REVISTA ELETRÔNICA AMPLAMENTE
v.4, n.4 out/dez. 2025 DOI: 10.47538/RA-2025.V4N4
ISSN: 2965-0003

PERÍCIA CRIMINAL E A INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA PERÍCIA CRIMINAL NA IDENTIFICAÇÃO DE PROVAS AUDIOVISUAIS FALSAS "*DEEPFAKES*"

Rafael Cardoso de Souza
Aluno do curso de Direito da Faculdade de Direito de Varginha – FADIVA.
https://orcid.org/0009-0008-1266-2040
E-mail: 013655@alunos.fadiva.edu.br

Cláudio Vilela Rodrigues
Professor orientador do curso de Direito da Faculdade de Direito de Varginha – FADIVA.
https://orcid.org/0009-0005-7882-7635
E-mail: claudio@fadiva.edu.br

DOI-Geral: http://dx.doi.org/10.47538/RA-2025.V4N4
DOI-Individual: http://dx.doi.org/10.47538/RA-2025.V4N4-18

RESUMO: O avanço das tecnologias de inteligência artificial trouxe benefícios relevantes, mas também inaugurou novas ameaças ao sistema de justiça, sobretudo com a disseminação das *deepfakes*. Essas manipulações digitais, capazes de reproduzir falas e imagens de forma convincente, impactam diretamente a confiabilidade das provas audiovisuais no processo penal. A investigação realizada teve como objetivo geral analisar os desafios enfrentados pela perícia criminal na identificação de provas audiovisuais falsas produzidas por inteligência artificial (*deepfakes*), no contexto jurídico brasileiro. A metodologia adotada consistiu em uma revisão bibliográfica de caráter qualitativo, com consulta a artigos científicos publicados entre 2019 e 2025. A análise demonstrou que a sofisticação das *deepfakes* impõe barreiras técnicas para a detecção de manipulações e evidencia lacunas normativas no ordenamento jurídico, como a ausência de tipificação penal específica e a fragilidade da regulamentação sobre cadeia de custódia digital. Conclui-se que há necessidade urgente de reformas legislativas, padronização de protocolos de análise digital e investimentos contínuos em capacitação técnica, a fim de assegurar maior efetividade da justiça penal diante das inovações tecnológicas.

PALAVRAS-CHAVE: *Deepfakes*. Inteligência artificial. Perícia criminal.

CRIMINALISTICS AND ARTIFICIAL INTELLIGENCE: CHALLENGES FOR CRIMINALISTICS IN IDENTIFYING FALSE AUDIOVISUAL EVIDENCE ("DEEPFAKES")

ABSTRACT: The advancement of artificial intelligence technologies has brought significant benefits but has also introduced new threats to the justice system, particularly with the spread of *deepfakes*. These digital manipulations, capable of convincingly reproducing speech and images, directly impact the reliability of audiovisual evidence in criminal proceedings. The research carried out aimed to analyze the challenges faced by forensic experts in identifying falsified audiovisual evidence produced by artificial intelligence (*deepfakes*) within the Brazilian legal context. The methodology adopted consisted of a qualitative bibliographic review, consulting scientific articles published between 2019 and 2025. The analysis demonstrated that the sophistication of *deepfakes* imposes technical barriers to manipulation detection and highlights normative gaps in the

legal framework, such as the absence of specific criminal typification and the fragility of regulations concerning the digital chain of custody. It is concluded that there is an urgent need for legislative reforms, the standardization of digital analysis protocols, and continuous investment in technical training, in order to ensure greater effectiveness of criminal justice in the face of technological innovations.

KEYWORDS: *Deepfakes*. Artificial intelligence. Forensic expertise.

INTRODUÇÃO

O avanço das tecnologias de inteligência artificial trouxe benefícios inegáveis, mas também inaugurou novos desafios para o campo jurídico, em especial no processo penal. Entre essas inovações, destacam-se os *deepfakes*, capazes de criar conteúdos audiovisuais quase indissociáveis da realidade, o que levanta sérias dúvidas sobre a confiabilidade das provas digitais em juízo. Freitas (2023) observa que tais tecnologias têm potencial de transformar profundamente a dogmática penal, exigindo novos enquadramentos jurídicos e repensando os limites da tipificação de condutas tradicionais à luz da manipulação digital.

Nakanishi (2023) chama atenção para o fato de que os *deepfakes* impactam diretamente o princípio da busca pela verdade real, pedra angular do processo penal brasileiro. A manipulação sofisticada de imagens e áudios pode induzir juízes e jurados ao erro, corroendo a credibilidade de provas historicamente consideradas confiáveis, como vídeos e gravações. Esse cenário exige que a perícia criminal desenvolva novas metodologias de verificação, sob pena de comprometer a legitimidade das decisões judiciais.

Outro aspecto relevante diz respeito à opacidade entre o real e o virtual no campo probatório, apontada por Silva (2024). Para a autora, a dificuldade de se estabelecer a autenticidade de conteúdos digitais cria um ambiente de insegurança jurídica, pois fragiliza a admissibilidade das provas e coloca em risco direitos fundamentais, como o contraditório e a ampla defesa. Diante dessa realidade, surge a tensão entre a necessidade de admitir novas formas de evidência em juízo e a obrigação constitucional de preservar a integridade do devido processo legal.

Dessa forma, discutir os desafios impostos pelos *deepfakes* à perícia criminal não é apenas uma questão técnica, mas uma preocupação que toca diretamente o núcleo da justiça penal. A ausência de regulamentação específica e de protocolos periciais robustos aumenta a vulnerabilidade do sistema diante da manipulação digital, abrindo espaço para nulidades processuais e injustiças. Assim, compreender esse fenômeno no contexto jurídico brasileiro é essencial para proteger a integridade do processo penal, garantir a segurança jurídica e fortalecer a confiança social no Poder Judiciário.

