.630/2020 ("Lei das Fake News") dirige-se à viralização de conteúdos em plataformas, o que tem baixa aplicabilidade à inserção, de forma dirigida e sigilosa, de um *deepfake* em autos judiciais.[195] Propostas setoriais — como a tipificação de conteúdos sexuais falsos ou agravantes ligados à violência psicológica por manipulação de imagem — são meritórias, mas estreitas diante do espectro de falsificações financeiras, contratuais e administrativas mobilizáveis em litígios.[196] O quadro legislativo, assim, reconhece o problema, mas ainda não oferece um paradigma probatório para a falsidade originária.

## 4.4 PROPOSTAS LEGISLATIVAS E PROCESSUAIS: DO "DETECTAR O FALSO" AO "EXIGIR AUTENTICIDADE VERIFICÁVEL"

Diante da lacuna, impõe-se uma agenda de reformas que dialogue com a técnica e reequilibre o processo. No plano penal, é defensável a criação de tipo autônomo — ou qualificadora do art. 347 do CP — para condutas de criar, desenvolver ou utilizar prova sintética gerada ou substancialmente alterada por IA com finalidade de induzir a erro juiz ou perito, com agravantes quando praticada por operadores jurídicos ou quando resultar em restrição indevida de liberdade ou perda patrimonial relevante. No plano processual, três eixos são centrais. Primeiro, protocolos de admissibilidade que exijam arquivos nativos com metadados preservados para documentos cruciais (contratos, transações, laudos), bem como prova de procedência técnica quando emitidos por instituições: registro de *hash* em blockchain no momento da criação, ou marca d'água digital frágil verificável como selo de integridade.[197]

Segundo um incidente processual específico de falsidade sintética, com rito abreviado, com prova pericial multimodal e decisão fundamentada em critérios técnicos transparentes. Terceiro, distribuição dinâmica do ônus probatório: uma vez demonstrada a suspeita plausível de síntese, o encargo de provar a autenticidade e a proveniência recai sobre quem juntou o arquivo, em simetria com a racionalidade do Tema 1.061/STJ quanto à autenticidade de assinaturas em contratos bancários.[198] Essas medidas não erguem barreiras indevidas à produção de provas; apenas recalibram presunções para um ambiente em que a aparência de

[195] BRASIL. Projeto de Lei nº 2.630, de 2020 (Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet), 2020, n.p.

[196] BRASIL. PL nº 370, de 2024 (violência psicológica/agravantes), 2024, n.p.; CÂMARA DOS DEPUTADOS. "Câmara aprova projeto que pune divulgação de *deepfake* com conteúdo sexual." 2024, n.p.

[197] LI, S.; ZHANG, X. "A new method for authenticating PDF documents based on fragile watermarking." In: *IIH-MSP 2006*, Pasadena, 2006, p. 351–354; ZEAR, A. et al. "A proposed method for digital image watermarking." *Journal of Physics: Conference Series*, v. 1530, 2020, 012048.

[198] STJ — Superior Tribunal de Justiça. Tema Repetitivo 1.061 (Notícia STJ, 04 fev. 2022), n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

autenticidade deixou de ser garantia de verdade.

## 5. RECOMENDAÇÕES E IMPLICAÇÕES PRÁTICAS PARA OS OPERADORES DO DIREITO

A adaptação à era da prova sintética exige mais do que reformas legislativas; demanda uma mudança de cultura e de competências por parte de todos os atores do sistema de justiça. A análise teórica deve ser traduzida em diretrizes práticas e acionáveis.

### 5.1 PODER JUDICIÁRIO: PROTOCOLOS, CAPACITAÇÃO E DESENHO INSTITUCIONAL

No plano judicial, recomenda-se a elaboração de protocolos de verificação (*bench cards* e guias de perguntas) que orientem a atuação do magistrado diante de alegações de *deepfake*, com roteiros mínimos de: (i) identificação de bandeiras vermelhas; (ii) especificação de prova técnica necessária (arquivos nativos, metadados preservados, cadeia de transmissão, *hash* ancorado em *blockchain* ou marca d'água frágil); e (iii) critérios de nomeação de peritos e delimitação do objeto da perícia.[199] Tais protocolos devem se articular a uma capacitação continuada de magistrados e servidores em forense digital, IA aplicada e limites da inspeção ocular, de modo a mitigar a confiança excessiva em documentos "perfeitos demais".[200]

Em cortes de maior porte, a criação de varas especializadas em crimes digitais e litígios de alta complexidade tecnológica permite concentrar a expertise, estabilizar a jurisprudência e servir de polo de referência às demais unidades. Por fim, convém estabelecer procedimentos de emergência para hipóteses em que o *deepfake* é descoberto após a decisão (preservação imediata de originais, *logs* e metadados; reabertura probatória estrita ao tema; parâmetros para revisão), evitando a erosão da confiança pública decorrente do chamado "dividendo do mentiroso".

