Provas digitais: ameaças não resolvidas à equidade e à presunção de inocência

Evidencia digital: amenazas no resueltas a la equidad y a la presunción de inocencia

João Pedro **Pereira Passos**

https://orcid.org/0000-0001-7181-4587
Universidade Federal do Tocantins
Correo electrónico: Joaopedro.Passos@Mail.Uft.Edu.Br

Recepción: 15 de septiembre de 2024
Aceptación: 13 de febrero de 2025
Publicación: 1 de julio de 2025

DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

Resumo: O artigo aborda os desafios e ameaças não resolvidas em relação ao uso de provas digitais no processo penal, com foco na falta de padronização e validação científica no Brasil. A datificação, que transforma interações humanas em dados digitais, é destacada como uma ferramenta importante, porém suscetível a abusos como a coleta massiva de dados sem verificação adequada, levando a possíveis erros judiciais. Além disso, há críticas à confiabilidade da perícia digital, com destaque para problemas na análise de grandes volumes de dados e a possibilidade de manipulação das provas digitais. O artigo destaca ainda a necessidade de intervenção legislativa para regulamentar o uso dessas provas, garantindo sua validação científica e a preservação dos direitos dos acusados, incluindo a adoção de padrões mínimos para a coleta e análise. A importância da imparcialidade e independência do perito é ressaltada como fundamental para a justiça.
Palavras-chave: provas digitais; presunção de inocência; validação científica.

Resumen: El artículo aborda los desafíos y amenazas no resueltos relacionados con el uso de pruebas digitales en los procesos penales, enfocándose en la falta de estandarización y validación científica en Brasil. La datificación, que transforma las interacciones humanas en datos digitales, se destaca como una herramienta importante, pero susceptible a abusos como la recopilación masiva de datos sin la verificación adecuada, lo que puede llevar a errores judiciales. Además, se critica la fiabilidad de la pericia digital, con énfasis en los problemas en el análisis de grandes volúmenes de datos y la posibilidad de manipulación de las pruebas digitales. El artículo también destaca la necesidad de una intervención legislativa para regular el uso de dichas pruebas, garantizando su validación científica y la preservación de los derechos de los acusados, incluyendo la adopción de estándares mínimos para la recopilación

y el análisis. La importancia de la imparcialidad e independencia del perito se resalta como fundamental para la justicia.
Palabras clave: pruebas digitales; presunción de inocencia; validación científica.

Sumario: I. *Introdução*. II. *Metodologia*. III. *Presunção de inocência na era digital*. IV. *A fragilidade da prova de DNA*. V. *IA e previsão criminal*. VI. Caminhos a seguir. VII. *Desafiando a proporcionalidade com confiabilidade*. VIII. *Conclusão*. IX. *Referências*.

I. Introdução

Em um recente julgado a 5º turma do STJ deixou claro que "são inadmissíveis no processo penal as provas obtidas de celular quando não forem adotados procedimentos para assegurar a idoneidade e a integridade dos dados extraídos"(STJ, 2024).

Interessante que no caso o principal fator que levou a unanimidade foi o fato de que "a análise dos dados se deu em consulta direta ao celular, sem o uso de máquinas extratoras"(STJ, 2024) isto devido a uma inviabilidade técnica da perícia cujo equipamento foi ineficaz.

Este caso é uma luz num cenário onde as provas digitais são cada vez mais apresentadas e aceitas nos tribunais sem validação científica da metodologia ou ferramentas de perícia digital padronizadas ou mesmo passíveis de serem contraditas.

Enquanto medidas investigativas clássicas estão sujeitas a limites rigorosos e garantias de julgamento justo, as investigações digitais ainda carecem de garantia de qualidade e responsabilização. Não há padrões mínimos no Brasil para provas digitais seu estabelecimento, aplicação e validação científica da perícia digital. Todas

O uso inadequado de tecnologia mal testada compromete o direito a um julgamento justo, conforme formulado no Art. 8º da 1.1.1 Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica, 1969) e ameaça a presunção de inocência em um estágio inicial da investigação, previsto em seu parágrafo 2º:

> Artigo 8: "Garantias judiciais"
> [...]

§2º: "Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias mínimas:
a) Direito do acusado de ser assistido por um defensor proporcionado pelo Estado, remunerado ou não conforme a legislação interna, se não tiver defensor particular;
b) Direito de o acusado ser informado previamente e detalhadamente sobre a acusação contra ele formulada;
c) Concessão ao acusado do tempo e dos meios necessários à preparação de sua defesa;
d) Direito do acusado de comunicar-se, livre e privativamente, com seu defensor;
e) Direito do acusado de ser assistido gratuitamente por um intérprete, se não compreender ou não falar o idioma do tribunal ou de não ser forçado a depor contra si mesmo ou a confessar-se culpado. (CADH)

Além disso, garantias ineficazes antes e durante o julgamento para réus não são adequadas para validar metodologias e ferramentas complexas de perícia digital, e a posição já frágil do suspeito/réu para coletar ou contestar provas digitais nos processos criminais é fraca.