A escolha deste tema se justifica pela crescente utilização de conteúdos audiovisuais manipulados por inteligência artificial e pelo impacto que tais provas podem ter no processo penal brasileiro. A relevância do estudo reside na necessidade de analisar de que forma a perícia criminal pode se adaptar a esse novo contexto, contribuindo para o aperfeiçoamento do sistema probatório e para a preservação das garantias constitucionais. Além disso, trata-se de um tema atual, que reflete um dos maiores desafios contemporâneos para o Direito Penal e Processual Penal.

A partir dessa problemática, formula-se a seguinte questão norteadora: De que maneira a inteligência artificial, por meio das *deepfakes*, desafia a atuação da perícia criminal e a confiabilidade das provas audiovisuais no processo penal brasileiro, e quais são as implicações jurídicas decorrentes desse cenário para a efetividade da justiça?

O objetivo geral deste trabalho é analisar os desafios enfrentados pela perícia criminal na identificação de provas audiovisuais falsas produzidas por inteligência artificial (*deepfakes*), no contexto jurídico brasileiro. Como objetivos específicos, estabelecem-se: investigar as implicações jurídicas da utilização de provas audiovisuais falsas (*deepfakes*) no processo penal brasileiro, considerando a sua autenticidade, validade e admissibilidade; examinar o papel da inteligência artificial na atuação da perícia criminal, considerando as técnicas disponíveis para detecção de manipulações digitais e identificar os principais obstáculos enfrentados pelo ordenamento jurídico brasileiro diante das *deepfakes*.

O presente trabalho adota o método de revisão bibliográfica, de caráter qualitativo, com o objetivo de reunir, analisar a produção acadêmica existente sobre os desafios enfrentados pela perícia criminal na identificação de provas audiovisuais falsas

produzidas por inteligência artificial (*deepfakes*). Esse tipo de pesquisa é possibilita o exame de diferentes perspectivas teóricas e jurídicas já consolidadas, permitindo identificar convergências e lacunas na literatura especializada.

Para a construção do referencial, foram utilizadas bases de dados como SciELO, Google Acadêmico, Portal de Periódicos da CAPES e Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), além de repositórios institucionais de universidades brasileiras. O período de publicações considerado abrange os anos de 2019 a 2025.

As buscas foram realizadas a partir de palavras-chave, como *deepfakes*, inteligência artificial e perícia criminal. O cruzamento dessas expressões resultou na seleção de artigos, dissertações e teses que abordam o fenômeno das *deepfakes* sob a ótica do Direito Penal e Processual Penal, compondo o corpus de análise do presente estudo.

PERÍCIA CRIMINAL E SUA IMPORTÂNCIA NO PROCESSO PENAL

Alves *et al*. (2024) ressaltam que a disseminação das *deepfakes* ampliou a utilização de recursos digitais para a prática criminosa, incluindo a adulteração de provas, a propagação de *fake news* e crimes contra a honra. Nesse contexto, a perícia assume a tarefa de identificar se tais conteúdos se amoldam a tipos penais já previstos, garantindo que a responsabilização não se faça por analogia, mas dentro da legalidade estrita. A dificuldade em rastrear autores de crimes digitais reforça a necessidade de métodos técnicos especializados, que permitam ao Estado identificar e punir condutas ilícitas sem violar garantias fundamentais. A perícia, assim, não se limita a verificar a materialidade, mas atua como instrumento de proteção da própria legitimidade do Direito Penal brasileiro.

A relevância da perícia também se manifesta na preservação da cadeia de custódia das provas digitais. Bellé e Souza (2025) enfatizam que a autenticidade e a integridade da prova devem ser tratadas como condições indispensáveis para sua admissibilidade em juízo. Com a digitalização dos processos, tornou-se imprescindível que peritos criminais dominem ferramentas capazes de detectar manipulações em áudios, vídeos e imagens, evitando presunções de veracidade que comprometam a justiça. A atuação pericial não se restringe à análise técnica, mas envolve também a observância de normas como o Marco

Civil da Internet, a Lei Geral de Proteção de Dados, que orientam a coleta e o tratamento de evidências digitais. Nesse sentido, a perícia não apenas auxilia o juiz, mas assegura que a prova digital cumpra critérios de auditabilidade e repetibilidade, fortalecendo o devido processo penal

O fenômeno das *deepfakes* intensificou os desafios da busca pela verdade processual. Freitas (2023) destaca que a procura da verdade no processo penal já era dificultada por limitações humanas e pela impossibilidade do julgador de presenciar os fatos diretamente. A manipulação de imagens e sons por inteligência artificial agrava esse cenário, tornando necessário o desenvolvimento de métodos forenses específicos que diferenciem o real do fabricado. Nesse contexto, a perícia criminal surge como mecanismo insubstituível, pois possibilita ao juiz formar convicção segura sobre a credibilidade da prova. A análise pericial permite não apenas identificar a adulteração, mas também contextualizar tecnicamente a evidência, fornecendo subsídios objetivos para a decisão judicia

A função da perícia no processo penal não se limita à esfera probatória, mas se estende à proteção de direitos fundamentais. Quando vídeos ou áudios manipulados são introduzidos em juízo, há o risco de violação ao contraditório, à ampla defesa e à presunção de inocência. Alves *et al*. (2024) lembram que a sensação de anonimato na internet e a dificuldade em punir esses crimes incentivam sua prática, exigindo do Estado uma resposta adequada. A perícia criminal, nesse contexto, não apenas identifica a falsidade, mas atua como mecanismo de contenção de injustiças, evitando condenações baseadas em provas frágeis ou fabricadas. É justamente essa função de equilíbrio entre inovação tecnológica e garantias constitucionais que assegura à perícia criminal sua relevância no processo penal contemporâneo

Bellé e Souza (2025) acrescentam que, diante do risco de manipulação digital, não é suficiente confiar na aparência de veracidade das provas audiovisuais. A perícia deve ser chamada a validar sua autenticidade, garantindo que a decisão judicial não se baseie em elementos contaminados por fraudes tecnológicas. A atuação pericial, portanto, representa não apenas um meio de prova, mas uma salvaguarda contra o colapso da confiança social no sistema de justiça. Afinal, um processo penal que admite provas

REVISTA ELETRÔNICA AMPLAMENTE
v.4, n.4 out/dez. 2025 DOI: 10.47538/RA-2025.V4N4
ISSN: 2965-0003

adulteradas compromete a própria função do Estado de aplicar o Direito com legitimidade e justiça.

