REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

DEEPFAKES, INTELIGÊNCIA ARTIFICIAL E BLOCKCHAIN NA PROVA PENAL: A (RE)CONSTRUÇÃO DA CONFIABILIDADE PROBATÓRIA NA ERA DIGITAL

DEEPFAKES, ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN IN CRIMINAL EVIDENCE: THE (RE)CONSTRUCTION OF EVIDENTIARY RELIABILITY IN THE DIGITAL AGE

Ciências Sociais Aplicadas • 18/06/2026

REGISTRO DOI: 10.70773/revistatopicos/781737566

Gustavo Henrique de Andrade Cordeiro[1]

Rodrigo Murad Vitoriano[2]

RESUMO

A maturação da inteligência artificial generativa converteu a falsificação audiovisual realista em capacidade amplamente disponível, ameaçando a confiabilidade da prova digital no processo penal. O estudo analisa o impacto dos deepfakes sobre a admissibilidade e a valoração das evidências eletrônicas e examina as salvaguardas tecnológicas de integridade, em especial a função de hash, o registro em blockchain e a certificação por carimbo de tempo. Recorre-se ao direito comparado, com destaque para o dever de transparência do Regulamento (UE) 2024/1689 e para a autenticação por certificação das Federal Rules of Evidence norte-americanas. Adota-se o método dedutivo, com pesquisa bibliográfica, documental e normativa. Conclui-se que a resposta adequada combina padronização técnica da cadeia de custódia, capacitação interdisciplinar e regulação, de modo a reconstruir a confiabilidade probatória sem sacrificar garantias.

Palavras-chave: Deepfake; Inteligência artificial; Blockchain; Cadeia de custódia digital; Confiabilidade probatória.

ABSTRACT

The maturation of generative artificial intelligence has turned realistic audiovisual forgery into a widely available capability, threatening the reliability of digital evidence in criminal proceedings. This study analyzes the impact of deepfakes on the admissibility and assessment of electronic evidence and examines the technological integrity safeguards, in particular hash functions, blockchain recording and time-stamp certification. Comparative law is invoked, with emphasis on the transparency duty of Regulation (EU) 2024/1689 and on the certification-based authentication of the United States Federal Rules of Evidence. The deductive method is adopted, with bibliographic, documentary and normative research.

It concludes that the adequate response combines technical standardization of the chain of custody, interdisciplinary training and regulation, so as to reconstruct evidentiary reliability without sacrificing safeguards.
Keywords: Deepfake; Artificial intelligence; Blockchain; Digital chain of custody; Evidentiary reliability.

1. INTRODUÇÃO

Durante grande parte da história do processo, a imagem e o som funcionaram como âncoras de certeza. Uma fotografia, uma gravação de voz ou um vídeo gozavam de presunção quase intuitiva de correspondência com a realidade, pois a falsificação convincente exigia recursos técnicos raros e dispendiosos. A inteligência artificial generativa dissolveu essa presunção. Hoje, ferramentas acessíveis produzem rostos, vozes e cenas inteiramente sintéticas com grau de realismo que desafia a percepção humana, instaurando uma crise de confiabilidade que atinge o coração da prova digital.

Os deepfakes, vídeos, áudios e imagens gerados ou manipulados por algoritmos de aprendizado profundo, deixaram de ser curiosidade tecnológica para tornar-se risco concreto à administração da justiça criminal. Se uma confissão em vídeo, um áudio comprometedor ou uma fotografia podem ser fabricados com verossimilhança, o sistema de justiça depara-se com problema inédito: como distinguir o registro autêntico do artificial quando a inspeção sensorial já não basta? A pergunta não é hipotética, pois casos de uso malicioso da síntese audiovisual multiplicam-se em escala global.

O problema de pesquisa que orienta este estudo pode ser assim enunciado: diante da capacidade de falsificação propiciada pela inteligência artificial generativa, quais salvaguardas técnicas e jurídicas são aptas a preservar a confiabilidade da prova digital no processo penal brasileiro, e em que medida o direito comparado oferece parâmetros úteis a essa reconstrução? Trata-se de questão que articula dogmática processual, ciências da computação e teoria da regulação.

O objetivo geral consiste em analisar criticamente as ameaças que a síntese audiovisual e a manipulação algorítmica representam para a prova penal e as respostas tecnológicas e normativas disponíveis para enfrentá-las. Os objetivos específicos compreendem caracterizar os deepfakes e seu potencial de fraude probatória; examinar as salvaguardas criptográficas de integridade, em especial hash, blockchain e certificação; e investigar caminhos de padronização, capacitação e regulação, à luz da experiência europeia e norte-americana.

Quanto à metodologia, adota-se o método dedutivo, partindo de premissas gerais sobre teoria da prova e confiabilidade probatória para alcançar conclusões específicas sobre o tratamento das evidências em ambiente de inteligência artificial. A pesquisa é bibliográfica, documental e normativa, de natureza exploratória, e recorre a legislação nacional e estrangeira, normas técnicas internacionais, doutrina qualificada e precedentes dos tribunais superiores, tomados de modo crítico e contextualizado.

O primeiro eixo expõe a ameaça. Examina o conceito de confiabilidade probatória, descreve a técnica e a tipologia dos deepfakes e analisa o dever de transparência consagrado no

Regulamento (UE) 2024/1689, que impõe a marcação do conteúdo sintético e oferece parâmetro relevante ao debate brasileiro sobre a identificação da prova manipulada.

O segundo eixo apresenta as salvaguardas. Detalha o funcionamento da função de hash como verificador de integridade, discute o potencial e os limites do registro em blockchain para a cadeia de custódia e analisa a certificação digital e o carimbo de tempo como infraestrutura de confiança apta a vincular um arquivo a um instante determinado e a uma origem verificável.

O terceiro eixo propõe respostas institucionais. Discute a padronização da cadeia de custódia digital por normas técnicas, a necessidade de capacitação interdisciplinar de peritos e operadores e os caminhos de regulação, com a defesa de uma cultura de integridade probatória que não se reduza ao formalismo nem ceda à ilusão de que a tecnologia, por si só, resolve problemas que são, em última análise, jurídicos e institucionais.