Dependência excessiva e uso inadequado da tecnologia em combinação com a posição fraca dos suspeitos/réus podem levar a um tratamento desigual dos mesmos e falta de certeza jurídica no processo judicial.

Portanto, este artigo é uma tentativa de esclarecer a conexão entre o direito a um julgamento justo, em particular a presunção de inocência (PI), com o desenvolvimento de regras de provas digitais como um *framework* teórico.

Este trabalho examina até que ponto as práticas de provas digitais cumprem os princípios de julgamento justo e como as investigações assistidas por tecnologia desafiam o procedimento criminal.

A prova digital é definida como qualquer evidência utilizada no processo judicial que tem sua origem ou pode ser demonstrada através de meios digitais. De acordo com Thamay e Tamer (2020) a prova digital pode ser entendida sob duas principais acepções: a primeira refere-se à demonstração de um fato que ocorreu nos meios digitais, como e-mails, mensagens de texto ou arquivos eletrônicos armazenados localmente ou na nuvem; a segunda acepção se refere à utilização de meios digitais para demonstrar a ocorrência de fatos que não necessariamente ocorreram em ambientes digitais,

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

como vídeos de câmeras de segurança ou registros de chamadas telefônicas interceptadas.

Essas provas podem ser apresentadas na forma de documentos digitais ou digitalizados, interceptações telemáticas (dados capturados durante uma comunicação eletrônica) e podem estar armazenadas localmente ou em servidores remotos (Capanema, 2024).

A validade e a força probante das provas digitais dependem de uma série de requisitos técnicos e legais específicos, incluindo a preservação da integridade dos dados e a autenticidade dos metadados que acompanham esses documentos digitais. Segundo Capanema (2024), a relevância jurídica da diferenciação entre as espécies de provas digitais reside nas suas bases legais e requisitos formais próprios.

Além disso, as provas digitais podem ser constituídas pela vontade humana, como e-mails, ou pela intervenção automatizada de sistemas de computadores, como registros de conexão de usuários na internet. A ausência de uma sistematização normativa clara e a infinita quantidade de provas digitais criadas por aplicativos, redes sociais e sites da internet tornam o tema desafiador e demandam um estudo aprofundado e contínuo

Portanto, Provas digitais são definidas como: qualquer informação processada por meio eletrônico que suporte ou refute uma hipótese sobre o estado de artefatos digitais ou eventos digitais, de relevância e valor probatório potenciais para uma investigação criminal [conceito nosso].

Provas digitais são o resultado de metodologias e ferramentas científicas que garantem que "sua autenticidade e integridade possam ser validadas". Assim como qualquer outra ciência forense, a perícia digital deve levar em consideração limitações de ferramentas, metodologias e humanas e até a inteligência artificial.

Padilha et al. (2021) enfatizam que a ciência forense digital (CFD) é um ramo da Ciência Forense que lida com a análise e investigação de conteúdos associados a dispositivos digitais, abrangendo desde equipamentos de grande porte até dispositivos móveis. Com a evolução da computação pessoal e o advento das mídias sociais, a CFD enfrenta desafios significativos, especialmente na coleta, filtragem e análise de um volume massivo de dados compartilhados online.

A validade das provas digitais depende de um rigoroso protocolo de análise que inclui a coleta de dados, sanitização e filtragem de relevância, organização semântica e mineração de conteúdo. Como destacam Padilha et al. (2021), cada etapa desse protocolo é crucial para garantir que as informações

recuperadas sejam confiáveis e possam ser utilizadas de forma eficaz em investigações e processos judiciais.

A aplicação de técnicas modernas de inteligência artificial (IA), como redes neurais convolucionais e algoritmos de reconhecimento facial, é essencial para lidar com a complexidade e o volume dos dados digitais, permitindo uma análise mais precisa e eficiente. No entanto, a interpretabilidade dos modelos de IA e a mitigação de vieses nos dados são desafios contínuos que precisam ser abordados para assegurar a equidade e a presunção de inocência no uso de provas digitais.

Devido à dinâmica no campo e ao amplo escopo de aplicação em todas as etapas do procedimento criminal, a prática da perícia digital deve ser guiada por padrões mínimos de qualidade e salvaguardas de julgamento justo, independentemente das diferenças jurisdicionais.

Este artigo classifica as ameaças não resolvidas à PI em relação às investigações assistidas por tecnologia e provas digitais em três grupos: uso inadequado e inconsistente da tecnologia, garantias processuais antigas, que não são adaptadas aos processos e serviços de provas digitais contemporâneas e a falta de testes de confiabilidade na prática da perícia digital.

Argumenta-se que o uso da tecnologia para fins de investigação deve ser avaliado em relação aos padrões de julgamento justo e confiabilidade. Destacam-se questões com o ônus da prova de fato revertido, processamento de dados de baixa qualidade, dependência de evidências digitais não testadas (opinião), e falta de garantias no procedimento criminal em retenção de dados, prevenção de crimes e procedimentos baseados em suspeitas.