Freitas (2023) observa que a credibilidade inerente ao que se vê ou ouve é justamente explorada pelas *deepfakes*, tornando-as especialmente perigosas. A perícia, nesse cenário, não deve ser vista apenas como instrumento auxiliar, mas como pilar fundamental da estrutura processual. É a expertise do perito que possibilita ao juiz superar a aparência enganosa das provas digitais e alcançar um juízo de valor seguro sobre sua validade. Nesse sentido, a perícia criminal torna-se uma ponte entre a tecnologia e o Direito, transformando complexas análises técnicas em informações compreensíveis e úteis para o processo.

INTELIGÊNCIA ARTIFICIAL E A PRODUÇÃO DE PROVAS DIGITAIS

A incorporação da inteligência artificial no contexto jurídico tem provocado profundas transformações na maneira como as provas são concebidas, produzidas e avaliadas no processo penal. As ferramentas de manipulação digital, como os *deepfakes*, são um exemplo paradigmático da tensão entre inovação tecnológica e segurança jurídica. No âmbito das provas digitais, essa realidade impõe novos desafios à perícia criminal, que precisa lidar com a autenticidade e a confiabilidade de conteúdos altamente sofisticados e difíceis de detectar. A literatura recente destaca que a manipulação audiovisual representa uma ameaça não apenas à integridade do processo penal, mas também à própria efetividade da justiça, uma vez que a produção de provas adulteradas pode comprometer a busca da verdade real (Silva, 2024).

A problemática das provas digitais se relaciona à admissibilidade processual e à necessidade de critérios técnicos e jurídicos claros que assegurem sua validade. A capacidade das inteligências artificiais de alterar imagens, áudios e vídeos de forma quase indetectável coloca em risco a credibilidade de um dos meios probatórios mais relevantes da atualidade. Nesse contexto, surge a preocupação com a possibilidade de condenações ou absolvições baseadas em evidências forjadas, cenário que exige reflexão doutrinária e respostas normativas mais robustas. O debate acadêmico aponta que, enquanto no passado os registros audiovisuais gozavam de elevada presunção de veracidade,

atualmente eles podem ser construções artificiais que distorcem a realidade dos fatos (Nakanishi, 2023).

Outro ponto central está na atuação da perícia criminal. O avanço da inteligência artificial, ao mesmo tempo que gera novas ameaças, também possibilita a criação de instrumentos de detecção e autenticação de provas digitais. A literatura jurídica ressalta que a perícia se torna elemento indispensável para verificar a integridade de conteúdos audiovisuais e digitais, empregando métodos forenses compatíveis com as manipulações algorítmicas mais sofisticadas. Esse papel ganha relevo diante da crescente utilização de *deepfakes* em contextos políticos, midiáticos e criminais, tornando urgente a atualização das práticas periciais e da legislação aplicável (Sandoval *et al*., 2024).

As implicações jurídicas dessa realidade vão além da esfera técnica. A produção de provas digitais mediada por inteligência artificial desafia princípios fundamentais do processo penal, como a ampla defesa, o contraditório e a presunção de inocência. O ordenamento brasileiro precisa adaptar-se a esse cenário, reconhecendo a vulnerabilidade epistêmica das provas digitais e estabelecendo parâmetros que assegurem sua legitimidade. A doutrina aponta que a ausência de mecanismos adequados de controle pode enfraquecer a confiança social na justiça criminal e comprometer a efetividade da tutela jurisdicional (Freitas, 2023).

Nesse sentido, a produção acadêmica brasileira enfatiza a necessidade de uma abordagem interdisciplinar, que envolva não apenas o direito, mas também áreas como ciência da computação e engenharia forense, no desenvolvimento de métodos de detecção e autenticação de provas digitais. O desafio consiste em equilibrar a inovação tecnológica com a preservação da segurança jurídica, garantindo que os avanços da inteligência artificial sejam utilizados a favor da justiça e não como instrumentos de fraude ou manipulação.

DEEPFAKES: CONCEITO, FUNCIONAMENTO E RISCOS JURÍDICOS

O advento da inteligência artificial trouxe ao cenário contemporâneo um conjunto de inovações capazes de transformar radicalmente a vida em sociedade. Entre essas inovações, destaca-se a tecnologia das *deepfakes*, que se caracteriza pela manipulação de

conteúdos audiovisuais a partir de algoritmos de aprendizado profundo, resultando em produções altamente realistas. Essa tecnologia, embora possua aplicações legítimas, gerou também preocupações crescentes no campo jurídico, sobretudo em relação à confiabilidade das provas no processo penal e às implicações ligadas à privacidade, à honra e à segurança jurídica. O conceito de *deepfake* é central para a compreensão de como a inteligência artificial pode ser usada tanto como ferramenta de inovação quanto como instrumento de fraude e engano, exigindo do Direito respostas eficazes frente a esses novos desafios (Alves *et al*., 2024).