2. A PROVA DIGITAL AMEAÇADA: DEEPFAKES E INTELIGÊNCIA ARTIFICIAL GENERATIVA

2.1. Confiabilidade Probatória e a Virada da Inteligência Artificial Generativa

A confiabilidade é atributo central de qualquer prova. No processo penal, ela condiciona tanto a admissibilidade quanto a valoração, pois apenas o elemento cuja correspondência com a realidade possa ser controlada serve à reconstrução dos fatos e à formação legítima do convencimento. Badaró (2021) sublinha que a prova técnica, por escapar ao conhecimento ordinário do julgador, exige métodos que assegurem sua fidedignidade, sob pena de converter a decisão em

ato de fé. No ambiente digital, essa exigência é potencializada pela facilidade de manipulação dos registros.

A inteligência artificial generativa introduz uma ruptura qualitativa. Até recentemente, a manipulação audiovisual sofisticada demandava perícia, tempo e equipamento, o que limitava sua disseminação e facilitava sua detecção. Modelos de aprendizado profundo inverteram essa equação: a síntese realista de imagem, voz e vídeo tornou-se acessível, rápida e barata. O resultado é que a presunção tácita de autenticidade que acompanhava a evidência audiovisual perdeu fundamento, exigindo do processo penal um deslocamento do paradigma da percepção para o paradigma da verificação técnica.

Esse deslocamento tem consequências dogmáticas precisas. Se antes a impugnação de um vídeo ou áudio era ônus excepcional, hoje a possibilidade de falsificação convincente recomenda que a confiabilidade seja demonstrada de modo afirmativo sempre que o elemento for central à imputação. Lopes Jr. (2023) recorda que o standard probatório no processo penal é elevado, exigindo certeza para além de dúvida razoável, e que a dúvida sobre a genuinidade de uma prova reverte em favor do acusado. A síntese algorítmica, ao multiplicar as fontes de dúvida razoável, fortalece, e não enfraquece, a exigência de verificação.

Convém precisar que o problema não é apenas o do falso positivo, a prova fabricada apresentada como autêntica, mas também o do falso negativo, a prova autêntica desacreditada sob a alegação de que poderia ter sido sintetizada. Esse segundo efeito, por vezes designado dividendo do mentiroso, permite que o autor de uma conduta registrada negue a autenticidade do registro genuíno,

explorando a desconfiança generalizada criada pela própria existência dos deepfakes. A reconstrução da confiabilidade probatória deve, portanto, responder a um duplo desafio: impedir que o falso seja admitido e evitar que o verdadeiro seja indevidamente descartado.

A resposta a esse duplo desafio não pode ser a rejeição indiscriminada da prova digital, que inviabilizaria a persecução em uma sociedade cuja vida se desenrola em meios eletrônicos, nem a sua aceitação acrítica, que abriria as portas à fraude. O caminho intermediário passa por instrumentos que permitam vincular o registro a uma origem e a um momento verificáveis e por uma cultura institucional que trate a confiabilidade como questão a ser ativamente demonstrada, e não passivamente presumida. É esse caminho que os eixos seguintes percorrem.

Importa, ainda, situar a confiabilidade no quadro mais amplo dos atributos da prova digital. A doutrina identifica como requisitos cumulativos a autenticidade, que liga o registro à sua fonte, e a integridade, que assegura a inalterabilidade do conteúdo desde a coleta. Thamay e Tamer (2020) observam que a prova digital, por sua natureza volátil e facilmente manipulável, reclama tratamento que reconheça essas especificidades, sob pena de equiparação indevida ao documento de papel. A inteligência artificial generativa acrescenta a esse quadro uma ameaça nova, que não recai sobre a alteração posterior do registro, mas sobre a própria gênese de um registro falso desde a origem, o que exige repensar o modo como a autenticidade é demonstrada.

2.2. Deepfakes: Técnica, Tipologia e Potencial de Fraude Probatória

O termo deepfake combina as expressões aprendizado profundo e falsificação, designando conteúdo audiovisual gerado ou manipulado por inteligência artificial de modo a parecer autêntico. A técnica mais difundida vale-se de arquiteturas em que duas redes neurais competem entre si, uma gerando conteúdo sintético e outra tentando distingui-lo do real, processo iterativo que aprimora progressivamente o realismo do resultado. A evolução dessas arquiteturas tornou possível substituir rostos em vídeos, clonar vozes a partir de breves amostras e criar cenas inteiras sem qualquer contraparte real.

A tipologia dos deepfakes é ampla. Há a substituição facial, que transplanta o rosto de uma pessoa para o corpo de outra; a sincronização labial, que faz alguém aparentar dizer o que nunca disse; a clonagem de voz, que reproduz o timbre e a entonação de um falante; e a geração integral de imagens de pessoas inexistentes. Cada modalidade comporta usos lícitos, no entretenimento e na acessibilidade, e usos ilícitos, como a fabricação de provas, a extorsão, a desinformação e a produção de material de abuso. Para o processo penal, interessa o uso voltado à fraude probatória.

O potencial lesivo no campo probatório é considerável. Um áudio sintético pode simular a confissão de um crime ou a combinação de um ilícito; um vídeo manipulado pode inserir um suspeito em local onde nunca esteve; uma imagem fabricada pode forjar a materialidade de um delito. A gravidade decorre da combinação entre o realismo do produto e a dificuldade de detecção, pois as ferramentas de identificação automática operam em corrida permanente com as de geração, sem garantia de superioridade estável. A consequência processual é que a mera verossimilhança sensorial deixa de ser indício suficiente de autenticidade.

A detecção técnica de deepfakes apoia-se em sinais residuais deixados pelo processo de síntese, como inconsistências em piscadas, sombras, reflexos, artefatos de compressão e padrões espectrais anômalos no áudio. Tais métodos, contudo, são probabilísticos e perecíveis: cada avanço na geração tende a eliminar os indícios que a geração anterior deixava. Por isso, a literatura forense recomenda não depositar confiança exclusiva na detecção a posteriori, e sim em mecanismos de proveniência que documentem a origem e a integridade do conteúdo desde a sua criação, deslocando o controle do produto para o procedimento.