Nos últimos anos, o uso de provas digitais no âmbito judicial tem se tornado cada vez mais comum, acompanhando o rápido avanço da tecnologia e a crescente digitalização de diversos aspectos da vida cotidiana. Esse cenário, no entanto, traz consigo uma série de desafios que ameaçam os princípios fundamentais do devido processo legal, especialmente a presunção de inocência e a equidade no julgamento.

A principal questão que surge com o uso de provas digitais no processo penal é a falta de padronização e validação científica dessas evidências. No Brasil, não há diretrizes claras e específicas sobre a coleta, preservação e análise das provas digitais, o que compromete a sua confiabilidade. Em muitos casos, os tribunais aceitam essas provas sem a devida análise crítica de sua integridade, o que pode resultar em erros judiciais graves.

Em decisões recentes, como o julgado da 5ª turma do Superior Tribunal de Justiça (STJ), foi determinado que "são inadmissíveis no processo

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

penal as provas obtidas de celular quando não forem adotados procedimentos para assegurar a idoneidade e a integridade dos dados extraídos" (STJ, 2024). Este julgamento destacou a ausência de validação científica para muitas das metodologias utilizadas na coleta e análise de dados digitais, revelando uma lacuna significativa na legislação brasileira.

Além disso, a falta de uniformidade no tratamento das provas digitais aumenta o risco de decisões judiciais desiguais, criando um ambiente de incerteza jurídica. A ausência de padrões mínimos de qualidade para a perícia digital pode comprometer a equidade no processo, uma vez que a defesa muitas vezes não tem acesso às mesmas ferramentas ou conhecimento técnico necessário para contestar a veracidade das provas.

Outro ponto crítico é a dependência excessiva de tecnologias mal testadas, que compromete o direito a um julgamento justo, conforme estabelecido no artigo 8º da Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica, 1969). As provas digitais, embora fundamentais para a investigação criminal moderna, trazem consigo o risco de manipulação e adulteração, o que pode enfraquecer a presunção de inocência em um estágio inicial da investigação.

Diante deste cenário, torna-se urgente discutir a implementação de normas mais rígidas para a coleta e validação de provas digitais no Brasil. Este artigo tem como objetivo examinar as ameaças não resolvidas à equidade e à presunção de inocência causadas pelo uso inadequado de provas digitais, destacando a necessidade de uma intervenção legislativa que estabeleça padrões mínimos e confiáveis para a utilização dessas evidências no processo penal.

II. Metodologia

Para alcançar os objetivos propostos, foi realizada uma revisão de literatura por meio de pesquisa bibliográfica e documental, utilizando abordagens qualitativas que permitiram a análise detalhada dos desafios e ameaças relacionadas ao uso de provas digitais no contexto jurídico. A pesquisa foi estruturada para identificar, analisar e sintetizar as principais evidências disponíveis, fornecendo uma visão abrangente sobre o estado atual das provas digitais e como elas afetam diretamente a equidade e a presunção de inocência.

A revisão bibliográfica incluiu a análise de trabalhos publicados nos últimos 20 anos, com ênfase em estudos acadêmicos, jurisprudência e relatórios

técnicos. A base de dados do *Google Acadêmico* foi amplamente utilizada como fonte primária de pesquisa devido à sua extensa coleção de artigos científicos em diversas disciplinas, incluindo Direito, Ciências Forenses e Tecnologia da Informação. As palavras-chave utilizadas para a busca incluíram termos como: "provas digitais"; "direito"; "equidade"; "presunção de inocência" e seus equivalentes em inglês: "digital evidence"; "law"; "fairness"; "presumption of innocence". Essas palavras-chave foram selecionadas com base na relevância para o contexto jurídico e técnico das provas digitais, a fim de garantir a abrangência da pesquisa.

Além disso, a pesquisa foi complementada com o uso da técnica *snowballing*, também conhecida como "referências das referências", conforme proposta por Greenhalgh e Peacock (2005). Essa técnica foi fundamental para expandir o número de fontes relevantes, uma vez que permitiu identificar novos trabalhos a partir das referências citadas em artigos previamente selecionados. A técnica de snowballing é particularmente eficaz quando a pesquisa inicial já oferece uma base sólida de fontes de alta qualidade. A aplicação dessa técnica permitiu a exploração de uma rede de estudos interconectados, proporcionando uma visão mais rica e completa das problemáticas associadas às provas digitais.

Outra técnica empregada foi a auditoria de fontes primárias, conforme descrito por Greenhalgh e Peacock (2005) e Richards (2006). Esse método sistemático ajudou a garantir que todos os trabalhos relevantes fossem devidamente analisados, especialmente aqueles que não estavam diretamente acessíveis por meio de simples buscas por palavras-chave. A auditoria de fontes foi conduzida de maneira rigorosa para evitar vieses e assegurar que apenas fontes de alta relevância fossem consideradas. Esse processo, além de aumentar a profundidade da análise, também permitiu a identificação de padrões e lacunas na literatura existente.

