Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i7.28062

AUTENTICIDADE E CADEIA DE CUSTÓDIA DE PROVAS DIGITAIS NO PROCESSO PENAL BRASILEIRO: RISCOS DA MANIPULAÇÃO POR INTELIGÊNCIA ARTIFICIAL[1]

João Marcos de Souza Santos[2]
Antônio da Silva Rocha Neto[3]
Emanuel Vieira Pinto[4]

RESUMO: O presente artigo analisa a autenticidade e a cadeia de custódia das provas digitais no processo penal brasileiro, com foco nos riscos de manipulação decorrentes das tecnologias de inteligência artificial (IA), em especial os *deepfakes*. A crescente digitalização das relações humanas impõe novos desafios à produção e valoração da prova penal, exigindo mecanismos robustos de preservação da integridade probatória. Questiona-se: de que maneira a prova digital pode manter sua integridade e confiabilidade diante dos riscos de falsificação potencializados pela IA? O objetivo geral consiste em analisar a importância da cadeia de custódia na preservação da autenticidade das provas digitais, à luz da Lei nº 13.964/2019. Especificamente, busca-se: compreender os fundamentos normativos da cadeia de custódia digital; analisar os critérios de validade da prova eletrônica; avaliar os impactos da IA sobre a credibilidade probatória; identificar mecanismos de controle como *blockchain* e criptografia; e refletir sobre perspectivas futuras. Trata-se de pesquisa qualitativa, bibliográfica e documental, empregando o método dedutivo. Os resultados indicam que a positivação da cadeia de custódia pelo Pacote Anticrime foi avanço necessário, mas insuficiente diante da ausência de padronização técnica e do acelerado desenvolvimento de ferramentas de manipulação sintética. Conclui-se pela urgência de governança jurídico-tecnológica integrada, capacitação dos operadores do direito e adoção de protocolos forenses alinhados aos princípios constitucionais do devido processo legal, do contraditório e da ampla defesa.

Palavras-chave: Prova digital. Cadeia de custódia. Deepfake. Inteligência artificial. Processo penal.

1 INTRODUÇÃO

O avanço tecnológico e a crescente digitalização das relações humanas transformaram profundamente o modo como a sociedade se comunica, produz informações e interage. No contexto jurídico, essas transformações impactam de forma decisiva a produção e a valoração

[1]Artigo apresentado à Faculdade de Ciências Sociais Aplicadas, como parte dos requisitos para obtenção do Título de Bacharel em Direito, em 2026.
[2]Graduando em Direito pela Faculdade de Ciências Sociais Aplicadas.
[3]Professor-Orientador. Docente na Faculdade de Ciências Sociais Aplicadas.
[4]Professor-Orientador. Mestre em Educação. Docente na Faculdade de Ciências Sociais Aplicadas.

das provas, especialmente no processo penal. As tecnologias digitais criaram novas formas de registro e armazenamento de informações, como mensagens eletrônicas, áudios, vídeos, dados de geolocalização e metadado, que passaram a ocupar papel central na reconstrução dos fatos e na busca pela verdade real. Entretanto, a natureza volátil, replicável e frágil dessas evidências traz desafios inéditos à investigação e à apreciação judicial.

Diante desse cenário, a cadeia de custódia consolida-se como instrumento técnico e jurídico indispensável para garantir a autenticidade, a integridade e a confiabilidade das provas digitais. Trata-se do conjunto de procedimentos formais que documentam, passo a passo, o caminho percorrido pela prova desde sua coleta até sua apresentação em juízo (Brasil, 2019). Segundo Prado, a cadeia de custódia é o dispositivo dirigido a assegurar a fiabilidade do elemento probatório, ao colocá-lo sob proteção de interferências capazes de falsificar o resultado da atividade probatória Araújo (2024, p. 144, apud Prado, 2021).

A situação se torna ainda mais complexa diante da expansão das tecnologias de inteligência artificial. Técnicas como os deepfakes permitem criar imagens, áudios e vídeos falsificados com alto grau de realismo, capazes de enganar até análises forenses preliminares, colocando em xeque a credibilidade das provas audiovisuais e ampliando a possibilidade de erros judiciários Nakanishi (2023). Dados recentes indicam que os arquivos de deepfake saltaram de 500 mil em 2023 para cerca de 8 milhões em 2025, crescimento de 900% em dois anos, com seres humanos identificando corretamente esses conteúdos em apenas 24,5% das vezes Deepmedia (2023) Deepstrike (2025).

Em resposta a esse cenário, a 5ª Turma do Superior Tribunal de Justiça decidiu, em 2024, que prints de tela e imagens digitais extraídas sem metodologia adequada carecem de valor probatório, enfatizando ser ônus do Estado comprovar a integridade e confiabilidade das fontes de prova digitais BRASIL (2024).

Emerge, assim, o problema central desta pesquisa: de que maneira a prova digital pode manter sua integridade e confiabilidade no processo penal diante dos riscos de manipulação, perda de autenticidade e falsificação potencializados por tecnologias de inteligência artificial, como os deepfakes?