As consequências processuais distribuem-se por todas as fases da persecução. Na investigação, um deepfake pode direcionar diligências contra inocente ou desviar o foco do verdadeiro autor; na fase de garantias, pode fundamentar medidas cautelares gravosas com base em material falso; na instrução, pode contaminar o conjunto probatório e induzir a condenação. A reação adequada não é a suspeição genérica que paralisa, mas a triagem criteriosa que reserva o exame técnico rigoroso para os casos em que a evidência audiovisual é central e a manipulação é plausível, preservando recursos periciais escassos para onde o risco de erro é mais elevado.

No processo penal brasileiro, a resposta a essa ameaça encontra ponto de apoio na exigência, já consolidada na jurisprudência, de metodologia adequada e de cadeia de custódia documentada. O Superior Tribunal de Justiça, ao reputar inadmissível a prova digital extraída sem procedimento que assegure idoneidade e integridade, fornece a moldura dentro da qual o problema dos deepfakes deve ser tratado: a evidência audiovisual relevante deve chegar ao processo acompanhada de elementos que permitam verificar sua

proveniência, e a dúvida razoável sobre a autenticidade impõe perícia ou conduz à exclusão (STJ, 2024).

A acessibilidade da tecnologia agrava a dimensão do problema. Aplicativos de uso corrente já oferecem substituição facial e clonagem de voz com poucos cliques, e a qualidade do resultado cresce a cada geração de modelos. Essa democratização da capacidade de falsificar significa que a fraude probatória deixou de exigir agentes especializados e passou a estar ao alcance de qualquer pessoa motivada, o que multiplica a frequência potencial do problema nos foros criminais e recomenda preparo institucional proporcional.

Há, ademais, uma dimensão temporal que o processo precisa absorver. A prova audiovisual costuma ser produzida e armazenada muito antes de tornar-se objeto de litígio, e a técnica de síntese evolui no intervalo. Um registro hoje considerado autêntico pode, no futuro, ser questionado à luz de capacidades de manipulação então existentes, e vice-versa. Essa assimetria temporal reforça a importância de mecanismos de proveniência aplicados no momento da captura, capazes de fixar a origem do conteúdo independentemente do estado da arte da falsificação no momento do julgamento.

2.3. Transparência e Marcação: O Parâmetro do AI Act Europeu

A União Europeia ofereceu a primeira resposta normativa horizontal ao problema da síntese algorítmica. O Regulamento (UE) 2024/1689, conhecido como Lei de Inteligência Artificial, adotado em 13 de junho de 2024 e com a maioria das disposições aplicável a partir de 2 de agosto de 2026, estrutura a regulação por níveis de risco e

estabelece deveres de transparência para o conteúdo gerado por inteligência artificial (UNIÃO EUROPEIA, 2024).

O núcleo da resposta está no artigo 50. O dispositivo impõe a quem implementa sistema que gera ou manipula imagem, áudio ou vídeo constituindo deepfake o dever de divulgar que o conteúdo foi artificialmente gerado ou manipulado (UNIÃO EUROPEIA, 2024). Em paralelo, exige-se que os provedores marquem as saídas em formato legível por máquina, de modo a permitir a detecção automatizada da origem sintética. O artigo 3, item 60, define deepfake como conteúdo que se assemelha a pessoas, objetos, lugares ou eventos existentes e que aparentaria falsamente ser autêntico ou verídico.

O modelo europeu é instrutivo por dois motivos. Primeiro, porque desloca parte do ônus da detecção a posteriori para a marcação a priori, criando obrigação de proveniência que facilita distinguir o sintético do autêntico. Segundo, porque prevê exceção expressa para o uso autorizado por lei na detecção, prevenção, investigação e repressão de infrações penais, reconhecendo que a atividade legítima de persecução pode demandar tratamento diferenciado, sem que isso dispense as garantias aplicáveis.

Esse arranjo dialoga com a tendência regulatória mais ampla. A Comissão Europeia tem publicado projetos de código de prática e diretrizes para operacionalizar a marcação e a detecção, sinal de que a transparência do conteúdo sintético é tratada como infraestrutura técnica, e não como mera recomendação ética. Para o processo penal, a lição é que a confiabilidade da prova audiovisual tende a depender, cada vez mais, de marcas de proveniência geradas na origem, e que sistemas jurídicos que não as exijam ficarão à mercê de uma detecção sempre defasada.

A transposição para o Brasil não é automática. O país discute projetos de marco regulatório da inteligência artificial, mas ainda não dispõe de regime vinculante de marcação de conteúdo sintético. Enquanto a regulação não amadurece, o ônus de demonstrar a autenticidade da prova audiovisual relevante recai sobre quem a apresenta, e a perícia continua a ser o instrumento central de controle. O parâmetro europeu sugere, contudo, que a política legislativa brasileira deve mirar não apenas a punição do uso malicioso, mas a criação de mecanismos preventivos de proveniência, mais eficazes do que a corrida perpétua da detecção.

Cabe registrar a ressalva de ordem aplicada à investigação penal. O artigo 50 do Regulamento (UE) 2024/1689 afasta o dever de divulgação quando o uso é autorizado por lei para detectar, prevenir, investigar ou reprimir infrações penais (UNIÃO EUROPEIA, 2024). A exceção é compreensível, pois revelar antecipadamente o emprego de determinada técnica poderia frustrar a diligência, mas não significa imunidade às garantias: o uso investigativo permanece sujeito a controle de legalidade, proporcionalidade e contraditório diferido. O modelo europeu, portanto, não opõe transparência e eficácia investigativa, mas as harmoniza mediante exceções delimitadas e controláveis.