Segundo Fidelis e Soares (2023), as *deepfakes* diferenciam-se de outros mecanismos de manipulação digital por sua sofisticação e pela capacidade de enganar até mesmo observadores experientes. A tecnologia emprega redes neurais artificiais que cruzam e processam grandes volumes de dados, permitindo a criação de áudios e vídeos que replicam características pessoais de forma quase indistinguível da realidade. Essa sofisticação traz riscos diretos à produção e à avaliação das provas digitais, pois rompe com a presunção de autenticidade antes atribuída a registros audiovisuais. No contexto jurídico, essa quebra de confiança compromete a estabilidade do processo penal e exige da perícia criminal instrumentos cada vez mais avançados de verificação da autenticidade.

Oliveira e Costa (2022) apontam que, do ponto de vista técnico, o funcionamento das *deepfakes* está associado ao uso de técnicas de *machine learning*, como os *Generative Adversarial Networks* (GANs), que funcionam em um processo de competição entre duas redes neurais: uma responsável por gerar imagens falsas e outra por identificar inconsistências. Esse processo iterativo resulta em vídeos e áudios progressivamente mais realistas, tornando a detecção extremamente desafiadora. Para o Direito, compreender esse funcionamento é essencial, pois a sofisticação técnica impacta diretamente a admissibilidade e a validade das provas digitais, criando um cenário em que a simples análise visual ou auditiva já não é suficiente para identificar manipulações.

O risco jurídico mais evidente associado às *deepfakes* está na possibilidade de uso fraudulento para a produção de provas falsas em processos judiciais. Siqueira e Andrade (2024) destacam que o ordenamento jurídico brasileiro enfrenta dificuldades em lidar com esse tipo de manipulação, sobretudo pela ausência de legislação específica que discipline a criação e o compartilhamento desses conteúdos. O uso indevido de *deepfakes*

pode afetar direitos fundamentais como a imagem, a privacidade e a honra, além de potencialmente ensejar responsabilização criminal. A manipulação de vídeos e áudios não apenas compromete a verdade processual, mas também agrava problemas já existentes relacionados à desinformação e à pós-verdade.

Alves *et al*. (2024) ressaltam que, ao se inserir no contexto da persecução penal, as *deepfakes* ampliam as dificuldades já enfrentadas pela perícia criminal na coleta e análise de provas digitais. O anonimato proporcionado pelo ambiente virtual, aliado à complexidade das técnicas de manipulação, dificulta a identificação dos responsáveis pela produção e difusão de conteúdos falsos. Essa situação levanta debates sobre a necessidade de atualizar as tipificações penais existentes, de forma a incluir condutas que envolvam diretamente a criação e o compartilhamento de *deepfakes*. Para além disso, há a necessidade de consolidar protocolos de perícia digital que garantam a integridade da cadeia de custódia e a confiabilidade das evidências apresentadas em juízo.

Fidelis e Soares (2023) destacam ainda que o impacto das *deepfakes* não se restringe ao processo penal, mas alcança também esferas civis, como a proteção da honra e da imagem, além de questões eleitorais e políticas. A possibilidade de manipulação de discursos de figuras públicas, por exemplo, pode comprometer o processo democrático, influenciando a opinião pública com base em informações falsas. Assim, os riscos jurídicos relacionados às *deepfakes* extrapolam o campo estritamente probatório e se relacionam diretamente com a manutenção da ordem democrática e da segurança coletiva.

Oliveira e Costa (2022) reforçam que a complexidade tecnológica das *deepfakes* coloca em xeque a capacidade do sistema de justiça em acompanhar a velocidade da inovação. O ordenamento jurídico, ao lidar com inovações disruptivas, enfrenta o desafio de criar respostas normativas que sejam suficientemente abrangentes para lidar com situações novas, mas também específicas para garantir segurança jurídica. A lacuna normativa quanto às *deepfakes* gera incertezas e pode abrir espaço para decisões judiciais conflitantes, fragilizando a uniformidade da jurisprudência e comprometendo a confiança no Judiciário.

Siqueira e Andrade (2024) observam que a proteção da privacidade constitui um dos maiores desafios trazidos pelas *deepfakes*. A facilidade com que imagens pessoais

disponíveis na internet podem ser apropriadas e manipuladas para a criação de conteúdos enganosos representa um grave risco à dignidade humana. Além disso, a popularização de aplicativos que permitem a criação de *deepfakes* por qualquer usuário amplia as possibilidades de violações em larga escala, tornando urgente a criação de mecanismos de regulação e responsabilização tanto no âmbito civil quanto no penal.

No plano internacional, Sandoval *et al*. (2024) destacam que o sistema de justiça criminal global enfrenta os mesmos dilemas. A manipulação digital desafia os métodos tradicionais de coleta e análise de provas, exigindo a adoção de tecnologias de detecção mais sofisticadas e a capacitação constante dos peritos criminais. A revisão sistemática conduzida pelos autores demonstra que os riscos das *deepfakes* são reconhecidos em diversos países e que as soluções adotadas envolvem não apenas reformas legislativas, mas também estratégias de cooperação entre governos, empresas de tecnologia e instituições acadêmicas.

No Brasil, o debate ainda se encontra em fase inicial, mas já se percebe a necessidade de articulação entre diferentes áreas do Direito para enfrentar os riscos trazidos pelas *deepfakes*. Alves *et al*. (2024) apontam que a responsabilização criminal de criadores e difusores desses conteúdos deve ser pensada à luz dos princípios constitucionais, evitando soluções que comprometam a liberdade de expressão ou gerem censura prévia. Nesse cenário, o papel da perícia criminal e da doutrina jurídica é central para equilibrar a proteção dos direitos fundamentais com a preservação da ordem pública.