### 5.2 ADVOCACIA E MINISTÉRIO PÚBLICO: DILIGÊNCIA PROBATÓRIA E TESES PROCESSUAIS

Para advogados e membros do Ministério Público, impõe-se uma due diligence probatória prévia à juntada de quaisquer arquivos digitais: verificação de origem e plausibilidade, documentação desde a primeira posse (e-mails de recebimento, cabeçalhos completos, *logs*), preservação de arquivos nativos e de metadados. Sempre que possível, recomenda-se exigir ou produzir prova de procedência técnica, *hash* gerado na criação e ancorado em *blockchain*, ou marca

[199] RUNYON, N. "Deepfakes as evidence: How judges can address the challenges of AI-generated content." *Thomson Reuters Institute*, 2025, n.p.

[200] RUNYON, N. *Deepfakes as evidence*... 2025, n.p.; SHERMAN, A. *A Feast of Fraud*... 2025, p. 95–96.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

d'água institucional frágil em extratos, certidões e laudos.[201]

No contencioso, duas frentes merecem protagonismo. A primeira é a distribuição dinâmica do ônus da prova: havendo suspeita plausível de síntese, o encargo de demonstrar a autenticidade e a proveniência deve recair sobre quem juntou o documento, em sintonia com a racionalidade do art. 429 do CPC e o Tema 1.061/STJ.[202] A segunda é a perda de uma chance probatória: a apresentação de prova digital sem trilha de auditoria — sem nativo, sem metadados íntegros, sem registro técnico, configura falha de diligência que pode justificar desde a inutilização do arquivo até a valoração severamente desfavorável ao seu proponente. Essa atuação deve ser acompanhada de parcerias interdisciplinares com peritos em IA e forense digital, sobretudo nas fases iniciais, quando pequenas inconsistências ainda são detectáveis.[203]

## 5.3 INSTITUIÇÕES DE ENSINO JURÍDICO: CURRÍCULO, PRÁTICA E PESQUISA APLICADA

As faculdades de Direito devem incorporar, em núcleo obrigatório, conteúdos de prova digital, segurança da informação e inteligência artificial aplicada ao processo, com oficinas práticas sobre análise de *deepfakes*, leitura de laudos explicáveis e noções de metadados e cadeia de custódia. É crucial fomentar a interdisciplinaridade entre Computação e Engenharia, clínicas tecnológicas, *labs* forenses, *moot courts* com peças e incidentes de falsidade sintética, para formar profissionais com vocabulário técnico mínimo e senso crítico adequado.[204]

Na pesquisa, priorizar soluções replicáveis ao foro brasileiro: *benchmarks* locais de detecção, *toolkits* de verificação para cartórios e repartições, modelos de petições e ordens judiciais para incidentes de falsidade sintética e guias de boas práticas de preservação.

## 5.4 INFRAESTRUTURA TÉCNICA E PADRÕES DE AUTENTICIDADE: DO REATIVO AO PROATIVO

No plano sistêmico, recomenda-se a adoção de um padrão de duas etapas: (i) autenticidade na origem, por registro de *hash* na criação (em *blockchain* pública ou permissionada, com *timestamp*) e/ou marca d'água frágil institucional; e (ii)