O diálogo com o regime de prova eletrônica reforça essa leitura. O Regulamento (UE) 2023/1543, ao disciplinar as ordens europeias de entrega e de conservação de prova eletrônica, condiciona o acesso a controle judicial, a limiar de gravidade e a direito de impugnação (UNIÃO EUROPEIA, 2023). A convergência entre os dois regulamentos sugere uma arquitetura europeia coerente, na qual o tratamento da prova digital, inclusive da sintética, combina facilitação do acesso legítimo com salvaguardas robustas,

oferecendo ao Brasil um modelo de equilíbrio que dispensa a falsa escolha entre eficiência e garantia.

3. SALVAGUARDAS CRIPTOGRÁFICAS: HASH, BLOCKCHAIN E CERTIFICAÇÃO

3.1. A Função de Hash e a Verificação de Integridade

A primeira e mais consolidada salvaguarda de integridade é a função de hash criptográfico. Trata-se de algoritmo que converte qualquer conjunto de dados, independentemente do tamanho, em uma sequência de comprimento fixo, o valor de hash, que opera como impressão digital do arquivo. A propriedade essencial é a sensibilidade: a alteração de um único bit produz valor inteiramente distinto, de modo que a comparação entre o hash registrado na coleta e o hash recalculado posteriormente revela, com objetividade matemática, se o arquivo permaneceu íntegro.

Casey (2011) descreve o cálculo e o registro do hash como prática nuclear da computação forense, por permitir demonstrar que a cópia examinada é duplicata exata do original e que não houve alteração ao longo da custódia. A norma ISO/IEC 27037:2012 incorpora essa prática ao recomendar o cálculo do valor de verificação em todas as etapas relevantes da manipulação probatória, de modo a tornar auditável a integridade do material (ISO/IEC, 2012). O hash não atesta a autoria nem o conteúdo verídico do registro, mas garante que ele não foi modificado após o momento documentado.

O direito comparado evidencia a centralidade jurídica dessa técnica. A Regra 902(14) das Federal Rules of Evidence dos Estados Unidos, vigente desde dezembro de 2017, admite a autoautenticação de

dados copiados de dispositivo eletrônico mediante certificação de pessoa qualificada que ateste a identidade entre os valores de hash do original e da cópia, dispensando, para a admissão, o testemunho presencial (ESTADOS UNIDOS, 2017). A solução converte um conceito técnico em mecanismo processual de autenticação, transferindo à parte adversa o ônus de impugnar a integridade.

O hash, todavia, não é panaceia. Ele pressupõe que o valor de referência tenha sido calculado e registrado no momento adequado, idealmente na coleta, sob procedimento confiável. Se o arquivo já foi adulterado antes do primeiro cálculo, o hash apenas certificará a integridade do material já corrompido. Daí a importância de que a geração do valor de verificação se insira em cadeia de custódia documentada, e não opere isoladamente. A integridade verificável por hash é condição necessária, mas não suficiente, da confiabilidade probatória.

Há, ademais, limitação intrínseca diante dos deepfakes. O hash garante que um vídeo não foi alterado após a coleta, mas nada diz sobre a sua origem sintética: um deepfake perfeitamente íntegro continua sendo um deepfake. A verificação de integridade responde à pergunta sobre se o arquivo mudou, não à pergunta sobre se ele retrata a realidade. Por isso, no enfrentamento da síntese algorítmica, o hash deve ser combinado com mecanismos de proveniência e, quando necessário, com perícia de autenticidade, compondo um sistema de salvaguardas em camadas.

Do ponto de vista prático, a incorporação do hash à rotina investigativa é de baixo custo e alto rendimento. Basta que o agente, no momento da coleta, calcule e registre o valor de verificação do material, repetindo o cálculo a cada transferência relevante, de

modo que qualquer divergência futura seja imediatamente detectável. A ausência desse registro, por outro lado, priva o processo de um instrumento objetivo de controle e transfere a discussão sobre integridade para o terreno incerto das presunções, justamente o que a jurisprudência tem buscado evitar ao exigir documentação metodológica da prova digital.

3.2. Blockchain e o Registro Distribuído de Evidências

A tecnologia de registro distribuído, popularizada sob a designação blockchain, tem sido proposta como instrumento de fortalecimento da cadeia de custódia digital. Em essência, trata-se de livro-razão replicado em múltiplos nós, no qual os registros são encadeados por funções de hash e validados por consenso, de modo que a alteração de um registro pretérito exigiria refazer toda a cadeia subsequente em maioria dos nós, tarefa computacionalmente proibitiva. Dessa arquitetura decorre a propriedade que interessa ao processo: a imutabilidade prática dos registros inseridos.

Aplicada à prova penal, a ideia consiste em registrar, em cadeia distribuída, os eventos relevantes da custódia, como a coleta, a transferência e a análise, com o respectivo valor de hash e o carimbo temporal de cada etapa. O resultado seria uma trilha de auditoria resistente à adulteração, que documentaria de modo verificável quem manipulou o material, quando e com qual finalidade. A proposta responde a uma das fragilidades mais sensíveis da cadeia de custódia tradicional, que é a dependência de registros que podem ser, eles próprios, alterados.

Os benefícios potenciais são relevantes, mas não dispensam cautela. Primeiro, a imutabilidade da blockchain refere-se ao registro, não ao

fato registrado: se um dado falso ou adulterado é inserido na cadeia, ela o preservará imutável, sem torná-lo verdadeiro. A máxima segundo a qual a entrada de lixo produz a saída de lixo aplica-se integralmente. Segundo, a inserção de dados pessoais em registro imutável tensiona o direito à proteção de dados, em especial a possibilidade de correção e eliminação, exigindo arquiteturas que armazenem apenas referências e valores de hash, e não o conteúdo sensível.

Há, ainda, obstáculos institucionais. A adoção de blockchain na persecução penal pressupõe definição de governança, com escolha entre redes públicas e redes permissionadas, atribuição de responsabilidade pela operação dos nós e integração com os sistemas dos órgãos de investigação e do Judiciário. Sem disciplina normativa e padronização, o uso da tecnologia corre o risco de gerar mais litígio sobre a sua própria confiabilidade do que segurança sobre a prova. A blockchain é ferramenta promissora de registro, não substituto da disciplina jurídica da cadeia de custódia.