IMPLICAÇÕES JURÍDICAS DA UTILIZAÇÃO DE PROVAS AUDIOVISUAIS FALSAS

Freitas (2023) analisa que a prova digital, que em princípio representava avanço no campo da persecução penal, agora pode se tornar fonte de insegurança quando manipulada por inteligência artificial. A dificuldade em identificar adulterações compromete princípios constitucionais, como o contraditório e a ampla defesa, previstos no artigo 5º da Constituição Federal de 1988. A introdução de vídeos e áudios falsos em processos judiciais tem o potencial de induzir julgadores a erro, gerar nulidades processuais e colocar em risco a liberdade dos acusados. A perícia criminal assume função

essencial nesse contexto, mas exige atualização constante de técnicas e ferramentas para enfrentar manipulações digitais cada vez mais sofisticadas.

Nakanishi (2023) aponta que a legislação processual brasileira ainda não foi estruturada para lidar com conteúdos produzidos ou adulterados por inteligência artificial. O Código Penal (Decreto-Lei nº 2.848/1940) e o Código de Processo Penal (Decreto-Lei nº 3.689/1941) regulam aspectos gerais da responsabilização criminal e da admissibilidade da prova, mas não contemplam a complexidade das manipulações digitais. A autora identifica um vácuo normativo que gera insegurança para juízes e peritos, que precisam decidir sobre a validade das provas sem parâmetros específicos. Essa lacuna amplia o risco de decisões contraditórias e fragiliza a uniformidade da jurisprudência.

Oliveira e Costa (2022) destacam que a força probatória das gravações audiovisuais sempre se vinculou à sua aparência de neutralidade. A tecnologia das *deepfakes* rompe com essa premissa, pois torna possível a criação de registros falsificados que imitam com precisão a realidade. A legislação brasileira atual apresenta dispositivos relevantes, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), que tipifica delitos informáticos relacionados à invasão de dispositivos, e a Lei nº 12.735/2012, que trata da responsabilização de provedores quanto a crimes cibernéticos. Contudo, essas normas não abrangem de forma adequada a produção e disseminação de conteúdos falsificados com recursos de inteligência artificial, revelando uma defasagem regulatória.

Pedrina (2019) ressalta que a utilização de tecnologias no processo penal não deve ser vista como neutra. A aplicação de inteligência artificial à produção de provas pode introduzir vieses e manipulações que afetam diretamente a confiabilidade dos resultados. No âmbito do direito penal, admitir provas manipuladas por algoritmos sem mecanismos eficazes de verificação viola o devido processo legal e a presunção de inocência, princípios constitucionais que estruturam a atuação do Judiciário. A análise crítica é indispensável para que se evite o uso acrítico de tecnologias que, ao invés de apoiar a justiça, podem distorcê-la.

Silva (2024) examina a incerteza criada pela ausência de regulamentação específica sobre manipulações digitais. O Marco Civil da Internet (Lei nº 12.965/2014) e

a Lei Geral de Proteção de Dados (LGPD) lei nº 13.709/2018, representam avanços ao disciplinarem princípios sobre o uso da rede e a proteção de dados pessoais. Contudo, não fornecem soluções completas para o problema das provas falsas. O Marco Civil estabelece normas de responsabilidade para provedores e proteção de direitos fundamentais online, enquanto a LGPD assegura direitos relacionados ao tratamento de dados pessoais. Nenhuma dessas legislações, porém, enfrenta de forma direta a questão da adulteração de áudios e vídeos utilizados como prova em processos criminais.

Siqueira e Andrade (2024) abordam as repercussões das manipulações digitais no campo civil e constitucional, salientando que a utilização indevida de imagens e vídeos pode violar o direito à imagem e à privacidade. A Lei nº 9.610/1998, que trata dos direitos autorais, protege contra a reprodução não autorizada de obras e imagens, enquanto a Lei nº 13.718/2018 tipifica crimes contra a dignidade sexual, incluindo a divulgação não consentida de imagens íntimas. Quando esses recursos são empregados em contexto probatório, as implicações jurídicas se multiplicam, pois o mau uso da tecnologia pode afetar diretamente a liberdade dos acusados e a proteção da dignidade das vítimas.

As implicações jurídicas da utilização de provas audiovisuais falsas envolvem três eixos centrais. O primeiro refere-se à validade da prova penal, já que manipulações audiovisuais colocam em risco a busca pela verdade real. O segundo está ligado à responsabilização dos agentes que produzem e difundem conteúdos falsos. O Código Penal e as legislações cibernéticas fornecem alguns mecanismos, mas não regulam de forma suficiente as condutas associadas às *deepfakes*. O terceiro eixo diz respeito à necessidade de atualização legislativa, que deve integrar os avanços tecnológicos com os princípios constitucionais que regem o processo penal brasileiro.

DESAFIOS PARA A PERÍCIA CRIMINAL NA IDENTIFICAÇÃO DE CONTEÚDOS MANIPULADOS

Bellé e Souza (2025) ressaltam que o processo penal brasileiro sempre atribuiu elevado valor às provas digitais, sobretudo aquelas de natureza audiovisual, em razão de sua capacidade de reproduzir de forma mais próxima a realidade dos fatos. Contudo, esse prestígio tradicional encontra limites na era da inteligência artificial. A sofisticação das

manipulações digitais coloca em dúvida a veracidade das evidências e amplia o risco de condenações injustas. O desafio para os peritos é identificar com precisão as alterações introduzidas, tarefa que se torna cada vez mais complexa diante do avanço das técnicas de aprendizado profundo aplicadas à produção de falsificações.

Fidelis e Soares (2023) observam que o ordenamento jurídico brasileiro carece de dispositivos específicos para lidar com a manipulação de conteúdos digitais em ambiente processual. O Código de Processo Penal não dispõe de normas claras sobre a admissibilidade de provas produzidas por inteligência artificial, e o Código Penal não tipifica de modo direto condutas relacionadas à criação e difusão de *deepfakes*. Embora existam leis como o Marco Civil da Internet (Lei nº 12.965/2014) e a LGPD (Lei nº 13.709/2018), sua aplicação ainda se mostra limitada quando a questão envolve adulteração probatória. A perícia, portanto, precisa atuar em um cenário jurídico fragmentado, sem instrumentos normativos capazes de orientar de maneira uniforme a avaliação de provas manipuladas.