O objetivo geral deste trabalho é analisar a importância da cadeia de custódia das provas digitais no processo penal, considerando os desafios impostos pela manipulação tecnológica e pela insuficiência da padronização normativa. Como objetivos específicos, propõe-se: compreender os fundamentos teóricos e normativos da cadeia de custódia digital; analisar a

natureza e os critérios de validade da prova eletrônica; avaliar os impactos da inteligência artificial sobre a credibilidade probatória; identificar mecanismos de controle e aprimoramento da cadeia de custódia; e refletir sobre os desafios e perspectivas futuras da prova digital.

A justificativa deste estudo decorre da urgência em adaptar o processo penal às novas realidades digitais, garantindo que a produção de provas esteja em conformidade com os princípios constitucionais do contraditório, da ampla defesa e do devido processo legal. A proliferação de conteúdos falsificados ameaça a confiança pública nas instituições judiciais e na própria administração da justiça, tornando o tema de relevância social e institucional indiscutível.

2 METODOLOGIA

O presente trabalho foi desenvolvido sob uma perspectiva qualitativa, voltada à análise teórica e interpretativa dos conceitos relacionados à cadeia de custódia das provas digitais e aos desafios decorrentes da manipulação de dados por meio da inteligência artificial. A abordagem qualitativa mostrou-se adequada em razão da complexidade do objeto estudado, que envolve não apenas aspectos jurídicos, mas também elementos tecnológicos e procedimentais relacionados à preservação da autenticidade probatória no processo penal contemporâneo.

Quanto ao tipo de pesquisa, o estudo enquadra-se como bibliográfico e documental, fundamentando-se em artigos científicos, monografias, dissertações, teses e obras doutrinárias especializadas sobre prova digital, cadeia de custódia e inteligência artificial aplicada ao processo penal. O aspecto documental complementou a pesquisa teórica mediante a análise de dispositivos legais, resoluções, projetos legislativos e entendimentos jurisprudenciais pertinentes ao tema, especialmente os arts. 158-A a 158-F do Código de Processo Penal, introduzidos pela Lei nº 13.964/2019, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e o Projeto de Lei nº 2.338/2023, que dispõe sobre o marco regulatório da inteligência artificial no Brasil.

Para assegurar maior rigor metodológico, a seleção das fontes observou critérios de pertinência temática, relevância acadêmica e atualidade, realizou-se levantamento bibliográfico nas bases Google Acadêmico, Scielo, repositórios universitários (UNIPAMPA, UNICEUB, PUC-Goiás e UFS) e no Portal de Periódicos da CAPES, priorizando produções publicadas entre os anos de 2021 e 2025, período em que se intensificaram os debates sobre deepfakes, inteligência artificial generativa e autenticidade das provas digitais. Também foram utilizados

materiais e documentos técnicos relacionados à segurança da informação e à computação forense.

O procedimento metodológico consistiu na leitura analítica, interpretação crítica e comparação das fontes selecionadas, com posterior sistematização dos conteúdos em categorias temáticas, tais como: fundamentos normativos da cadeia de custódia digital; vulnerabilidades e riscos de adulteração das provas eletrônicas; impactos da inteligência artificial na credibilidade probatória; lacunas normativas existentes; e mecanismos tecnológicos de preservação da integridade dos vestígios digitais.

Adotou-se, ainda, abordagem interdisciplinar, integrando conhecimentos do Direito Processual Penal, da Tecnologia da Informação e da Perícia Digital, com o objetivo de compreender de maneira ampla os impactos das novas tecnologias sobre as garantias constitucionais do contraditório, da ampla defesa e do devido processo legal. A partir desse diálogo entre diferentes áreas do conhecimento, buscou-se analisar não apenas os desafios jurídicos atuais, mas também as possíveis soluções técnicas e regulatórias voltadas ao fortalecimento da autenticidade e da confiabilidade das provas digitais no processo penal brasileiro.

3 REVISÃO DE LITERATURA

3.1 Breve Histórico Mundial e Nacional da Cadeia de Custódia Digital

O conceito de cadeia de custódia surgiu originalmente no campo das ciências forenses, nas primeiras décadas do século XX, em países como os Estados Unidos e o Reino Unido, quando se consolidaram as práticas laboratoriais de documentação de vestígios físicos e materiais apreendidos em investigações criminais. Nessa fase, o objetivo era garantir que o objeto analisado em juízo fosse o mesmo coletado no local do crime, estabelecendo uma sequência de controle que assegurasse sua autenticidade e integridade.

Com o avanço da tecnologia da informação, especialmente a partir da década de 1990, as provas começaram a migrar do meio físico para o ambiente digital, exigindo novas metodologias de coleta, armazenamento e análise. Como destaca Rodrigues (2024), a transformação digital deslocou o foco da custódia material para a custódia lógica, impondo a necessidade de garantir a integridade dos dados eletrônicos com o mesmo rigor que se aplicava aos objetos físicos. Nora e Freitas (2024) situam essa transformação na emergência de uma "sociedade informacional", caracterizada pela velocidade, amplitude e impacto sistêmico das

mudanças tecnológicas, na qual os dados e informações gerados nos ambientes digitais passam a ser fundamentais como fontes de prova.

Nos Estados Unidos e na Europa, o desenvolvimento de padrões técnicos internacionais como as diretrizes do National Institute of Standards and Technology (NIST) e do European Network of Forensic Science Institutes (ENFSI) estabeleceu parâmetros de verificação da autenticidade digital. No Brasil, a norma ABNT NBR ISO/IEC 27037:2013 traz diretrizes para identificação, coleta, aquisição e preservação de evidências digitais, com três pilares fundamentais: relevância, confiabilidade e suficiência Nora e Freitas (2024). A adoção desses parâmetros internacionais representa um esforço de harmonização técnica ainda incompleto no âmbito das instituições brasileiras de segurança pública e do sistema de justiça.