[201] LI, S.; ZHANG, X. *Fragile watermarking for PDFs*, 2006, p. 351–354; ZEAR, A. et al. *Digital image watermarking*, 2020, 012048.
[202] BRASIL. CPC, art. 429, 2015, n.p.; STJ — Tema 1.061, 2022, n.p.; SILVA, J. A. R. O. *A prova digital...*, 2022, n.p.
[203] FLORES, L. *Perda de uma chance probatória*, 2023, n.p.; LOPES, A. B.; TATSUO, E. P. *Perda da chance probatória*, 2022, n.p.; ROSA, A. M. *Guia do processo penal...*, 2017, n.p.; KELLNER, C. *The End of Reality?*, 2025, n.p.; RAMALHO, D. S. *Métodos Ocultos...*, 2017, p. 258; CYBEREXPERTS *Investigação forense...*, 2024, n.p.
[204] GLESS, S. *AI in the Courtroom*, 2020, p. 240; CARRÃO, M. C. C. *AI in Criminal Proceedings*, 2022, n.p.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

detecção *ex post*, por perícia algorítmica multimodal e explicável.[205]

É preciso reconhecer limitações: *blockchain* não impede a inserção inicial de um documento falso (apenas prova a imutabilidade desde o registro), ao passo que detectores de IA ainda sofrem com generalização reduzida entre dados de laboratório e cenários "selvagens".[206]

Por isso, a política pública deve estabelecer requisitos mínimos de procedência para documentos críticos no PJe e em serviços administrativos, por exemplo, a exigência de arquivo nativo e metadados íntegros como condição de admissibilidade, e a justificativa técnica quando apenas cópias rasterizadas forem apresentadas, além de formatos preferenciais e manuais operacionais para órgãos emissores.

### 5.5 GOVERNANÇA, CAPACITAÇÃO E TRANSPARÊNCIA PERICIAL

A construção de resiliência sistêmica passa ainda por (i) cadastro público de peritos com experiência em IA e forense digital; (ii) protocolos de escopo pericial que descrevam métodos, *datasets* e limites de inferência; e (iii) transparência das decisões técnicas, em linguagem acessível, com ênfase na explicabilidade dos classificadores. Ao mesmo tempo, convém promover treinamento transversal, magistratura, Ministério Público, advocacia pública e privada, com foco em *red flags* documentais, leitura crítica de metadados, e compreensão da corrida armamentista entre geradores e detectores. Esse arranjo organizacional reduz o espaço para a retórica da dúvida generalizada e reforça a valoração probatória em critérios verificáveis.

Em suma, o eixo das recomendações é recalibrar presunções e redistribuir competências: do parecer autêntico ao ser tecnicamente autêntico; da detecção tardia à proveniência exigível; da perícia ininteligível à explicabilidade auditável. Somente com protocolos judiciais claros, diligência probatória efetiva e uma infraestrutura técnica que una *hash* ancorado e *watermarking* a detectores multimodais será possível restituir à prova digital sua condição de vestígio confiável no processo.[207]

## CONCLUSÃO

[205] LI; ZHANG, 2006, p. 351–354; GOYAL, H. et al. *State-of-the-art*..., 2025, n.p.; NGUYEN, T. D. et al. *Forensic Self-Descriptions*..., 2025, n.p.

[206] MASOOD, M.; NAWAZ, M. *Deepfakes generation and detection*..., 2023, passim; ZHANG, Y. *A survey on deepfake techniques*..., 2022, passim

[207] Vide: RUNYON, 2025, n.p.; SHERMAN, 2025, p. 95–96 (protocolos judiciais, limites da inspeção ocular e "dividendo do mentiroso"); BRASIL, CPC art. 429, 2015, n.p.; STJ, Tema 1.061, 2022, n.p.; SILVA, 2022, n.p.; LOPES & TATSUO, 2022, n.p. (ônus dinâmico e diligência probatória); LI & ZHANG, 2006, p. 351–354; ZEAR et al., 2020, 012048 (marca d'água frágil e verificação de integridade); GOYAL et al., 2025, n.p.; NGUYEN et al., 2025, n.p.; ZHANG, 2022, passim (perícia algorítmica multimodal, explicabilidade e limites de generalização).

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

A ameaça dos deepfakes documentais ao processo judicial já não é hipótese acadêmica, mas realidade operacional, comprovada por fraudes de alto valor e por ataques multimodais que combinam *phishing*, *voice cloning* e avatares de vídeo em tempo real. A mesma engenharia que libera transferências milionárias é capaz de fabricar contratos, recibos e cadeias de e-mails com aparência impecável, prenunciando seu ingresso rotineiro nos autos brasileiros. Quando a confiabilidade da prova — pedra angular da jurisdição — é minada por tecnologias de síntese acessíveis e sofisticadas, todo o edifício da justiça entra em risco estrutural.