Freitas (2023) analisa que a função da perícia, neste contexto, não se resume à análise técnica de arquivos digitais. É necessário compreender o impacto que as manipulações exercem sobre o devido processo legal, a ampla defesa e o contraditório, princípios constitucionais previstos no artigo 5º da Constituição Federal. A dificuldade em distinguir entre registros autênticos e adulterados compromete a paridade de armas entre acusação e defesa, já que uma prova falsificada pode induzir o magistrado ao erro ou prolongar indevidamente o processo em razão da necessidade de contraprovas. O perito, nesse cenário, atua como peça-chave na proteção dos direitos fundamentais.

Nakanishi (2023) destaca que os desafios enfrentados pela perícia criminal na identificação de conteúdos manipulados não se restringem ao campo técnico. Existe um déficit normativo que agrava as dificuldades práticas. O Código Penal (Decreto-Lei nº 2.848/1940) tipifica condutas como falsidade documental, mas não alcança a complexidade das adulterações digitais geradas por inteligência artificial. Situação semelhante ocorre com a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que prevê punições para crimes informáticos relacionados à invasão de dispositivos, mas não disciplina de forma específica a criação de conteúdos digitais falsificados. Essa

ausência de normas claras repercute diretamente na atuação pericial, que precisa fundamentar tecnicamente suas conclusões sem apoio legislativo específico.

Oliveira e Costa (2022) enfatizam que a credibilidade das provas audiovisuais sempre se apoiou em sua aparência de neutralidade. A manipulação promovida pelas *deepfakes* rompe esse paradigma, ao permitir a produção de registros que imitam com precisão a fala e os gestos de pessoas reais. A perícia, que antes podia se concentrar na verificação de metadados ou na identificação de edições mais simples, agora enfrenta falsificações que exigem técnicas avançadas de análise forense. O uso de inteligência artificial para detectar manipulações é uma resposta promissora, mas que também gera questionamentos sobre a confiabilidade dos próprios algoritmos empregados.

Outro desafio relevante consiste na rapidez com que novas técnicas de adulteração surgem. A cada avanço no campo da detecção, há o desenvolvimento de métodos capazes de contornar os mecanismos existentes. Isso coloca a perícia em posição reativa, sempre correndo atrás das inovações tecnológicas utilizadas para burlar a verificação. Esse cenário cria um ciclo de constante adaptação, no qual a atualização de ferramentas e a capacitação dos peritos tornam-se imprescindíveis. Sem esses investimentos, a perícia corre o risco de se tornar obsoleta frente a técnicas de falsificação em rápida evolução (Bellé; Souza, 2025).

O contexto processual reforça a complexidade do tema. Uma prova audiovisual manipulada, se admitida sem a devida verificação, pode gerar condenações injustas ou absolvições indevidas, ferindo princípios basilares da justiça penal. A necessidade de garantir a integridade do processo exige que a perícia criminal seja valorizada como mecanismo de controle, evitando que manipulações tecnológicas comprometam a função jurisdicional. A jurisprudência brasileira, embora ainda incipiente, tem reconhecido a importância de submeter provas digitais a exames periciais aprofundados, justamente para evitar a fragilização do processo penal (Fidelis; Soares, 2023).

Os peritos enfrentam ainda obstáculos práticos relacionados à cadeia de custódia da prova digital. Qualquer falha na preservação de arquivos pode comprometer a credibilidade do laudo pericial e abrir margem para alegações de manipulação. A Lei nº 13.964/2019, conhecida como “Pacote Anticrime”, trouxe dispositivos relevantes sobre a

cadeia de custódia no processo penal, mas sua aplicação ao ambiente digital ainda é objeto de debate. A adaptação de tais normas para provas audiovisuais adulteradas por inteligência artificial é um campo que exige desenvolvimento doutrinário e jurisprudencial.

Freitas (2023) argumenta que a perícia precisa assumir também uma função pedagógica, ao esclarecer aos magistrados e às partes a natureza das manipulações digitais e as limitações dos métodos de detecção. Sem essa mediação, há risco de decisões equivocadas baseadas em percepções subjetivas da veracidade de vídeos e áudios. Essa função didática não significa ultrapassar os limites técnicos da perícia, mas sim fornecer subsídios claros para que os julgadores compreendam a complexidade envolvida na análise de provas digitais manipuladas.

Nakanishi (2023) reforça que a construção de um marco normativo específico é indispensável para que a atuação pericial seja fortalecida. Enquanto o legislador não oferecer regras claras, caberá à perícia preencher lacunas com relatórios técnicos baseados em métodos científicos atualizados. Essa situação gera insegurança, pois as conclusões podem variar conforme a instituição ou os recursos disponíveis, criando desigualdades entre processos conduzidos em diferentes regiões do país.

O enfrentamento dessas dificuldades exige uma abordagem integrada. É necessário investir em pesquisa e inovação no campo da ciência forense digital, garantindo que os peritos tenham acesso a tecnologias capazes de identificar manipulações com precisão. É igualmente essencial que o legislador avance na construção de normas específicas que contemplem a complexidade das provas digitais adulteradas.

OBSTÁCULOS NORMATIVOS E LACUNAS DO ORDENAMENTO JURÍDICO BRASILEIRO

Freitas (2023) analisa que, embora a Constituição Federal de 1988 estabeleça princípios fundamentais como o devido processo legal, o contraditório e a ampla defesa, não existem parâmetros normativos específicos que regulem a produção, a validade e a admissibilidade de provas digitais manipuladas. A ausência de tais diretrizes abre espaço

para interpretações divergentes e decisões judiciais pouco uniformes, além de permitir que conteúdos adulterados possam ter repercussão prática antes mesmo da devida análise pericial. Nesse cenário, a atuação da perícia criminal assume papel central, mas suas conclusões técnicas enfrentam insegurança quanto ao respaldo normativo.