Em síntese, o registro distribuído pode reforçar a auditabilidade da custódia digital, sobretudo quando combinado com hash e carimbo de tempo, mas opera como camada complementar, e não como solução autônoma. Seu valor probatório dependerá sempre da confiabilidade do momento e do modo de inserção dos dados, o que reconduz a discussão, mais uma vez, à qualidade do procedimento e à sua aptidão para ser controlado em contraditório.

Convém ainda ponderar o risco de uma confiança excessiva na aura tecnológica da blockchain. A apresentação de um registro distribuído como prova pode induzir o julgador a presumir confiabilidade que a tecnologia, em rigor, não garante quanto ao

fato registrado. Esse efeito de deslumbramento técnico é particularmente perigoso no processo penal, em que a presunção de inocência impõe ônus rigoroso à acusação. A blockchain deve, portanto, ser tratada como aquilo que é, um mecanismo de registro resistente à adulteração, e não como selo de veracidade do conteúdo, cabendo ao contraditório expor essa distinção sempre que a tecnologia for invocada.

A experiência internacional, ainda incipiente, sugere que o emprego de registro distribuído na gestão de evidências é mais promissor no plano administrativo, como ferramenta interna de rastreamento da custódia entre órgãos, do que como prova autônoma da veracidade do conteúdo perante o juízo. Nessa função instrumental, a blockchain dialoga com a exigência jurisprudencial de documentação das fases de manuseio do vestígio, ao oferecer trilha de auditoria difícil de adulterar. O proveito, portanto, é real, mas circunscrito: reforça o controle sobre quem fez o quê e quando, sem dispensar a verificação independente da autenticidade do material custodiado.

3.3. Certificação, Carimbo de Tempo e Infraestrutura de Confiança

A terceira salvaguarda é a certificação digital, que vincula uma chave criptográfica a uma identidade por meio de autoridade de confiança. No Brasil, a Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileira e conferiu presunção de autenticidade aos documentos assinados com certificado nela emitido (BRASIL, 2001). Aplicada à prova digital, a assinatura por autoridade ou perito certificado permite atestar, de modo verificável, quem produziu determinado laudo ou registro e que este não foi alterado depois de assinado.

O carimbo de tempo complementa a certificação ao vincular um arquivo a um instante determinado, comprovando que ele existia, em certa forma, em dado momento. Essa função é decisiva no enfrentamento dos deepfakes, pois um registro carimbado antes do surgimento de uma técnica de síntese, ou imediatamente após a sua captura por dispositivo confiável, oferece elemento adicional de proveniência. A combinação de certificação de origem e carimbo de tempo constrói o que se pode designar infraestrutura de confiança, na qual a autenticidade não depende da inspeção do conteúdo, mas de garantias técnicas verificáveis.

Pastore (2020) observa que a confiança na prova digital migra do suporte para o procedimento, dependendo da demonstração rastreável de origem e de inalterabilidade. A certificação e o carimbo de tempo materializam essa migração, ao substituir a confiança na palavra do agente pela verificação criptográfica reproduzível. Trata-se, em rigor, da mesma lógica que orienta a Regra 902(14) norte-americana e a marcação de proveniência preconizada pelo Regulamento (UE) 2024/1689, ainda que por instrumentos distintos (ESTADOS UNIDOS, 2017; UNIÃO EUROPEIA, 2024).

A articulação entre as três salvaguardas é o ponto decisivo. O hash garante a integridade, a blockchain reforça a auditabilidade do registro de custódia, e a certificação com carimbo de tempo atesta origem e momento. Nenhuma delas, isoladamente, resolve o problema da autenticidade audiovisual, mas a sua combinação compõe um sistema de proveniência em camadas que eleva substancialmente o custo da fraude e amplia as possibilidades de controle. A confiabilidade probatória, na era da síntese algorítmica, é função dessa arquitetura combinada.

Um exemplo concreto ilustra o ponto. Suponha-se a apreensão de um vídeo relevante. A captura por dispositivo que calcule o hash no instante da aquisição, a assinatura do laudo pericial por profissional certificado e o carimbo de tempo aplicado por autoridade confiável compõem, em conjunto, um lastro de proveniência que permite ao juízo controlar, de modo objetivo, a integridade desde a coleta, a identidade de quem produziu a análise e o momento de cada etapa. Diante de alegação posterior de manipulação, esse lastro converte a discussão, antes especulativa, em verificação técnica reproduzível, o que aproxima a prática brasileira do padrão de autenticação por certificação consagrado no direito comparado.

Resta examinar, todavia, que mesmo a melhor arquitetura técnica é inerte sem instituições aptas a operá-la. A existência de hash, blockchain e certificação não assegura, por si, que a coleta seja feita por quem detenha competência, que os laudos sejam compreendidos pelos julgadores e que o contraditório técnico seja efetivo. Por isso, o terceiro eixo desloca o foco da tecnologia para as condições institucionais de sua utilização: padronização, capacitação e regulação.

Antes desse deslocamento, cabe uma observação sobre a relação entre as salvaguardas e o regime jurídico vigente. A Medida Provisória nº 2.200-2/2001, embora concebida para o documento eletrônico assinado, fornece o arcabouço de uma infraestrutura de confiança já operante no país, com autoridades certificadoras e cadeia de certificação auditável (BRASIL, 2001). A tarefa pendente não é criar do nada um sistema de proveniência, mas estender e adaptar instrumentos existentes ao tratamento da prova audiovisual, articulando a certificação e o carimbo de tempo com os protocolos de coleta forense, de modo que a confiabilidade deixe de depender

da sorte do caso concreto e passe a resultar de um desenho institucional deliberado.