Este estudo evidenciou vulnerabilidades interligadas do ordenamento: métodos tradicionais de autenticação, centrados na cadeia de custódia da coleta, não alcançam a falsidade originária típica de documentos nativamente digitais; a jurisprudência de rejeição a *prints* sem metodologia forense protege o percurso, mas não o ser do arquivo. O impacto repercute em princípios basilares — verdade material, contraditório e paridade de armas — e é agravado pelo "dividendo do mentiroso", fenômeno que permite desacreditar provas autênticas sob a sombra da síntese.

A análise semiótica mostrou por que o documento sintético convence: ao combinar iconicidade, indexicalidade e simbolicidade, ele produz um *interpretante* de autenticidade em relação a um objeto inexistente. Em paralelo, a literatura técnica e os relatórios de risco já apontam para a disseminação de manipulações documentais em fluxos financeiros e de *compliance*. A resposta adequada exige mudança de paradigma: da postura reativa — tentar detectar o falso depois — para um modelo proativo de autenticidade na origem, com *hash* ancorado em *blockchain* e marca d'água frágil como selos verificáveis, combinados a perícia algorítmica multimodal e explicável para a valoração *ex post*.

No plano processual, impõe-se recalibrar as presunções: havendo suspeita plausível de síntese, a distribuição dinâmica do ônus deve trasladar ao proponente o dever de provar a autenticidade e a proveniência, em sintonia com o art. 429 do CPC e com a racionalidade do Tema 1.061/STJ; quando a parte traz arquivo sem trilha auditável, configura-se a perda de uma chance probatória, com consequências para a admissibilidade e a valoração.

Para orientar a prática, *bench cards* e protocolos de verificação judiciais — com listas de "bandeiras vermelhas", requisitos técnicos mínimos e critérios de perícia — devem ser implementados e ensinados em formação continuada.Ao mesmo tempo, é preciso reconhecer limites persistentes: detectores sofrem com a generalização fora de laboratório e se inserem numa corrida armamentista com os geradores, o que reforça a centralidade da proveniência verificável.

Nada indica que essa será uma batalha com "vitória final". A natureza evolutiva da IA generativa impõe construir resiliência sistêmica, capaz

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

de manter a função jurisdicional cética, mas não paralisada; informada tecnologicamente, mas não tecnocrática. Isso supõe coordenação entre Judiciário, Ministério Público, Advocacia, cartórios e órgãos emissores, e academia, para alinhar protocolos, capacitação e infraestrutura de autenticidade. A alternativa é um contencioso onde tudo pode ser contestado e quase nada é verificável. A escolha, portanto, não é entre agir ou aguardar; é entre reconstruir agora o alicerce probatório da justiça — com salvaguardas robustas e competências adequadas — ou ceder espaço a um contágio de falsificações que torne indistinguíveis fato e ficção nos tribunais. O tempo adequado não é futuro; é presente.

## REFERÊNCIAS

AIMULTIPLE. *27 Real-World Blockchain Case Studies & Applications in 2025*. AIMultiple Research, 2025. Disponível em: https://research.aimultiple.com/blockchain-case-studies/. Acesso em: 11 mar. 2026.

ALBERGARIA, Pedro Soares et al. *Comentário Judiciário do Código de Processo Penal*. t. II. Coimbra: Almedina, 2019.

BARCHI, Geraldo. STJ: provas digitais e a importância da metodologia adequada na extração de dados. MFBD Advogados, 2024. Disponível em: https://mfbd.com.br/stj-provas-digitais-e-a-importancia-da-metodologia-adequada-na-extracao-de-dados/. Acesso em: 11 mar. 2026.

BLOCK, Matthias. *Deepfakes und Recht: Einführung in den deutschen Rechtsrahmen für synthetische Medien*. Wiesbaden: Springer, 2023.

BRASIL. *Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil*. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 11 mar. 2026.

BRASIL. Congresso. Senado Federal. *Projeto de Lei nº 2.338, de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&disposition=inline. Acesso em: 11 mar. 2026.

BRASIL. Congresso. Senado Federal. *Projeto de Lei nº 2.630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Senado Federal, 2020. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-2630-2020. Acesso em: 11 mar. 2026.