No campo infraconstitucional, o Código Penal (Decreto-Lei nº 2.848/1940) e o Código de Processo Penal (Decreto-Lei nº 3.689/1941) não contêm dispositivos específicos voltados à manipulação de imagens e áudios digitais. Condutas relacionadas à falsidade documental ou ideológica (arts. 297 a 304 e art. 299 do Código Penal) foram elaboradas em contexto analógico, o que dificulta a sua aplicação direta às adulterações digitais. Fidelis e Soares (2023) observam que a falta de tipificação clara torna complexo enquadrar juridicamente os criadores e difusores de *deepfakes*, obrigando operadores do direito a recorrerem a interpretações extensivas ou a tipos penais que não contemplam a especificidade da conduta.

Pedrina (2019) aponta que o problema não se restringe à tipificação. Questões práticas como a preservação da cadeia de custódia das provas digitais também carecem de normatização clara. A Lei nº 13.964/2019, conhecida como "Pacote Anticrime", trouxe importantes disposições sobre a cadeia de custódia, mas não detalhou procedimentos aplicáveis às provas digitais complexas. A ausência de critérios específicos enfraquece a credibilidade do laudo pericial, abrindo margem para alegações de contaminação ou adulteração da prova ao longo do processo. Essa fragilidade compromete a confiança no trabalho pericial e na própria instrução criminal.

Robles-Lessa e Cabral (2020) enfatizam que a manipulação de imagens e vozes por inteligência artificial ameaça diretamente direitos fundamentais como a dignidade da pessoa humana, a privacidade e a honra. Contudo, não há no Código Penal uma tipificação que contemple de forma específica a criação e a disseminação de *deepfakes*. A Lei nº 12.737/2012, chamada Lei Carolina Dieckmann, aborda a invasão de dispositivos eletrônicos, mas não contempla a manipulação de conteúdos digitais. Essa lacuna normativa expõe a vulnerabilidade dos indivíduos e deixa a justiça criminal desprovida de instrumentos claros para responsabilizar os agentes que produzem e utilizam conteúdos adulterados em contextos probatórios.

REVISTA ELETRÔNICA AMPLAMENTE
v.4, n.4 out/dez. 2025 DOI: 10.47538/RA-2025.V4N4
ISSN: 2965-0003

Sandoval *et al*. (2024) observam que o desafio normativo não é exclusivo do Brasil, mas uma dificuldade comum a diversos países que também lidam com a disseminação de *deepfakes*. A diferença está na celeridade com que outros ordenamentos têm debatido e elaborado legislações específicas, ao passo que no Brasil o tema ainda é tratado de forma fragmentada. A morosidade legislativa nacional amplia a distância entre a evolução tecnológica e a proteção jurídica, o que deixa a perícia criminal em posição desvantajosa, forçada a lidar com complexas manipulações digitais sem apoio normativo proporcional.

A análise também deve contemplar normas mais recentes relacionadas ao ambiente digital, como o Marco Civil da Internet (Lei nº 12.965/2014). Essa legislação é relevante por disciplinar direitos e deveres no uso da internet, mas, como observa Nakanishi (2023), sua preocupação central está na guarda de registros e na responsabilização de provedores. O artigo 19, que condiciona a retirada de conteúdos à ordem judicial, mostra-se incompatível com a velocidade da circulação de *deepfakes*, que podem causar danos à reputação ou influenciar processos penais antes da análise pericial.

A LGPD (Lei nº 13.709/2018) também se mostra pertinente, pois a utilização indevida de imagens e vozes sem autorização do titular constitui violação a dados pessoais. Siqueira e Andrade (2024) apontam que, embora a LGPD traga mecanismos de proteção civil e administrativa, ela não resolve a problemática penal, tampouco estabelece critérios sobre a admissibilidade de provas adulteradas no processo. A lei opera como instrumento de prevenção e responsabilização no âmbito civil, mas não fornece soluções específicas para a utilização de *deepfakes* em litígios criminais.

Silva (2024) acrescenta que a ausência de normas claras sobre provas digitais repercute em diferentes esferas do direito, mas seus impactos são especialmente graves no campo penal, onde a busca pela verdade real é princípio estruturante. A insegurança normativa leva a decisões judiciais contraditórias e aumenta o risco de condenações ou absolvições baseadas em provas de autenticidade duvidosa. A falta de regulamentação específica, portanto, compromete não apenas a atuação da perícia criminal, mas a própria legitimidade do processo penal.

Robles-Lessa e Cabral (2020) reforçam que a ausência de políticas públicas voltadas ao enfrentamento das *deepfakes* amplia a sobrecarga sobre a perícia criminal. Em vez de atuar amparada por diretrizes claras, a perícia precisa preencher lacunas legais com relatórios técnicos, cujas conclusões podem variar de acordo com os recursos disponíveis ou a interpretação dos peritos. Essa disparidade gera desigualdade entre processos e fragiliza a uniformidade de julgados. A regulação normativa, portanto, é indispensável para equilibrar o peso entre a inovação tecnológica e a proteção jurídica.

A superação desses desafios exige reformas legislativas que contemplem de forma específica as particularidades das provas digitais manipuladas. É necessário que o legislador avance na criação de tipos penais adequados, que garantam a responsabilização de quem cria e difunde *deepfakes*, bem como na elaboração de normas processuais que disciplinem a cadeia de custódia e a admissibilidade de tais provas. Ao mesmo tempo, é fundamental fortalecer a atuação da perícia criminal, garantindo acesso a recursos tecnológicos de ponta e formação contínua, de modo a reduzir a distância entre a sofisticação das manipulações digitais e a capacidade de detecção.