No contexto nacional, o ordenamento jurídico evoluiu lentamente. Até o início da década de 2010, não havia regulamentação específica sobre a cadeia de custódia, situação que, segundo Sobrinha (2021), gerava insegurança jurídica e comprometia a confiabilidade das provas digitais produzidas em investigações criminais. O marco de virada ocorreu com a Lei nº 13.964/2019 (Pacote Anticrime), que inseriu os arts. 158-A a 158-F no Código de Processo Penal, positivando o conceito e os procedimentos da cadeia de custódia.

A partir dessa alteração legislativa, o Brasil passou a reconhecer formalmente a necessidade de documentação contínua de cada etapa do manejo da prova, inclusive em formato eletrônico. Contudo, Silva (2025) adverte que a positivação legal não eliminou as deficiências práticas do sistema, destacando a falta de padronização tecnológica e de capacitação dos agentes públicos como entraves à efetividade da custódia digital. Esse diagnóstico revela que a evolução normativa, embora necessária, é insuficiente sem o correspondente investimento em infraestrutura técnica e formação profissional.

3.2 Conceito e Fundamentos da Cadeia de Custódia Digital

A cadeia de custódia representa o conjunto de procedimentos formais e contínuos destinados a assegurar a autenticidade, a integridade e a rastreabilidade das provas coletadas no curso da investigação e do processo penal. Conforme definição normativa constante do art. 158-A do Código de Processo Penal:

> Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. (BRASIL, 2019, art. 158-A)

Silva, (2025, p. 17) caracteriza o instituto como "o conjunto de procedimentos utilizados, desde o reconhecimento do vestígio até seu descarte, para manter e documentar a história cronológica das provas coletadas em locais ou em vítimas de crimes, visando asseverar a autenticidade das evidências apanhadas". Tal definição demonstra que a cadeia de custódia não se limita à formalidade administrativa, mas assume caráter técnico e jurídico.

No ambiente digital, a volatilidade das informações exige cuidados redobrados. Rodrigues (2024) observa que os dados digitais, pela sua natureza replicável e intangível, demandam protocolos específicos de segurança para que se mantenha a integridade da informação original. Araújo (2024) reforça que a cadeia de custódia é regida por dois princípios fundamentais: a mesmidade, que exige que a prova valorada seja exatamente aquela colhida, e a desconfiança, que impõe que a integridade e autenticidade da prova não sejam presumidas, mas comprovadas. Tais princípios são especialmente críticos nas provas digitais, que são mais suscetíveis de sofrer alterações em seu conteúdo.

Nora e Freitas (2024) destacam que os dados digitais, por sua imaterialidade, permitem a criação de cópias idênticas ao original, dificultando a identificação de adulterações e exigindo que a cadeia de custódia abranja procedimentos de criptografia, hash code e registro cronológico imutável de cada etapa do manuseio da evidência. A ausência de um relatório completo dessas etapas impede a análise judicial posterior, representando prejuízo direto ao exercício do contraditório. Essa constatação é particularmente relevante no contexto brasileiro, onde a ausência de protocolos forenses padronizados torna a documentação da cadeia de custódia dependente das práticas individuais de cada instituição investigativa.

Conforme apontam Bellé e Souza (2025), o sistema jurídico brasileiro ainda carece de padronização normativa e infraestrutura tecnológica para garantir que as etapas da custódia digital sejam plenamente observadas. A quebra da cadeia de custódia, segundo a corrente doutrinária liderada por Prado e adotada na jurisprudência do Superior Tribunal de Justiça, implica na inadmissibilidade da prova, por violação à sua fiabilidade enquanto elemento de convicção judicial BRASIL (2024). Compreender, portanto, os fundamentos da custódia digital é o primeiro passo para identificar onde os sistemas atuais falham e onde as soluções tecnológicas podem ser implementadas.

3.3 A Prova Digital no Processo Penal: Natureza, Validade e Desafios Práticos

A transformação digital redefiniu os parâmetros de produção e valoração da prova no processo penal. Hoje, informações antes restritas a suportes físicos encontram-se armazenadas em bancos de dados, redes sociais e plataformas em nuvem, ampliando exponencialmente o volume de elementos probatórios disponíveis. Vaz (2012, p. 64) define a prova digital como os "dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias". Ela se distingue das demais provas documentais exatamente pela forma de arquivamento da informação, que demanda procedimentos especiais de obtenção e produção probatória.

Segundo Sobrinha (2021), a prova digital é caracterizada por sua volatilidade e vulnerabilidade à manipulação, por depender de sistemas informáticos sujeitos a alterações automáticas, como atualizações de software, compressão de arquivos e modificações de metadados, que podem comprometer a autenticidade da evidência sem deixar rastros perceptíveis. Nora e Freitas (2024) acrescentam quatro características que distinguem a prova digital: imaterialidade, volatilidade, suscetibilidade à clonagem e indispensabilidade de dispositivo acessório para sua leitura. Essas características tornam a prova digital essencialmente distinta das provas materiais tradicionais, exigindo um tratamento jurídico igualmente diferenciado.