O método de revisão sistemática da literatura foi complementado por uma análise crítica dos estudos selecionados, focando em aspectos práticos e teóricos das ameaças não resolvidas relacionadas às provas digitais. Foram considerados estudos de diversas jurisdições, o que permitiu uma comparação entre as práticas legais internacionais e os desafios específicos enfrentados no Brasil. A pesquisa também explorou a evolução das normas técnicas relacionadas à validação de provas digitais, como a ISO/IEC 27037, e como essas normas influenciam o cenário jurídico nacional.

A aplicação desses métodos forneceu uma base sólida para a construção de um panorama abrangente sobre as principais ameaças não resolvidas re-

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

lacionadas às provas digitais, destacando tanto os desafios práticos quanto as soluções propostas na literatura. Ao final do processo, foi possível avaliar criticamente as soluções sugeridas e identificar áreas que ainda precisam de desenvolvimento, tanto no campo jurídico quanto técnico, para mitigar os riscos associados ao uso de provas digitais nos tribunais.

III. Presunção de inocência na era digital

A presunção de inocência em investigações assistidas por tecnologia é primeiramente desafiada pelo uso inadequado e inconsistente da tecnologia. Isso cria questões, algumas das quais já examinadas, como visão em túnel em um estágio inicial da investigação; falta de provas confiáveis e completas; construção paralela de fatos; falta de acesso a provas e recursos forenses relevantes pela defesa; retenção excessivamente longa de provas e dados sobre pessoas absolvidas/suspeitas para comparação. A necessidade de harmonização de garantias processuais mínimas em relação a medidas investigativas intrusivas é discutida extensivamente.

1. *Dataficação*

Dataficação refere-se ao processo pelo qual aspectos da vida cotidiana são transformados em dados digitais, os quais podem ser coletados, armazenados, analisados e utilizados para uma ampla gama de finalidades, incluindo a investigação criminal. Esse conceito envolve a conversão de comportamentos, interações e informações humanas em formatos digitais que podem ser processados por computadores e outras tecnologias avançadas, permitindo a manipulação de grandes volumes de dados. A dataficação engloba desde simples registros de atividades online, como cliques e navegação, até complexas interações digitais, como comunicações via redes sociais, transações financeiras e o uso de dispositivos conectados à internet, como smartphones e assistentes virtuais (Segata et al., [*s. d.*])

Na investigação criminal, a dataficação desempenha um papel fundamental, especialmente com o avanço das tecnologias digitais e a crescente digitalização de diversos aspectos da vida cotidiana. A capacidade de coletar e analisar grandes volumes de dados em tempo real revolucionou a forma como as investigações são conduzidas. Por meio da dataficação, informações sobre suspeitos, testemunhas e vítimas podem ser obtidas rapidamente, ofe-

recendo aos investigadores um vasto arsenal de dados que, em teoria, podem fornecer evidências valiosas para a resolução de crimes. Dados de smartphones, geolocalização, histórico de navegação na internet, mensagens de texto e vídeos de câmeras de segurança são exemplos de fontes de informações cruciais que podem ser exploradas durante as investigações (Mariobo Franck *et al.*, [*s. d.*]).

Entretanto, a datafication também apresenta desafios significativos, especialmente no que tange aos direitos fundamentais, como a presunção de inocência (PI) e o direito à privacidade. A coleta massiva de dados aumenta o risco de processamento indevido de informações pessoais, levando à possibilidade de erros judiciais. A confiança excessiva em provas digitais, que muitas vezes são coletadas sem a devida validação científica ou análise criteriosa, pode resultar em uma dependência perigosa desses dados. Um dos maiores riscos associados à datafication é a chamada visão em túnel, onde os investigadores focam exclusivamente em dados que corroboram suas hipóteses iniciais, desconsiderando informações que poderiam exonerar o suspeito ou fornecer uma visão mais completa dos fatos (Mariobo Franck *et al.*, [*s. d.*]).

A visão em túnel ocorre quando os dados são interpretados de forma tendenciosa, levando a uma investigação parcial. Isso pode acontecer, por exemplo, quando a polícia ou os promotores se baseiam excessivamente em dados de geolocalização que colocam um suspeito próximo ao local do crime, sem considerar outras explicações plausíveis para a presença da pessoa naquele local. Da mesma forma, a análise de comunicações digitais, como mensagens de texto ou e-mails, pode ser manipulada para sustentar uma narrativa específica, ignorando o contexto mais amplo ou outros elementos que poderiam alterar o entendimento da situação.