CONCLUSÃO

A investigação permitiu compreender, com base nos objetivos propostos, os limites enfrentados pela perícia criminal diante de provas audiovisuais falsas produzidas por inteligência artificial. Evidenciou-se que a sofisticação das *deepfakes* compromete a confiabilidade do processo penal e revela insuficiências do ordenamento jurídico quanto à autenticidade e à admissibilidade dessas provas. Verificou-se, ainda, que a perícia desempenha papel decisivo para preservar a integridade da instrução, embora atue em ambiente marcado por lacunas normativas que dificultam a plena efetividade da justiça.

A questão-problema foi respondida, pois ficou demonstrado de que modo a produção e a disseminação de *deepfakes* desafiam a atuação pericial ao elevar o grau de complexidade na verificação de autoria, integridade, cadeia de custódia e rastreabilidade, com reflexos diretos na confiabilidade das evidências audiovisuais. Também se esclareceu quais implicações jurídicas decorrem desse cenário: tensão sobre o devido processo legal, riscos à ampla defesa e ao contraditório, incerteza na valoração probatória

e necessidade de critérios técnicos e processuais atualizados para evitar decisões baseadas em material de autenticidade duvidosa. Assim, a análise expôs o nexo entre os obstáculos técnicos de detecção e as lacunas legislativas que dificultam respostas céleres e uniformes no âmbito penal. Confirma-se que o objetivo geral foi plenamente alcançado, uma vez que foram identificadas e discutidas as barreiras práticas e jurídicas que permeiam a identificação de conteúdos adulterados e seu impacto na efetividade do processo penal.

Recomenda-se avançar em reformas legislativas específicas para provas digitais manipuladas, padronizar protocolos nacionais de verificação e de cadeia de custódia, investir na capacitação contínua de peritos e operadores do direito e estimular pesquisas aplicadas que validem métodos de detecção, estabeleçam parâmetros de qualidade para laudos e avaliem empiricamente a eficácia das soluções adotadas. Esses passos tendem a fortalecer a confiança nas provas, reduzir a margem de erro decisório e alinhar a resposta jurídica ao ritmo de evolução tecnológica.

REFERÊNCIAS

ALVES, B. M.; ARAÚJO, A. K. V.; CAVALCANTE, J. F.; GALDINO JÚNIOR, F. E.; RODRIGUES, L. H. L.; OLIVEIRA, P. H. S. de. Análise da responsabilização criminal dos criadores e propagadores de “deep fakes” no ordenamento jurídico brasileiro. **Caderno Pedagógico**, *[S. l.]*, v. 21, n. 6, p1-33, 2024. Disponível em: https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348. Acesso em:18 set. 2025.

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, p.48-60, 2025. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/184/142. Acesso em: 18 set. 2025.

FIDELIS, V. C.; SOARES, D. V. OS desafios do ordenamento jurídico brasileiro frente às *deepfakes*. **Revista Pensamento Jurídico**, v. 17, n. 1, p. 1-40, 2023. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/711. Acesso em: 18 set. 2025.

FREITAS, Pedro Miguel. *Deepfakes*, conteúdo gerado por inteligência artificial e verdade processual. In: **El proceso penal ante una nueva realidad tecnológica europea**. Thomson Reuters Aranzadi, 2023. p. 195-205. Disponível em: https://dialnet.unirioja.es/descarga/articulo/8857600.pdf. Acesso em: 15 set. 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. Tese de Direito - Centro Universitário de Brasília – UniCEUB. Brasília, 2023. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/17157/1/22001667.pdf. Acesso em: 15 set. 2025.

OLIVEIRA, Pedro Enrico de; COSTA, Rafael Lima da. **Ensaio sobre o uso de deepfake no processo criminal: possíveis riscos e soluções**. [S.l.: s.n.], 2022. Disponível em: https://www.enfam.jus.br/wp-content/uploads/2022/01/DIG_ENSAIO-SOBRE-O-USO-DE-DEEPFAKE-NO-PROCESSO-CRIMINAL-possi%CC%81veis-riscos-e-soluc%CC%A7o%CC%83es.pdf. Acesso em: 18 set. 2025.

PEDRINA, G. M. L. Consequências e perspectivas da aplicação de inteligência artificial a casos penais. **Revista Brasileira de Direito Processual Penal**, v. 5, n. 3, p. 1589-1606, 2019. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/265. Acesso em: 17set. 2025.

ROBLES-LESSA, M. M.; CABRAL, H. L. T. B. Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço. **Revista Derecho y Cambio Social**, n. 61, p. 475-487, 2020. Disponível em: https://dialnet.unirioja.es/descarga/articulo/7525024.pdf. Acesso em: 17set. 2025.

SANDOVAL, Maria-Paz; VAU, Maria de Almeida; SOLAAS, John; RODRIGUES, Luano. Threat of *deepfakes* to the criminal justice system: a systematic review. **Crime Science**, [S.l.], v.13, n.1, p.1-16, 2024. Disponível em: https://link.springer.com/article/10.1186/s40163-024-00239-1. Acesso em: 18 set. 2025.

SILVA, A. M. Inteligência artificial e a validade das provas no processo penal: deepfake e a insegurança causada pela opacidade entre o real e o virtual. **Portal de Trabalhos Acadêmicos**, *[S. l.]*, v. 16, n. 1, 2024. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/3080. Acesso em: 15 set. 2025.

SIQUEIRA, Mariana; ANDRADE, Ester Jerônimo. Deepfake e privacidade: uma análise jurídica sobre manipulação de imagens por usuários. **Revista Focus**, v. 17, nº. 8, p.1-34, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/download/5679/4216. Acesso em: 18 set. 2025.

Submissão: julho de 2025. Aceite: agosto de 2025. Publicação: novembro de 2025.