BRASIL. Congresso. Senado Federal. *Projeto de Lei nº 370, de 2024*. Altera a pena para o crime de violência psicológica contra a mulher. Brasília, DF: Senado Federal, 2024. Disponível em: https://www25.senado.leg.br/we

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

b/atividade/materias/-/materia/159756. Acesso em: 11 mar. 2026.

BURKE, Ronan. This receipt was made by AI. Can you tell? *Inscribe Blog*, 2025. Disponível em: https://www.inscribe.ai/blog/this-receipt-was-made-by-ai-can-you-tell. Acesso em: 11 mar. 2026.

CÂMARA DOS DEPUTADOS. Câmara aprova projeto que pune divulgação de deepfake com conteúdo sexual. Brasília, DF: Câmara dos Deputados, 19 jun. 2024. Disponível em: https://www.camara.leg.br/noticias/1175501-camara-discute-regras-para-obtencao-e-uso-de-provas-digitais-em-investigacoes-criminais. Acesso em: 11 mar. 2026.

CÂMARA DOS DEPUTADOS. Projeto que regulamenta uso da inteligência artificial no Brasil. Brasília, DF: Câmara dos Deputados, 15 maio 2025. Disponível em: https://www.camara.leg.br/noticias/1159193-projeto-que-regulamenta-uso-da-inteligencia-artificial-no-brasil. Acesso em: 11 mar. 2026.

CARRÃO, Maria do Céu Cunha. *Artificial Intelligence in Criminal Proceedings: The admissibility of AI-generated evidence*. 2022. Dissertação (Mestrado) — Nova School of Law, Lisboa, 2022.

CARRÃO, Maria do Céu Cunha. The Principle of Immediacy and AI Evidence. In: *Artificial Intelligence in Criminal Proceedings*. Lisboa: Nova School of Law, 2022. p. 58-59.

CLICKSIGN. STJ reafirma os entendimentos acerca da validade jurídica das assinaturas eletrônicas. *Clicksign Blog*, 2024. Disponível em: https://www.clicksign.com/blog/stj-reafirma-os-entendimentos-acerca-da-validade-juridica-das-assinaturas-eletronicas. Acesso em: 11 mar. 2026.

COLMAN, Ben. Why detecting dangerous AI is key to keeping trust alive. *World Economic Forum*, jul. 2025. Disponível em: https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/. Acesso em: 11 mar. 2026.

CYBEREXPERTS. Investigação Forense e Perícia Digital em Deep Fakes de Áudios e Conteúdos Criados com Inteligência Artificial. *CyberExperts Blog*, 2024. Disponível em: https://cyberexperts.com.br/investigacao-forense-e-pericia-digital-em-deep-fakes-de-audios-e-conteudos-criados-com-inteligencia-artificial/. Acesso em: 11 mar. 2026.

DATA PRIVACY BRASIL. Senado aprova PL que regulamenta IA: confira críticas e elogios ao projeto. 2024. Disponível em: https://www.dataprivacybr.org/documentos/senado-aprova-pl-que-regulamenta-ia-confira-criticas-e-elogios-ao-projeto/. Acesso em: 11 mar. 2026.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

FIGUEIREDO DIAS, Jorge. *Direito Processual Penal*. v. I. Coimbra: Coimbra Editora, 1974.

FONTENELE LEMOS, Diego; Homsi Cavalcante, Larissa; Gonçalves Mota, Rafael. A prova digital no direito processual brasileiro. *Revista Acadêmica Escola Superior do Ministério Público do Ceará*, v. 13, n. 1, p. 11-34, 2021. DOI: 10.54275/raesmpce.v13i1.147.

GFT. Pontos-chaves do projeto de lei sobre uso de IA no Brasil. *GFT Blog*, 2024. Disponível em: https://www.gft.com/br/pt/blog/pontos-chaves-do-projeto-de-lei-sobre-uso-de-ia-no-brasil. Acesso em: 11 mar. 2026.

GLESS, Sabine. AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials. *Georgetown Journal of Legal Ethics*, v. 33, p. 240, 2020.

GOMES FILHO, Antonio Magalhães. *Direito à prova no processo penal*. São Paulo: Editora Revista dos Tribunais, 1997.