Além disso, o fenômeno da datafication exacerba outro problema: o processamento massivo de dados. A quantidade de informações disponíveis em uma investigação moderna é praticamente ilimitada, devido à ubiquidade de dispositivos digitais e à interconectividade das tecnologias da informação. Esse excesso de dados, embora aparentemente benéfico, pode levar a dificuldades práticas na triagem e filtragem de informações realmente relevantes. A sobrecarga de dados pode resultar em erros de julgamento, com dados cruciais sendo negligenciados ou mal interpretados. Muitas vezes, o volume de informações processadas supera a capacidade dos investigadores de lidar com todas as nuances dos dados disponíveis, criando um cenário onde a simplificação excessiva ou a confiança em algoritmos automatizados se torna uma solução tentadora, mas potencialmente perigosa (Segata et al., n.d.).

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

Outro risco associado ao uso de grandes volumes de dados na investigação criminal é o aumento de suspeitas vagas, baseadas em correlações superficiais ou na interpretação errônea de padrões de comportamento digital. A análise de big data, embora poderosa, frequentemente falha em diferenciar entre coincidências e provas concretas. Por exemplo, uma pessoa pode ser marcada como suspeita simplesmente por estar conectada a uma rede *Wi-Fi* próxima a uma cena de crime, ou por ter feito uma compra online de um item que foi utilizado em um ato criminoso. No entanto, essas ligações são frequentemente circunstanciais e não estabelecem uma conexão direta com o crime. A confiança cega nesses tipos de dados pode resultar na detenção ou acusação injusta de indivíduos inocentes, comprometendo gravemente a presunção de inocência.

A utilização de ferramentas de inteligência artificial e algoritmos no tratamento de dados é outro elemento que merece atenção. Enquanto essas tecnologias têm o potencial de aprimorar significativamente a capacidade de análise de grandes volumes de informações, elas também introduzem novos desafios, como a falta de transparência nos processos de decisão e a possibilidade de vieses implícitos nos algoritmos. Estudos mostram que algoritmos de reconhecimento facial e análise de dados podem apresentar taxas de erro mais altas para certos grupos raciais ou demográficos, aumentando a desigualdade no tratamento de suspeitos e exacerbando as disparidades já existentes no sistema de justiça criminal.

Assim, embora a datificação ofereça um grande potencial para auxiliar nas investigações criminais, também levanta preocupações éticas e legais que não podem ser ignoradas. O excesso de confiança em dados digitais, sem um exame rigoroso de sua origem, autenticidade e contexto, pode comprometer a integridade do processo judicial e violar direitos fundamentais. Para garantir que a justiça seja feita de forma adequada, é essencial que sejam implementadas diretrizes claras e procedimentos robustos para a coleta, armazenamento e análise de dados digitais, de modo a minimizar os riscos associados à datificação.

A. *Qualidade das Provas*

A confiança excessiva em dados digitais pode comprometer a qualidade das provas, pois a autenticidade e integridade desses dados nem sempre são verificadas adequadamente (Dias Moreira de Resende *et al.*, 2023).

Dados digitais podem ser facilmente manipulados, adulterados ou mal interpretados, e sem processos rigorosos de validação, sua utilização pode levar a conclusões errôneas (Dias Moreira de Resende *et al.*, 2023).

A Associação Brasileira de Normas Técnicas (ABNT) estabeleceu somente em 2023, por meio da NBR ISO/IEC 27037, diretrizes para a identificação, coleta, aquisição e preservação de evidências digitais. Essas normas visam garantir a integridade e a confiabilidade das provas digitais, minimizando riscos de adulteração ou perda de dados durante o processo de coleta e análise(Associação Brasileira de Normas Técnicas, 2023).

Todavia a utilização da NBR ISO/IEC 27037 não é obrigatória por lei no Brasil, mesmo sendo altamente recomendada para assegurar a integridade e a confiabilidade das evidências digitais.

A falta de padronização legal nos métodos de coleta e análise de dados digitais agrava ainda mais o problema, tornando fundamental a implementação de protocolos robustos para garantir que apenas provas de alta qualidade e verificadas sejam admissíveis em processos judiciais, assegurando assim a justiça e a integridade do sistema legal.

Particularmente problemáticas para a PI são situações onde o suspeito ou acusado sofre uma limitação de sua liberdade ou privacidade com base em suspeitas vagas. Além das ameaças de desvio e erosão à PI, tais medidas podem ter efeitos adversos na qualidade das provas e no julgamento em geral.

2. *Crise de confiabilidade na perícia digital?*

No domínio jurídico, várias questões com provas forenses não confiáveis são relatadas e discutidas extensivamente. Vários relatórios concluíram que confissões falsas e provas forenses não confiáveis são fatores em condenações errôneas. Além disso, acadêmicos discutem sobre a superestimação sistemática do peso do testemunho de especialistas. Em muitas jurisdições, juízes continuam a não receber orientação real sobre como devem determinar a confiabilidade das provas, o que também leva ao tratamento desigual de suspeitos e réus.