4. PADRONIZAÇÃO, CAPACITAÇÃO E REGULAÇÃO

4.1. Normas Técnicas e Padronização da Cadeia de Custódia Digital

A padronização da cadeia de custódia digital é condição de comparabilidade e de controle. Sem procedimentos uniformes, cada coleta torna-se um evento singular, de qualidade variável e difícil auditoria, o que alimenta a insegurança jurídica e a litigiosidade sobre a confiabilidade da prova. A família de normas técnicas internacionais oferece referencial maduro: a ISO/IEC 27037:2012 trata da identificação, coleta, aquisição e preservação da evidência digital, e normas correlatas tratam da análise, da interpretação e da prontidão investigativa (ISO/IEC, 2012).

A ISO/IEC 27037:2012 condiciona a coleta a quatro princípios que merecem incorporação ao processo penal: auditabilidade, que exige documentar cada ação de modo que possa ser examinada; repetibilidade, que demanda que o mesmo procedimento, nas mesmas condições, produza o mesmo resultado; reprodutibilidade, que requer que outro examinador, com método equivalente, alcance resultado análogo; e justificação, que impõe fundamentar tecnicamente cada escolha metodológica (ISO/IEC, 2012). Esses princípios transformam a coleta de ato discricionário em procedimento controlável.

O Superior Tribunal de Justiça, embora reconheça que tais normas não possuem força de lei, tem-nas invocado como referencial de boas práticas, ao exigir que a obtenção da prova digital seja

documentada em laudo que esclareça a metodologia e as ferramentas empregadas (STJ, 2024). Essa recepção pretoriana confere às normas técnicas relevância processual indireta, na medida em que a sua inobservância passa a sinalizar fragilidade metodológica apta a comprometer a confiabilidade do material e, conforme o caso, a sua admissibilidade.

A padronização, contudo, não deve ser confundida com a importação mecânica de normas estrangeiras. As normas técnicas oferecem método, mas a sua articulação com as garantias do processo penal brasileiro, em especial o contraditório, a ampla defesa e a presunção de inocência, é tarefa jurídica que não se delega ao padrão técnico. O risco a evitar é a tecnocracia probatória, em que a conformidade formal a uma norma privada substitui a avaliação substantiva da confiabilidade pelo juiz natural.

O caminho recomendável é a edição de protocolos nacionais que adaptem os padrões internacionais à realidade institucional brasileira, com definição clara de responsabilidades, formulários padronizados de registro e exigência de cálculo e documentação de hash em todas as etapas. Tais protocolos, dotados de força normativa adequada, reduziriam a heterogeneidade de práticas e ofereceriam parâmetro objetivo de controle, beneficiando tanto a eficiência da persecução quanto a segurança do acusado.

A padronização produz, ainda, um efeito virtuoso sobre o contraditório. Quando o procedimento de coleta segue protocolo conhecido e documentado, a defesa pode aferir, ponto a ponto, a sua observância, identificando desvios que comprometam a confiabilidade. Inverte-se, assim, a lógica da opacidade: em vez de a parte ter de demonstrar, no escuro, que a prova é frágil, ela passa a

dispor de um referencial objetivo contra o qual confrontar a atuação estatal. A padronização, longe de ser exigência meramente burocrática, é instrumento de transparência e de controle democrático sobre a produção da prova penal.

4.2. Capacitação Interdisciplinar e o Papel do Perito

Nenhuma norma técnica e nenhuma ferramenta criptográfica produzem confiabilidade sem profissionais capacitados para operá-las. A perícia forense digital situa-se na interseção entre a ciência da computação e o direito, exigindo do perito não apenas domínio técnico, mas compreensão dos princípios jurídicos que regem a admissibilidade da prova. Marcella e Guillossou (2012) descrevem a disciplina como ciência aplicada que demanda formação interdisciplinar, capaz de articular o conhecimento sobre sistemas e algoritmos com a lógica probatória do processo.

A capacitação não pode restringir-se aos peritos. Juízes, membros do Ministério Público e advogados precisam de alfabetização técnica suficiente para formular as perguntas certas, avaliar laudos e exercer o contraditório de modo substantivo. Lopes Jr. (2023) adverte que o contraditório efetivo pressupõe reais condições de influir na formação da prova, o que, no campo digital, exige que os operadores compreendam minimamente os métodos empregados. A assimetria de conhecimento técnico, quando não enfrentada, converte a prova pericial em oráculo, subtraída ao controle das partes e do julgador.

O problema agrava-se diante dos deepfakes, cuja detecção exige conhecimento especializado e atualizado. A formação de quadros aptos a identificar a síntese algorítmica, a operar ferramentas de

detecção e a interpretar criticamente os seus resultados probabilísticos é investimento institucional incontornável. Mason e Seng (2017) registram que, nos sistemas que melhor lidam com a prova eletrônica, a confiabilidade decorre tanto de regras de admissibilidade quanto da existência de uma comunidade técnica qualificada, submetida a padrões profissionais e a escrutínio recíproco.

A independência do perito é outra dimensão sensível. A confiabilidade do laudo depende da ausência de subordinação que comprometa a imparcialidade da análise, e o sistema deve assegurar à defesa a possibilidade efetiva de produzir contraperícia ou, ao menos, de submeter o laudo oficial a crítica técnica qualificada. Sem essa simetria, a sofisticação tecnológica da prova converte-se em fator de desigualdade processual, e não de busca da verdade, recolocando o problema da paridade de armas em chave digital.

Convém, ainda, prevenir um equívoco recorrente, o de tratar o laudo pericial como conclusão definitiva e infensa a controle. O perito opera com métodos que comportam margens de erro, premissas e limitações, sobretudo na detecção de conteúdo sintético, cujos resultados são probabilísticos. Cabe ao operador jurídico compreender essas limitações e ao julgador valorar o laudo como elemento do conjunto probatório, e não como veredito técnico vinculante. A alfabetização digital dos atores do processo é, nesse sentido, condição para que a prova pericial permaneça sob o controle do contraditório e não se converta em transferência velada da decisão ao especialista.

A capacitação, por fim, deve ser permanente. A velocidade da evolução tecnológica torna obsoleto, em poucos anos, qualquer

corpo de conhecimento estático. Programas de formação continuada, integração entre universidades, órgãos periciais e instituições de justiça, e a constituição de laboratórios de referência são medidas que sustentam, no tempo, a capacidade institucional de lidar com provas digitais cada vez mais complexas. A confiabilidade probatória, nesse sentido, é menos um estado e mais um processo de atualização contínua.