GOYAL, Harshika et al. State-of-the-art AI-based Learning Approaches for Deepfake Generation and Detection, Analyzing Opportunities, Threading through Pros, Cons, and Future Prospects. *arXiv:2501.01029 [cs.LG]*, 2025.

IJERT. A Survey on Digital Watermarking for Image Authentication. *International Journal of Engineering Research and Technology*, v. 2, n. 11, nov. 2013.

INCODE. Top 5 Cases of AI Deepfake Fraud from 2024 Exposed. *Incode Blog*, 2024. Disponível em: https://incode.com/blog/top-5-cases-of-ai-deepfake-fraud-from-2024-exposed/. Acesso em: 11 mar. 2026.

J.P. Morgan. AI Scams: Deep Fakes, Impersonations, Oh My! 2025. Disponível em: https://www.jpmorgan.com/insights/fraud/fraud-protection/ai-scams-deep-fakes-impersonations-oh-my. Acesso em: 11 mar. 2026.

KELLNER, Chuck. The End of Reality? How to combat deepfakes in our legal system. *ABA Journal*, 10 mar. 2025. Disponível em: https://www.abajournal.com/columns/article/the-end-of-reality-how-to-combat-deepfakes-in-our-legal-system. Acesso em: 11 mar. 2026.

KENNEY, Andrew. How CPAs can combat the rising threat of deepfake fraud. *Journal of Accountancy*, 1 maio 2025.

KHAN, Asif et al. A Digital Image Watermarking Application for Authentication of Official Documents. *Electronics*, v. 10, n. 14, p. 1744, 2021. DOI: 10.3390/electronics10141744.

LI, Shujun; ZHANG, Xiang-Gen. A new method for authenticating PDF documents based on fragile watermarking. In: *Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Pasadena, CA, USA, 2006. p. 351-354.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

LOPES, Anderson Bezerra; Tatsuo, Eliakin Pires. Teoria da perda da chance probatória. *Boletim do Instituto Brasileiro de Ciências Criminais*, 2022. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1521. Acesso em: 11 mar. 2026.

LOPES JÚNIOR, Aury. *Direito processual penal*. 18. ed. São Paulo: Saraiva, 2021.

LOPES, Vitor Hugo. STJ inviabiliza uso de prints de WhatsApp como meio de prova. *Migalhas*, 2024. Disponível em: https://www.migalhas.com.br/quentes/422402/juiz-invalida-prints-de-whatsapp-como-prova-por-falta-de-autenticidade. Acesso em: 11 mar. 2026.

MASOOD, M.; Nawaz, M. Deepfakes generation and detection: open challenges and way forward. *Applied Intelligence*, v. 53, p. 1-35, 2023.

MIGALHAS. STJ valida assinatura eletrônica fora do sistema ICP-Brasil. *Migalhas*, 30 set. 2024. Disponível em: https://www.migalhas.com.br/quentes/416221/stj-valida-assinatura-eletronica-fora-do-sistema-icp-brasil. Acesso em: 11 mar. 2026.

MOLDSTUD. Blockchain for Digital Identity: Real-World Case Studies and Practical Applications. *MoldStud*, 2025. Disponível em: https://moldstud.com/articles/p-blockchain-for-digital-identity-real-world-case-studies-and-practical-applications. Acesso em: 11 mar. 2026.

NGUYEN, Tai D. et al. Forensic Self-Descriptions Are All You Need for Zero-Shot Detection, Open-Set Source Attribution, and Clustering of AI-generated Images. *arXiv:2503.21003 [cs.CV]*, 2025.

OPIAH, Abigail. Deepfake financial fraud to surge over the next 12 months, Deloitte reveals. *Biometric Update*, 19 set. 2024.

PACHECO, Rodrigo. Senado Federal aprova marco regulatório da Inteligência Artificial. *Ministério da Cultura*, 2023. Disponível em: https://www.gov.br/cultura/pt-br/assuntos/noticias/senado-federal-aprova-marco-regulatorio-da-inteligencia-artificial. Acesso em: 11 mar. 2026.

PEIRCE, Charles Sanders. *Collected Papers*. Cambridge: Harvard University Press, 1931-1958.

PIGÃO, Larissa. Deepfakes em provas judiciais: estamos prontos para a manipulação de evidências digitais? *GSGA*, 2024. Disponível em: https://gsga.com.br/deepfakes-em-provas-judiciais-estamos-prontos-para-a-manipulacao-de-evidencias-digitais/. Acesso em: 11 mar. 2026.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2014.