Como observa Rodrigues (2024), a valoração das evidências tecnológicas exige o mesmo rigor aplicado às provas tradicionais, acrescido de garantias adicionais relacionadas à rastreabilidade e à documentação de todo o ciclo de vida da informação. A ausência de comprovação da origem e da integridade dos dados pode conduzir à inutilização da prova, por ofensa ao devido processo legal e à segurança jurídica. Em sentido convergente, Araújo (2024) ressalta que a integridade e a autenticidade de uma prova digital não são presumidas, mas devem ser comprovadas, de modo que durante a investigação deve ficar demonstrado que o elemento probatório não foi manipulado pelos agentes do Estado responsáveis pela custódia.

De forma particularmente relevante, a 5ª Turma do Superior Tribunal de Justiça decidiu que prints de tela e imagens digitais extraídas sem metodologia adequada não possuem valor como prova, consignando que é ônus do Estado comprovar a integridade e a confiabilidade das fontes de prova, inclusive quando elas tiverem natureza digital Brasil (2024). Essa orientação jurisprudencial representa um avanço significativo: ao elevar a cadeia de custódia ao status de requisito de admissibilidade probatória, o STJ sinaliza que a validade da prova digital no Brasil

não se satisfaz com a mera juntada do elemento ao processo, pois, exige documentação técnica de toda a sua trajetória.

A prova digital deve, portanto, ser tratada como elemento híbrido, que combina aspectos técnicos e jurídicos: requer controle tecnológico para assegurar a imutabilidade dos dados e, ao mesmo tempo, demanda interpretação jurídica rigorosa para garantir o respeito aos direitos fundamentais. A efetividade desse equilíbrio depende da atuação coordenada de peritos, magistrados e operadores do Direito. O que pressupõe formação técnica multidisciplinar ainda incipiente no Brasil.

3.4 Inteligência Artificial, Deepfakes e os Riscos à Autenticidade da Prova Digital

O avanço da inteligência artificial trouxe benefícios inegáveis à investigação criminal e à análise de provas, permitindo o processamento de grandes volumes de dados e a identificação de padrões com alta precisão. No entanto, essas mesmas tecnologias introduzem riscos inéditos à autenticidade probatória, especialmente com o surgimento dos chamados deepfakes, que são conteúdos sintéticos gerados por redes neurais capazes de criar áudios, vídeos e imagens falsificadas com realismo quase absoluto.

> Os deepfakes representam uma ameaça substancial no combate à desinformação. A capacidade de criar vídeos falsos convincentes, nos quais pessoas reais parecem estar dizendo ou fazendo coisas que nunca fizeram, pode ser explorada para manipular a opinião pública, uma vez que essa tecnologia não possui regulamentação própria ou limites nos dias atuais. Nakanishi (2023, p. 23)

Essa constatação coloca em xeque um dos pilares do processo penal: a confiança na materialidade da prova. Ao contrário das falsificações tradicionais, os deepfakes reconstroem a informação com base em padrões de aprendizado profundo (deep learning), tornando a adulteração praticamente invisível Bellé e Souza (2025). O cenário é agravado pela difusão dessas ferramentas em plataformas de código aberto, que democratiza o poder de criar conteúdos falsificados e amplia o potencial de uso malicioso da IA em contextos criminais.

Para além da falsificação ativa, o processo penal passa a conviver com um duplo risco: a fabricação de provas e a negação estratégica da autenticidade, situação em que o acusado alega que a prova legítima é um deepfake para criar dúvida razoável. Como afirmam Bellé e Souza (2025), o sistema de justiça enfrenta uma crise de autenticidade, em que a prova digital, antes considerada elemento objetivo, passa a exigir novas formas de validação técnica e jurídica. Trata-se de uma inversão paradigmática: se antes a existência de um vídeo ou áudio era

suficiente para sustentar uma acusação, hoje a própria existência da mídia como prova precisa ser provada.

No plano normativo, o Brasil ainda carece de regulamentação específica sobre o uso da IA em perícias forenses. O PL nº 2.338/2023, aprovado pelo Senado em dezembro de 2024 e em tramitação na Câmara dos Deputados, institui o marco legal da inteligência artificial no Brasil, adotando abordagem baseada em risco. Sistemas utilizados na administração da justiça são classificados como de alto risco e sujeitos a exigências reforçadas de transparência, documentação técnica e avaliação de impacto algorítmico (Brasil, 2023). Desse modo, a inexistência de protocolos oficiais para autenticação de dados digitais faz com que decisões judiciais dependam, muitas vezes, de laudos periciais despadronizados ou de ferramentas tecnológicas de origem privada, sem transparência sobre seus algoritmos.

Sobrinha (2021) defende que a confiabilidade da prova digital no contexto da IA depende da criação de mecanismos de verificação criptográfica e certificação pública, capazes de assegurar a imutabilidade dos dados e rastrear qualquer alteração posterior. Contudo, não basta a adoção de instrumentos técnicos: é também necessário desenvolver uma ética probatória digital, baseada na transparência, na responsabilidade e no controle social sobre o uso da inteligência artificial no processo penal. A responsabilidade sobre a autenticidade da prova não pode recair apenas sobre o perito, mas deve ser compartilhada institucionalmente pelo Estado que produziu e apresentou a evidência.