A dimensão orçamentária não pode ser ignorada. A estruturação de laboratórios, a aquisição de ferramentas e a formação de quadros exigem investimento sustentado, frequentemente escasso nas instituições de persecução e, sobretudo, na defesa pública. A desigualdade de recursos entre acusação e defesa, quando não enfrentada por política pública específica, compromete a paridade de armas e, com ela, a própria legitimidade do resultado probatório. Soluções como a disponibilização obrigatória do material íntegro à defesa, a realização de perícia oficial a requerimento e convênios com instituições acadêmicas atenuam essa assimetria sem onerar excessivamente o sistema.

4.3. Caminhos Regulatórios e a Cultura de Integridade Probatória

A resposta jurídica ao desafio dos deepfakes situa-se em três planos articulados. No plano repressivo, discute-se a tipificação ou o agravamento de condutas relacionadas à produção e ao uso malicioso de conteúdo sintético, especialmente quando voltado à fraude probatória, à extorsão ou à ofensa à dignidade. No plano preventivo, cogita-se a exigência de marcação de proveniência do conteúdo gerado por inteligência artificial, na linha do modelo europeu. No plano processual, impõe-se disciplinar a

admissibilidade e a valoração da prova audiovisual em ambiente de síntese algorítmica.

O Regulamento (UE) 2024/1689 oferece parâmetro relevante ao combinar regulação por risco e dever de transparência, ao exigir que o conteúdo sintético seja identificado como tal e ao ressalvar o uso autorizado por lei na investigação penal (UNIÃO EUROPEIA, 2024). O Regulamento (UE) 2023/1543, por sua vez, ilustra como o acesso a prova eletrônica pode ser submetido a controle judicial e a direito de impugnação, evidenciando que eficiência e garantia não são termos antagônicos (UNIÃO EUROPEIA, 2023).

No Brasil, a regulação da inteligência artificial encontra-se em debate legislativo, sem regime vinculante de marcação de conteúdo sintético. Enquanto a disciplina não amadurece, a tutela da confiabilidade probatória apoia-se na construção jurisprudencial sobre cadeia de custódia e na exigência de perícia diante de dúvida razoável, conforme orientação recente segundo a qual, havendo dúvida sobre a integridade e a autenticidade de provas digitais, impõe-se o exame pericial, não podendo o material duvidoso ser utilizado contra o réu (STJ, 2026).

Esse arranjo provisório, contudo, é insuficiente para o enfrentamento sistemático do problema. A tutela apenas reativa, que aguarda a impugnação para então determinar a perícia, sobrecarrega o sistema, retarda a marcha processual e deixa ao acaso a sorte de cada caso. Uma política mais consistente combinaria a previsão expressa, em lei processual, de critérios de admissibilidade e valoração da prova audiovisual em ambiente de síntese, com a indução de mecanismos de proveniência na origem, seja por dever de marcação imposto aos provedores, seja por incentivo à captura

mediante dispositivos certificadores. A experiência comparada demonstra que a antecipação regulatória é mais eficaz do que a remediação tardia.

A regulação, porém, não basta. Normas e tecnologias são condições necessárias, mas insuficientes, se não acompanhadas de uma cultura institucional de integridade probatória. Por cultura de integridade entende-se a internalização, por todos os atores do sistema, da premissa de que a confiabilidade da prova é valor a ser ativamente construído e demonstrado, e não pressuposto a ser comodamente presumido. Essa cultura traduz-se em práticas cotidianas: documentar, calcular e registrar valores de verificação, preservar originais, submeter laudos a contraditório e desconfiar metodicamente da evidência que não possa ser controlada.

A síntese aqui defendida recusa tanto o tecno-otimismo, que enxerga na blockchain ou na detecção automática a solução definitiva, quanto o tecno-pessimismo, que conclui pela impossibilidade de confiar em qualquer prova digital. A confiabilidade probatória é reconstruível, mas a sua reconstrução é tarefa simultaneamente técnica, jurídica e institucional. Cabe ao direito processual penal orquestrar esses planos, assegurando que a tecnologia sirva à verdade e à justiça, e não as substitua nem as comprometa.

5. CONCLUSÃO

A investigação demonstrou que a maturação da inteligência artificial generativa instaurou uma crise de confiabilidade que atinge o núcleo da prova digital no processo penal. A falsificação audiovisual realista, antes restrita a recursos raros, tornou-se

capacidade amplamente disponível, dissolvendo a presunção intuitiva de autenticidade que acompanhava a imagem e o som e exigindo do sistema de justiça o deslocamento do paradigma da percepção para o da verificação técnica.

O objetivo geral, de analisar as ameaças da síntese algorítmica e as respostas técnicas e normativas disponíveis, foi alcançado mediante o exame da técnica e da tipologia dos deepfakes, das salvaguardas criptográficas de integridade e dos caminhos de padronização, capacitação e regulação, em diálogo com o direito comparado europeu e norte-americano.

No primeiro eixo, evidenciou-se que a confiabilidade probatória, condição de admissibilidade e de valoração, foi posta em xeque pela inteligência artificial generativa, que produz tanto o risco do falso admitido quanto o do verdadeiro indevidamente descartado. O parâmetro do Regulamento (UE) 2024/1689, ao impor a marcação do conteúdo sintético, sinalizou que a resposta mais eficaz desloca o controle da detecção a posteriori para a proveniência documentada na origem.

No segundo eixo, analisaram-se as salvaguardas criptográficas. A função de hash garante a integridade do registro, mas não a sua origem nem a sua veracidade; a blockchain reforça a auditabilidade da custódia, mas preserva imutável tanto o dado verdadeiro quanto o falso nela inserido; a certificação com carimbo de tempo atesta origem e momento. Nenhuma resolve isoladamente o problema, mas a sua combinação compõe um sistema de proveniência em camadas que eleva o custo da fraude e amplia o controle.