As funções de *hash* são algoritmos matemáticos que transformam dados de qualquer tamanho em uma sequência fixa de caracteres, que funciona como uma «impressão digital» dos dados. Na perícia forense digital, essas funções são amplamente utilizadas para verificar a integridade de imagens, e-mails, mensagens e outros tipos de dados digitais(Kizza e Migga Kizza, 2011).

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

Por exemplo, quando um perito adquire uma imagem digital de um disco rígido para análise, ele utiliza uma função de *hash* como MD5 ou SHA-1 para gerar um valor de *hash* da imagem. Esse valor é então comparado com o valor de *hash* original em momentos posteriores para garantir que a imagem não foi alterada, assegurando a autenticidade dos dados analisados.

As funções de hash, como MD5 e SHA-1, são ferramentas fundamentais na perícia forense digital para garantir a integridade dos dados. No entanto, essas funções apresentam limitações significativas que podem comprometer a confiabilidade das provas digitais. Pesquisas demonstram que, sob condições controladas, é possível gerar dois arquivos distintos com o mesmo valor de *hash* MD5, fenômeno conhecido como colisão de *hash,* segundo Kyssa:

> Researchers have found that two files that have the same MD5 hash value can be generated under controlled conditions. Similar weaknesses have been found in other hashing algorithms, including SHA-1. Fortunately, this type of hash collision does not invalidate the use of MD5 or SHA-1 to document the integrity of digital evidence. (Kizza e Migga Kizza, 2011, p. 23)

Fraquezas semelhantes foram encontradas no SHA-1, o que levanta preocupações sobre a eficácia desses algoritmos em contextos forenses. Embora as colisões de *hash* não invalidem completamente o uso de MD5 e SHA-1 para documentar a integridade das evidências digitais, elas destacam a necessidade de cuidados adicionais na análise forense(Kizza e Migga Kizza, 2011, p. 23).

A fragilidade das provas digitais é exacerbada pela facilidade com que podem ser manipuladas ou destruídas. Evidências digitais podem ser alteradas ou obliteradas, tanto intencionalmente por infratores quanto acidentalmente durante a coleta, sem deixar sinais evidentes de adulteração(Kizza e Migga Kizza, 2011, p. 26).

Este fato torna crucial a manutenção de uma cadeia de custódia rigorosa e a implementação de procedimentos padronizados de manuseio de evidências. Falhas na documentação e preservação podem gerar dúvidas sobre a autenticidade e confiabilidade das provas apresentadas, prejudicando o processo judicial e a presunção de inocência dos acusados.

Além disso, as evidências digitais são, em grande parte, circunstanciais, dificultando a atribuição precisa de atividades de computador a indivíduos específicos. A natureza abstrata das provas digitais significa que pequenas mudanças no conteúdo podem resultar em valores de *hash* completamen-

te diferentes, complicando a verificação da integridade dos dados(Thamay e Tamer, 2020).

Para mitigar esses desafios, algumas ferramentas forenses digitais calculam automaticamente os valores de *hash* MD5 e SHA-1 das evidências adquiridas, proporcionando uma camada adicional de segurança. No entanto, mesmo essa abordagem pode não ser suficiente para garantir a confiabilidade absoluta das provas.

Finalmente, a rapidez com que a tecnologia evolui e a complexidade inerente às análises forenses introduzem uma margem de erro significativa. As ferramentas forenses, ao introduzirem uma camada adicional de abstração, podem gerar erros, como reconstruções incorretas ou incompletas de sistemas de arquivos e outras estruturas de dados(Kizza e Migga Kizza, 2011, p. 76).

A. *Suspeitas vagas*

A datafication pode resultar em limitações à liberdade ou privacidade de indivíduos com base em suspeitas infundadas ou vagas, simplesmente devido à facilidade de acesso a informações digitais.

A coleta e a análise de evidências digitais, como conteúdo de smartphones e computadores, tornaram-se rotineiras nas investigações criminais devido ao volume de dados relevantes contidos nesses dispositivos (Dias Moreira de Resende *et al.*, 2023).

No entanto, isso apresenta desafios significativos em relação à admissibilidade e confiabilidade das provas digitais. O artigo também destaca a importância da formação e capacitação de juízes e profissionais do direito para lidar com esses desafios (Dias Moreira De Resende *et al.*, 2023).

O fácil acesso a uma ampla gama de dados pessoais permite que as autoridades construam casos preliminares baseados em informações superficiais, muitas vezes sem a devida verificação ou validação.

Isso pode levar a ações injustas contra indivíduos que não são realmente culpados, mas que são investigados com base em dados facilmente acessíveis e interpretados de forma errônea ou fora de contexto.

Em um caso recente envolvendo o ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), gravações vazadas revelaram que um de seus assessores teria solicitado que um perito "usasse sua criatividade" ao produzir um relatório. As mensagens sugerem que a intenção era ajustar um documento a ser utilizado em investigações, o que gerou controvérsia

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

sobre a integridade das provas produzidas e a imparcialidade dos procedimentos periciais.