3.5 Mecanismos de Controle, Aprimoramento e Prevenção na Cadeia de Custódia Digital

A efetividade da cadeia de custódia digital depende da implementação de mecanismos técnicos e procedimentais que assegurem a integridade, a rastreabilidade e a autenticidade das provas eletrônicas. Conforme Rodrigues (2024), a mitigação dos riscos digitais exige a adoção de protocolos técnicos de preservação da prova baseados em métodos criptográficos, hash codes e certificação digital, técnicas que criam assinaturas matemáticas únicas e comprovam a integridade dos arquivos digitais, permitindo verificar se houve qualquer alteração posterior ao momento da coleta. Esses mecanismos são, em essência, a contrapartida tecnológica dos princípios jurídicos da mesmidade e da desconfiança: oferecem a comprovação objetiva que o direito exige, mas que a perícia tradicional nem sempre consegue garantir.

Nesse sentido, a tecnologia blockchain emerge como uma das estratégias mais seguras para registrar a trajetória da prova digital. Araújo (2024) demonstrou a compatibilidade entre o

blockchain e os princípios da cadeia de custódia no ordenamento jurídico brasileiro: por operar em rede descentralizada e imutável, o blockchain permite armazenar cada ação sobre o arquivo, coleta, análise, movimentação e apresentação, de modo cronológico e auditável, de forma que qualquer tentativa de adulteração seja automaticamente detectada pela quebra da sequência lógica dos registros.

Por conseguinte, Nora e Freitas (2024) destacam que as características da tecnologia blockchain oferecem uma ferramenta viável para realizar o procedimento de cadeia de custódia de forma transparente, uma vez que a informação registrada é validada por vários nós da rede e todos os passos são imutavelmente gravados, garantindo que a prova não poderá ser manipulada após seu registro.

Nesse contexto, Nora e Freitas (2024) apresentam ainda o modelo CustodyBlock (CB), proposto por Alruwaili (2021), que utiliza a tecnologia Hyperledger, um protocolo de blockchain privado, com contratos inteligentes para apoiar o controle, transferência, análise e monitoramento da cadeia de custódia de provas digitais. Esse modelo demonstra como é possível mapear, em registros imutáveis, cada uma das etapas previstas no art. 158-B do Código de Processo Penal, desde o reconhecimento inicial do vestígio até seu descarte, conferindo rastreabilidade transparente a todos os participantes autorizados, como autoridades policiais, Ministério Público e magistrados. A viabilidade técnica do modelo CustodyBlock indica que a adoção do blockchain na custódia digital não é apenas teoricamente possível, mas operacionalmente implementável dentro do marco legal brasileiro vigente.

Contudo, é importante reconhecer que a segurança do blockchain não é absoluta. Nora e Freitas (2024) advertem que o ponto crítico de vulnerabilidade permanece na fase de coleta e hash inicial da evidência, momento em que um ator mal-intencionado pode inserir dados adulterados antes de seu registro na cadeia de blocos. Por isso, a implementação do blockchain deve ser acompanhada de rigorosos protocolos de coleta forense e de auditoria dos procedimentos de entrada da evidência, o que reforça que a solução tecnológica não substitui, mas complementa, o rigor procedimental humano.

Outro aspecto relevante é a padronização institucional dos procedimentos de coleta e guarda. Sobrinha (2021) salienta que a ausência de uniformidade nos métodos periciais é uma das principais causas de nulidade processual envolvendo provas digitais, defendendo a criação de protocolos nacionais compartilhados entre as polícias, o Ministério Público e o Poder Judiciário. Bellé e Souza (2025) reforçam que a legitimidade das provas digitais depende da

capacidade das partes de auditar os procedimentos de custódia, o que concretiza o princípio do contraditório técnico e assegura que o controle da prova não se restrinja ao poder estatal. Sem essa padronização, mesmo as ferramentas mais sofisticadas perdem eficácia, pois os elos mais frágeis da cadeia continuarão a comprometer a integridade do conjunto.

No plano preventivo, Nakanishi (2023) propõe a criação de sistemas automatizados de verificação de integridade baseados em inteligência artificial forense, capazes de identificar padrões de manipulação digital, como edições ocultas, alterações de pixels e distorções sonoras, antes mesmo de a prova ser admitida em juízo. Araújo (2024) complementa esse ponto ao defender que a inteligência artificial pode ser empregada na análise de metadados, com o objetivo de identificar eventuais alterações nos vestígios digitais, enquanto o blockchain serviria para preservar a integridade e a autenticidade das informações após esse processamento.

A combinação dessas abordagens com detecção forense por IA e registro imutável por blockchain, configura uma arquitetura de confiança que pode elevar significativamente os padrões probatórios brasileiros, desde que acompanhada de regulamentação técnica específica e formação continuada dos operadores do direito.

3.6 Desafios Tecnológicos e Perspectivas Futuras da Cadeia de Custódia Digital

A consolidação da cadeia de custódia digital como instrumento essencial à validade da prova no processo penal impõe uma reflexão sobre seus desafios tecnológicos e perspectivas futuras. A rápida evolução da inteligência artificial, a expansão do uso de algoritmos autônomos e a virtualização das relações humanas transformam o modo como as provas são produzidas, armazenadas e apresentadas em juízo.