No terceiro eixo, demonstrou-se que a tecnologia é inerte sem condições institucionais adequadas. A padronização da cadeia de custódia por normas técnicas, a capacitação interdisciplinar de peritos e operadores e a regulação articulada nos planos repressivo, preventivo e processual são as condições de possibilidade de uma resposta sustentável, sob pena de a sofisticação técnica converter-se em fonte de desigualdade e de insegurança.

Quanto ao problema de pesquisa, conclui-se que a preservação da confiabilidade da prova digital, em ambiente de inteligência artificial, depende da combinação entre salvaguardas técnicas de proveniência e integridade, padronização metodológica controlável em contraditório e uma cultura institucional que trate a confiabilidade como valor a ser ativamente demonstrado. O direito comparado confirma que eficiência e garantia podem coexistir, desde que a tecnologia se submeta ao controle jurídico, e não o contrário.

O debate comporta posições divergentes. De um lado, sustenta-se que o rigor crescente inviabilizaria a persecução, sobretudo em jurisdições com recursos periciais escassos, e que a desconfiança generalizada quanto à prova audiovisual beneficiaria a impunidade. De outro, defende-se que a gravidade da condenação injusta e a facilidade da fraude impõem rigor máximo na verificação, com perícia obrigatória sempre que a prova sintética for plausível e central. Ambas as perspectivas apresentam fundamentos legítimos e merecem consideração.

A posição adotada busca síntese proporcional: o rigor exigível deve crescer com a centralidade da prova na imputação, com a gravidade do delito e com a plausibilidade concreta de manipulação

algorítmica. Quando a evidência audiovisual é essencial e há dúvida razoável sobre a sua autenticidade, a verificação técnica é imperativa; quando apenas corrobora conjunto independente, admite-se procedimento simplificado, assegurada a contraprova. A reconstrução da confiabilidade probatória na era digital não é tarefa exclusivamente tecnológica, mas projeto jurídico e institucional, no qual a tecnologia é meio, e a justiça, o fim.

REFERÊNCIAS BIBLIOGRÁFICAS

BADARÓ, Gustavo Henrique. Processo penal. 9. ed. São Paulo: Thomson Reuters Brasil, 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 9 jun. 2026.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 9 jun. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 jun. 2026.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 9 jun. 2026.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Brasília, DF: Presidência da República, 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 9 jun. 2026.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Habeas Corpus nº 828.054/RN. Relator: Min. Joel Ilan Paciornik. Quinta Turma. Julgado em: 23 abr. 2024. DJe 29 abr. 2024. Informativo de Jurisprudência nº 811, 2024.

BRASIL. Superior Tribunal de Justiça. Sexta Turma afasta prisão até conclusão de perícia sobre prints de WhatsApp usados como prova. Brasília: STJ, 9 mar. 2026. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2026/09032026-Sexta-Turma-afasta-prisao-ate-conclusao-de-pericia-sobre-prints-de-WhatsApp-usados-como-prova.aspx. Acesso em: 9 jun. 2026.

CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the internet. 3rd ed. Waltham: Elsevier, 2011.

CONSELHO DA EUROPA. Convenção sobre o Cibercrime (Convenção de Budapeste). Budapeste: Conselho da Europa, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 9 jun. 2026.

ESTADOS UNIDOS. Federal Rules of Evidence. Rule 902(13)-(14): self-authentication of electronic evidence. Washington: U.S.

Government, 2017. Disponível em: https://www.rulesofevidence.org/fre/article-ix/rule-902/. Acesso em: 9 jun. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27037:2012: information technology, security techniques, guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO/IEC, 2012. Disponível em: https://www.iso.org/standard/44381.html. Acesso em: 9 jun. 2026.

LOPES JR., Aury. Direito processual penal. 20. ed. São Paulo: Saraiva, 2023.

MARCELLA, Albert J.; GUILLOSSOU, Frederic. Cyber forensics: from data to digital evidence. New Jersey: Wiley, 2012.

MASON, Stephen; SENG, Daniel (ed.). Electronic evidence. 4th ed. London: University of London, 2017.

PASTORE, Guilherme de Siqueira. Considerações sobre a prova digital e a cadeia de custódia. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (org.). Direitos fundamentais e processo penal na era digital. São Paulo: InternetLab, 2020.

THAMAY, Rennan Faria Krüger; TAMER, Maurício Antonio. Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial

(Regulamento Inteligência Artificial). Jornal Oficial da União Europeia, L 2024/1689, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 9 jun. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de entrega e de conservação de provas eletrónicas em processo penal. Jornal Oficial da União Europeia, L 191, 28 jul. 2023. Disponível em: https://eur-lex.europa.eu/eli/reg/2023/1543/oj. Acesso em: 9 jun. 2026.

---

[1] Doutor em Direito pela Instituição Toledo de Ensino (ITE). Mestre em Direito pelo Centro Universitário Eurípides de Marília (UNIVEM). Promotor de Justiça no Ministério Público do Estado de São Paulo. Pró-Reitor Acadêmico e Professor Titular do Programa de Mestrado em Direito do UNIVEM (Marília-SP). Coordenador do Grupo de Estudos de Marília 'João Batista de Santana' da Associação Paulista do Ministério Público. E-mail: acesse o artigo original para visualizar o e-mail. Currículo Lattes: http://lattes.cnpq.br/6687308419664444. ORCID: https://orcid.org/0000-0002-4035-1628.

[2] Mestrando em Direito pelo Centro Universitário Eurípides de Marília (UNIVEM). Procurador Jurídico do Poder Legislativo de Jales-SP. Pós-graduado em Direito Público pelas Universidades Potiguar e Gama Filho, com ênfase em Direito Penal, Constitucional, Civil e Processual Civil. Integrante do grupo de pesquisa NODICO, com atuação em direito digital e inteligência artificial. E-mail: acesse o artigo original para visualizar o e-mail. Currículo Lattes: https://lattes.cnpq.br/2051996455632539. ORCID: https://orcid.org/0009-0009-4015-2934