Esse tipo de comunicação levantou dúvidas sobre a neutralidade das provas no âmbito de investigações que envolvem temas sensíveis, como as milícias digitais e as *fake news*, nas quais Moraes desempenha um papel central. A Associação Nacional dos Peritos Criminais Federais criticou publicamente esse tipo de interferência, destacando que a produção de provas periciais deve ser regida por critérios científicos rigorosos e pela autonomia técnica dos peritos, garantindo a isenção necessária para o processo judicial.

A referida associação reforçou a importância de que os laudos periciais não sejam influenciados por demandas externas, enfatizando que os peritos devem agir de forma autônoma e imparcial, conforme previsto no Código de Processo Penal, para garantir que as provas apresentadas sejam justas e equidistantes das partes envolvidas no processo (Exame, 2023).

Essa situação suscitou debates na esfera pública e política, com grupos bolsonaristas levantando a possibilidade de interferência no processo eleitoral de 2022, questionando a legalidade das ações de Moraes no contexto das investigações das fake news e das milícias digitais. A controvérsia também reacendeu discussões sobre a necessidade de regulamentar de maneira mais rigorosa o papel dos peritos e a relação entre autoridades e produção de provas (DW, 2024).

B. *Processamento Massivo de Dados*

A quantidade crescente de dados processados nas investigações criminais pode levar a uma sobrecarga de informações, onde provas incriminatórias podem ser encontradas entre grandes volumes de dados irrelevantes.

Essa sobrecarga dificulta a identificação de informações verdadeiramente pertinentes e pode resultar na inclusão de dados desnecessários, confundindo o processo investigativo e judicial. Além disso, a prática de corroborar dados digitais para construir um caso contra um suspeito pode obscurecer a verdade ao apoiar narrativas preexistentes, criando uma espécie de incidente de "falsas memórias digitais" (Lima e Venturin, 2020).

Dessa forma, dados que confirmam hipóteses iniciais são privilegiados, enquanto informações que poderiam fornecer uma visão mais equilibrada são negligenciadas, comprometendo a equidade do julgamento.

A disponibilidade de vastas quantidades de dados digitais pode induzir os investigadores a focarem em informações que confirmem suas hipóteses iniciais, negligenciando dados que possam exonerar o suspeito.

Esse fenômeno, conhecido como visão em túnel, pode levar a erros judiciais graves, uma vez que os investigadores se concentram em construir um caso ao invés de explorar todas as possibilidades de forma imparcial.

A visão em túnel é exacerbada pela pressão para resolver casos rapidamente, o que pode resultar em investigações superficiais e parciais, comprometendo a justiça. O caso de Johnny Depp (Bedigan, 2022; Depp V. Heard - Wikipedia, [*s. d.*]; Wallis, [*s. d.*]) é o paradigma perfeito do processo de datatificação, visão de túnel e qualidade das provas que provocou a condenação prévia pela mídia pode resultar em enormes prejuízos antes mesmo de um veredito judicial. Após as acusações de violência doméstica feitas por sua ex-esposa, Amber Heard, Depp enfrentou uma série de consequências profissionais e pessoais, incluindo a perda de papéis importantes em grandes franquias de Hollywood, como "Piratas do Caribe". A cobertura midiática intensa e frequentemente unilateral contribuiu para a sua queda de imagem pública. No entanto, durante o julgamento de difamação de 2022, Depp foi absolvido das acusações mais graves, com o júri concluindo que Heard havia agido com malícia ao publicar um artigo de opinião que insinuava abuso.

Este veredito não apenas restaurou a reputação de Depp, mas também ressaltou os danos irreparáveis que podem ser causados pela mídia ao influenciar a opinião pública antes do devido processo legal

3. *Circunvenção tecnológica*

A captura extensiva e sistemática de dados sobre suspeitos pelo Estado torna outras medidas – que são bem adaptadas ao procedimento criminal, como interrogatório, exame de testemunhas ou até mesmo detenção – inúteis, uma vez que o Estado pode "*hackear*" seu caminho para os detalhes mais íntimos da vida dos suspeitos (Dias Moreira De Resende *et al.*, 2023).

Preferir dados em vez de métodos policiais clássicos não apenas aumenta o perigo de conclusões errôneas e prematuras na investigação, mas evita o procedimento criminal por completo, pois diminui os direitos associados a um interrogatório ou direitos e garantias de declarações de testemunhas.

A falta de "descoberta precoce e completa desfavorece os inocentes factual mais do que qualquer outro conjunto de réus"(citação própria), como

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

argumentado, e isso é particularmente problemático na atual dependência excessiva da tecnologia.

Temos por exemplo os casos de buscas em bancos de dados e identificações por fotos feitos por algoritmos, tais buscas podem resultar em identificações equivocadas porque se baseiam na semelhança física com o perpetrador, o que pode ser altamente impreciso(Risinger e Risinger, 2011).