> À medida que os algoritmos de criação melhoram, fica cada vez mais difícil para os algoritmos de detecção identificarem as diferenças que separam o material falso do autêntico, aumentando então a probabilidade de espectadores comuns e até mesmo especialistas se equivocarem com o material espalhado. NAKANISHI (2023, p. 25)

Essa constatação revela que a expansão tecnológica demanda do sistema jurídico uma postura adaptativa contínua, sob pena de tornar obsoletos os mecanismos tradicionais de controle da prova. A custódia digital, antes voltada à documentação de vestígios físicos, precisa agora abranger o universo de dados digitais complexos, que circulam em múltiplos ambientes virtuais e são processados por sistemas automatizados.

Nora e Freitas (2024) situam esse desafio no contexto mais amplo da quarta revolução industrial, caracterizada pela velocidade, amplitude e impacto sistêmico das mudanças tecnológicas, características que se refletem diretamente na prática delitiva e nos procedimentos de investigação criminal, exigindo do Direito uma postura adaptativa constante. Nesse cenário, a defasagem entre a velocidade da inovação tecnológica e a lentidão do processo legislativo representa um dos maiores desafios para a efetividade da cadeia de custódia digital no Brasil.

Araújo (2024) defende que o futuro da cadeia de custódia deve se basear na combinação entre inteligência artificial e blockchain: a IA seria empregada na análise de metadados e identificação de manipulações, enquanto o blockchain garantiria a imutabilidade do registro de toda a trajetória probatória. Para o autor, o ordenamento jurídico brasileiro já autoriza esse uso, uma vez que os dispositivos legais não esgotam as técnicas a serem empregadas na preservação dos elementos de prova, abrindo espaço para adoção de meios tecnológicos compatíveis com os fins pretendidos pelo legislador. Essa interpretação é promissora, pois indica que a inovação tecnológica na cadeia de custódia não exige necessariamente nova legislação, pois, pode ser implementada dentro do marco normativo atual, desde que orientada por uma interpretação finalística das normas.

Por outro lado, Silva (2025) alerta para o risco da automatização excessiva: a utilização de ferramentas de IA para validar provas pode reduzir a intervenção humana e, consequentemente, comprometer o exercício do contraditório. A busca por eficiência não pode suprimir o controle judicial e a transparência processual, sob pena de transformar o processo penal em procedimento tecnocrático. Há, portanto, um equilíbrio necessário entre a automação dos mecanismos de custódia e a preservação do controle humano sobre as decisões probatórias, equilíbrio que o direito processual penal precisa definir com clareza.

No plano regulatório, a aprovação do PL nº 2.338/2023 pelo Senado Federal representa avanço significativo ao classificar sistemas de IA com impacto sobre a administração da justiça como de alto risco, exigindo transparência, rastreabilidade algorítmica e avaliações de impacto periódicas (Brasil, 2023). Sua efetividade, contudo, dependerá de regulamentação infralegal robusta e de capacidade institucional de fiscalização.

Conforme argumentam Bellé e Souza (2025), o futuro da prova digital dependerá da confiança pública nos sistemas tecnológicos que a produzem e validam, confiança que não se constrói apenas pela sofisticação dos algoritmos, mas pela transparência e auditabilidade dos

métodos empregados. Silva (2025) reforça que a efetividade da cadeia de custódia digital depende tanto da infraestrutura tecnológica quanto da capacitação humana: de nada adianta um sistema digital seguro se os agentes públicos não forem capazes de operá-lo adequadamente. Em síntese, o futuro da prova digital exigirá não apenas novas ferramentas, mas um novo paradigma de responsabilidade institucional e formação profissional.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A análise da literatura consolidada neste estudo evidencia que a cadeia de custódia digital no processo penal brasileiro encontra-se em um ponto de inflexão: avançou normativamente com a Lei nº 13.964/2019, mas permanece vulnerável operacionalmente diante da velocidade com que as tecnologias de manipulação se desenvolvem. Essa tensão entre avanço formal e insuficiência prática é o fio condutor que perpassa toda a problemática investigada.

A positivação dos arts. 158-A a 158-F do CPP representou reconhecimento formal de uma necessidade que a doutrina e a prática forense já apontavam há anos. Entretanto, como demonstrado por Nora e Freitas (2024), a norma concentrou-se sobretudo em vestígios físicos, deixando lacunas consideráveis quanto aos procedimentos específicos para evidências digitais, como a imaterialidade dos dados, a possibilidade de clonagem sem deixar rastros e a dependência de dispositivos acessórios para leitura.

Um exemplo concreto dessas lacunas é a ausência, na lei, de exigência expressa de uso de hash criptográfico no momento da extração de dados de dispositivos móveis. Essa omissão viabilizou a prática reiterada de extrações por meio de simples capturas de tela, sem qualquer verificação de integridade, sendo este exatamente o cenário que levou o STJ a anular provas no julgamento do AgRg no HC 828.054/RN (Brasil, 2024). A omissão legislativa, portanto, não é meramente teórica: tem consequências processuais concretas e mensuráveis.