RAMALHO, David Silva. *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017.

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

RAMALHO, David Silva. Digital Chain of Custody. In: *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Coimbra: Almedina, 2017. p. 258.

REIS, Advocacia. Golpes com Deepfake: Responsabilidade Civil e Indenização. *Advocacia Reis*, 2024. Disponível em: https://advocaciareis.adv.br/blog/familia/golpes-com-deepfake/. Acesso em: 11 mar. 2026.

RESISTANT.AI. Document Fraud Analysis. In: U.S. Department of Homeland Security. *Impact of Artificial Intelligence on Criminal and Illicit Activities*. Washington, D.C., 2024. p. 23.

ROITMAN, Marcelo. Deepfakes em provas judiciais: estamos preparados para a manipulação de evidências digitais? *LexLegal*, 2024. Disponível em: https://lexlegal.com.br/deepfakes-em-provas-judiciais-estamos-preparados-para-a-manipulacao-de-evidencias-digitais/. Acesso em: 11 mar. 2026.

ROSA, Alexandre Morais da. *Guia do processo penal conforme a teoria dos jogos*. Florianópolis: Empório do Direito, 2017.

RUNYON, Natalie. Deepfakes as evidence: How judges can address the challenges of AI-generated content. *Thomson Reuters Institute*, 2025. Disponível em: https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/. Acesso em: 11 mar. 2026.

SCHIFF, Kaylyn Jackson; Schiff, Daniel S.; Bueno, Natália S. The Liar's Dividend: Can Politicians Use Deepfakes and Fake News to Evade Accountability? *SocArXiv*, maio 2022. DOI: 10.31235/osf.io/q6mwn.

SHERMAN, A. A Feast of Fraud: How International Hesitations to Regulate Deepfakes Are Creating a Buffet for Financial Crime. *Journal of Financial Crime*, 2025.

SILVA, José Antônio Ribeiro de Oliveira. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. *Revista do Tribunal Superior do Trabalho*, v. 88, n. 2, p. 199-219, abr./jun. 2022.

SILVEIRA, Sebastião Sérgio da; Silveira, Ricardo dos Reis. A prova eletrônica no processo penal. *Revista da Faculdade de Direito da UFG*, v. 39, n. 1, p. 217-237, jan./jun. 2015.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). Instituição financeira é responsável por provar autenticidade de assinatura em contrato questionado pelo cliente. Brasília, DF: STJ, 4 fev. 2022. (Tema Repetitivo 1.061). Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04022022-Instituicao-financeira-e-responsavel-por-provar-autenticidade-de-assinatura-em-contrato-

Revista Eletrônica de Direito Processual
Rio de Janeiro – Brasil
e-ISSN 1982-7636

questionado-pelo-cliente-.aspx. Acesso em: 11 mar. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). 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: 11 mar. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). Recurso Especial nº 2.159.442 – PR. Relatora: Min. Nancy Andrighi. Brasília, DF, 30 set. 2024.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). Acórdão 1750473. Relator: Roberto Freitas Filho. Brasília, DF, 24 ago. 2023.

TURNER, L.; Beyk, S. A systematic literature review of deepfake detection. *Journal of Cyber Security Technology*, v. 7, n. 1, p. 1-25, 2023.

U.S. Department of Homeland Security. *Impact of Artificial Intelligence on Criminal and Illicit Activities*. Washington, D.C., 2024. Disponível em: https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf. Acesso em: 11 mar. 2026.

ULAM. Blockchain Analysis in Action: Real-Life Use Cases and Insights. *Ulam Blog*, 2024. Disponível em: https://www.ulam.io/blog/blockchain-analysis-in-action-real-life-use-cases-and-insights. Acesso em: 11 mar. 2026.

VALENTE, Manuel Monteiro Guedes. *Processo Penal*. Tomo I. 4. ed. Coimbra: Almedina, 2020.

ZEAR, A. et al. A proposed method for digital image watermarking. *Journal of Physics: Conference Series*, v. 1530, p. 012048, 2020.

ZHANG, Y. A survey on deepfake techniques: generation, detection and applications. *Multimedia Tools and Applications*, v. 81, p. 36465-36506, 2022.