O fenômeno dos deepfakes ilustra com particular intensidade esse dilema. As mesmas tecnologias de IA que oferecem instrumental poderoso para detecção forense de falsificações também permitem criar conteúdos sintéticos praticamente indistinguíveis da realidade. Como demonstra Araújo (2024), a inteligência artificial pode ser empregada tanto na preservação quanto na subversão da cadeia de custódia, o que torna a ausência de regulamentação técnica específica para seu uso em perícias forenses um grave risco ao sistema probatório. Diante desse cenário, entende-se que a IA forense deve ser integrada à cadeia de custódia como camada adicional de verificação, mas nunca como substituta do rigor procedimental humano.

A convergência entre blockchain, protocolos de hash criptográfico e sistemas de IA forense configura o que se pode denominar de tríade tecnológica da custódia digital. Cada elemento, isoladamente, apresenta limitações apontadas pela literatura: o blockchain não protege contra adulterações anteriores ao registro Nora e Freitas (2024), o hash criptográfico não detecta manipulações invisíveis aos algoritmos tradicionais; e a IA forense pode ser enganada por deepfakes de última geração Nakanishi (2023). A sinergia entre os três, contudo, cria camadas sobrepostas de controle que elevam significativamente o custo e a complexidade de qualquer tentativa de adulteração probatória. Nenhuma dessas tecnologias representa solução definitiva isoladamente, mas sua combinação configura a resposta mais robusta disponível no atual estado da arte.

No plano dos direitos fundamentais, a questão transcende o aspecto técnico. A integridade da cadeia de custódia é condição de efetividade do contraditório: sem ela, a defesa não tem como auditar ou contestar a origem e a trajetória da evidência, o que viola as garantias do art. 5º, LV, da Constituição Federal. A recente decisão do STJ (Brasil, 2024) consolida essa perspectiva ao exigir comprovação estatal da integridade das fontes de prova digitais, transformando a cadeia de custódia em garantia constitucional de primeira ordem.

Ademais, em sentido contrário, a ausência de cadeia de custódia também pode ser usada de forma oportunista pela defesa para questionar provas legítimas, o que reforça a necessidade de protocolos robustos que confiram objetividade à verificação de integridade probatória.

Diante desse quadro, entende-se que a solução mais viável, no contexto brasileiro atual, não é apostar em uma única tecnologia, mas combinar regulamentação clara, protocolos técnicos padronizados e supervisão humana qualificada. A blockchain tende a ser a ferramenta mais promissora para registro e auditabilidade; contudo, sua eficácia depende da qualidade da coleta inicial e da uniformização dos procedimentos periciais. Assim, a resposta mais consistente ao problema não é apenas tecnológica, mas institucional.

A análise sugere que a solução para os desafios da prova digital no contexto da IA não pode ser exclusivamente tecnológica nem exclusivamente normativa. Ela requer uma abordagem de governança integrada, que articule legislação atualizada, protocolos técnicos padronizados, capacitação continuada dos operadores do direito e mecanismos de controle social sobre o uso de IA no processo penal. Dentre essas dimensões, considera-se que a padronização técnica nacional, que ainda inexiste, é a mais urgente, pois é o alicerce sobre o qual todas as demais soluções precisam se sustentar.

5 CONCLUSÃO

O presente estudo demonstrou que a autenticidade e a cadeia de custódia das provas digitais no processo penal brasileiro enfrentam desafios de crescente complexidade, potencializados pela expansão das tecnologias de inteligência artificial, em particular, os deepfakes. A análise bibliográfica e documental realizada permitiu alcançar os objetivos propostos e oferecer respostas à questão central da pesquisa.

Em relação aos fundamentos normativos, verificou-se que a Lei nº 13.964/2019 representou avanço histórico ao positivar o conceito de cadeia de custódia no Código de Processo Penal. Contudo, a norma revela insuficiências ao abordar primariamente vestígios físicos, deixando lacunas procedimentais relevantes para o tratamento de evidências digitais, especialmente quanto à sua imaterialidade, volatilidade e suscetibilidade à clonagem sem rastros.

No tocante à validade da prova eletrônica, o estudo evidenciou que ela depende não apenas da admissibilidade formal, mas de uma legitimidade epistêmica que só se alcança com rigorosa documentação da cadeia de custódia, verificação técnica da integridade dos dados e transparência sobre os sistemas tecnológicos que produziram ou armazenaram a evidência. A recente jurisprudência do STJ (Brasil, 2024) consolida essa perspectiva ao exigir que o Estado comprove a integridade das fontes de prova digitais.

Quanto aos impactos da inteligência artificial sobre a credibilidade probatória, os dados são inequívocos: o crescimento exponencial dos deepfakes de 500 mil para 8 milhões de arquivos entre 2023 e 2025 Deepmedia (2023) Deepstrike (2025) e a baixa taxa de identificação humana desses conteúdos (24,5%) revelam uma vulnerabilidade estrutural do sistema probatório tradicional. O processo penal não pode ignorar essa realidade; precisa adaptá-la como variável central de seu desenho normativo e procedimental.

Em relação aos mecanismos de controle, a tríade blockchain, criptografia e IA forense apresenta potencial transformador para a custódia digital. O modelo CustodyBlock (CB), apresentado por Nora e Freitas (2024) com base no trabalho de Alruwaili (2021), e a proposta de Araújo (2024) de combinação entre IA para análise de metadados e blockchain para preservação da integridade demonstram a viabilidade técnico-jurídica dessas ferramentas no ordenamento brasileiro. A adoção dessas tecnologias, porém, deve ser acompanhada de protocolos rigorosos na fase de coleta, para evitar que dados adulterados sejam registrados como autênticos.

No plano das perspectivas futuras, o PL nº 2.338/2023 aprovado pelo Senado em dezembro de 2024, representa passo relevante ao classificar sistemas de IA com impacto sobre a administração da justiça como de alto risco, sujeitos a exigências especiais de transparência e rastreabilidade. No entanto, a efetividade do marco regulatório dependerá de regulamentação infralegal específica e de capacidade institucional de fiscalização.

Conclui-se, portanto, que a preservação da autenticidade das provas digitais no contexto da inteligência artificial exige uma resposta multidimensional: atualização normativa com foco específico em evidências digitais; adoção de protocolos técnicos nacionais padronizados inspirados na norma ABNT NBR ISO/IEC 27037:2013; implementação de tecnologias de verificação de integridade como blockchain e criptografia; desenvolvimento de sistemas forenses baseados em IA para detecção de deepfakes; formação continuada dos operadores do direito em segurança da informação e forense digital; e governança compartilhada entre o Direito, a tecnologia e a ética pública.

A cadeia de custódia digital deve ser compreendida, em última análise, como pilar de legitimidade do processo penal democrático. Sem ela, a busca pela verdade processual torna-se vulnerável às distorções da era sintética. Com ela, bem implementada e tecnologicamente atualizada, o processo penal pode manter sua função essencial: a realização da justiça com respeito aos direitos fundamentais e à dignidade humana.

REFERÊNCIAS

ALRUWAILI, Fahad F. CustodyBlock: a distributed chain of custody evidence framework. Information, Basel, v. 12, n. 2, p. 88, fev. 2021. DOI: 10.3390/info12020088. Disponível em: https://www.mdpi.com/2078-2489/12/2/88. Acesso em: 23 mai. 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, fluxo contínuo, e47605, 2024. DOI: 10.35699/2965-6931.2023.47605. Disponível em: https://periodicos.ufmg.br/index.php/revistadaufmg/article/view/47605. Acesso em: 23 mai. 2026.

BELLÉ, Adriano Vottri; SOUZA, Ayleen Dywaine. Provas digitais no processo penal: autenticidade, manipulação por inteligência artificial e desafios ao devido processo. Revista Jurídica Gralha Azul – TJPR, v. 1, n. 28, 2025. DOI: 10.62248/cbjxxr83. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/184. Acesso em: 22 out. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 out. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 out. 2025.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 22 out. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial (Marco Legal da IA). Aprovado pelo Senado em dez./2024; em tramitação na Câmara dos Deputados. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 20 mai. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). Agravo Regimental no Habeas Corpus nº 828.054/RN. Relator: Min. Joel Ilan Paciornik. Brasília: STJ, julgado em 23 abr. 2024, DJe 07 mai. 2024. Disponível em: https://www.stj.jus.br. Acesso em: 20 mai. 2026.

DEEPMEDIA. Deepfake statistics: 500,000 video and voice deepfakes shared on social media in 2023. San Francisco: DeepMedia AI, 2023. Reportado por: Reuters. Disponível em: https://deepmedia.ai. Acesso em: 20 mai. 2026.

DEEPSTRIKE. Deepfake statistics 2025: the data behind the AI fraud wave. Mohammed Khalil. DeepStrike Cybersecurity, set. 2025. Disponível em: https://deepstrike.io/blog/deepfake-statistics-2025. Acesso em: 20 mai. 2026.

LOBÃO SOBRINHA, Maria Quaranta de. Cadeia de custódia das provas digitais: a perícia técnica como instrumento das garantias. 2021. Monografia (Graduação em Direito) – Universidade Federal de Sergipe, São Cristóvão, SE, 2021. Disponível em: https://ri.ufs.br/jspui/handle/riufs/14545. Acesso em: 22 out. 2025.

NAKANISHI, Maria Fernanda Mugnaini. A problemática jurídica dos deepfakes: uma análise do uso da inteligência artificial na produção de provas e suas repercussões penais. 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário de Brasília, Brasília, 2023. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/17157. Acesso em: 22 out. 2025.

NORA, Heloísa Daniela; FREITAS, Cinthia Obladen de Almendra. A tecnologia blockchain como ferramenta viável para cadeia de custódia de provas digitais. Ponto de Vista Jurídico, Caçador (SC), v. 13, n. 2, p. e3540-e3540, jul./dez. 2024. DOI: 10.33362/juridico.v13i2.3540. Disponível em: https://periodicos.uniarp.edu.br/index.php/juridico/article/view/3540. Acesso em: 23 mai. 2026.

RODRIGUES, Beatriz de Carvalho e Silva Brun. A forma como garantia: uma análise da cadeia de custódia de provas digitais no processo penal brasileiro. 2024. Trabalho de Conclusão

de Curso (Bacharelado em Direito) – Unipampa, Santana do Livramento, 2024. Disponível em: https://repositorio.unipampa.edu.br/items/03bc156e-8a7a-4cf4-a440-9de7ed6472ad. Acesso em: 22 out. 2025.

SILVA, Gheovanna Santos da. Crimes cibernéticos e a inviolabilidade de provas: delimitação de critérios para garantir a integridade da cadeia de custódia no âmbito virtual. 2025. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2025. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/9365. Acesso em: 22 out. 2025.

VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 26 mai. 2026.