Até mesmo as evidências de DNA e problemas de "*Cold Hits*", onde perfis de DNA são comparados com grandes bancos de dados na esperança de encontrar uma correspondência. Isso pode resultar em problemas se as condições de busca não forem bem compreendidas pelos jurados, levando-os a dar peso excessivo a coincidências que podem ser estatisticamente esperadas em grandes conjuntos de dados (Risinger e Risinger, 2011).

Esses pontos destacam a complexidade e os riscos envolvidos no uso de provas digitais e identificações baseadas em bancos de dados e esboços, enfatizando a necessidade de procedimentos rigorosos e imparciais para proteger os inocentes no sistema de justiça criminal.

4. *Desafios recentes e impacto das tecnologias na validação das provas digitais*

Nos últimos anos, o uso de tecnologias avançadas, como análise de DNA e inteligência artificial (IA), trouxe inovações significativas ao processo de investigação criminal. No entanto, tais avanços também têm sido acompanhados por uma série de desafios e riscos que afetam a equidade e a confiabilidade das provas digitais nos tribunais (Andrea *et al.*, 2022; Cataleta, 2023; Heffernan, 2008).

IV. A Fragilidade da Prova de DNA

A análise de DNA é amplamente reconhecida como uma poderosa ferramenta de identificação em casos criminais, mas pesquisas recentes demonstram que ela não está isenta de erros. A formação de perfis de DNA, mesmo quando completa, pode coincidir com a de indivíduos que não têm relação com o crime. Perfis parciais, por sua vez, apresentam ainda mais riscos, pois podem corresponder a múltiplas pessoas, aumentando as chances de condenações equivocadas. Além disso, erros de laboratório, como a mistura acidental de amostras de múltiplos indivíduos, podem levar à geração de perfis

equivocados. Portanto, a análise de DNA deve ser interpretada com cautela e em conjunto com outras provas, utilizando métodos estatísticos rigorosos, como a razão de verossimilhança, para avaliar a probabilidade de a amostra pertencer ao suspeito comparada com a hipótese de ser de outra pessoa (Chow-White e Duster, 2011; Debenedictis D J, 1992; Dodd *et al.*, 2012; Elster, 2017; Heffernan, 2008; Sterritt, 2006; Syndercombe, 2017).

Casos recentes, como o de um homem com doença de Parkinson condenado por um crime devido a um perfil parcial de DNA, demonstram os perigos de confiar excessivamente nesta tecnologia. Após análises adicionais, ele foi exonerado, evidenciando que a análise de DNA, quando isolada e mal interpretada, pode levar a graves erros judiciais. A sensibilidade crescente das tecnologias de DNA também apresenta uma faca de dois gumes. Por um lado, possibilita a detecção de evidências mais utilizáveis, mas, por outro, aumenta a probabilidade de detecção de DNA transferido secundariamente ou contaminado, confundindo investigações e decisões judiciais (Dodd *et al.*, 2012).

Além disso, o uso de bancos de dados de DNA levanta questões éticas e de privacidade. A manutenção de perfis de DNA em bases de dados, especialmente quando incluem parentes de suspeitos, pode levar a falsas identificações. Um estudo de 2011 questionou se essas bases de dados poderiam aumentar disparidades raciais, destacando que comunidades menos privilegiadas tendem a ser super-representadas nesses bancos de dados, resultando em identificação errônea de suspeitos e perpetuando desigualdades no sistema de justiça criminal (Chow-White e Duster, 2011; Dodd *et al.*, 2012).

V. IA e previsão criminal

A aplicação de inteligência artificial (IA) em práticas policiais tem gerado preocupações significativas sobre a equidade e confiabilidade das provas digitais. Programas que utilizam IA para prever crimes são frequentemente alimentados por dados históricos, o que pode perpetuar vieses existentes, especialmente em comunidades sub-representadas. Se bairros específicos são identificados como "de alto risco", a alocação de mais policiais nessas áreas pode criar um ciclo de retroalimentação, reforçando falsas ideias sobre a localização dos crimes. Em muitos casos, os algoritmos replicam vieses ao analisar dados pré-existentes, resultando em um policiamento que pode aumentar desigualdades sociais e raciais(Yeung, Khan, Kalra, e Osoba, 2021).

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

Uma problemática adicional é a falta de supervisão humana nos processos automatizados. À medida que as agências policiais dependem cada vez mais de ferramentas de aprendizado profundo, as decisões dos algoritmos são muitas vezes tomadas como definitivas e inquestionáveis. Isso cria um "vazio de responsabilidade", no qual nem os desenvolvedores das tecnologias nem as agências que as utilizam se responsabilizam pelos danos resultantes de decisões equivocadas. A consequência é um sistema automatizado que pode agir de forma autônoma, afetando diretamente os direitos dos indivíduos sem a devida prestação de contas (Cataleta, 2023).

Em termos de reconhecimento facial, um exemplo extremo da falha dos algoritmos é a rotulação incorreta de indivíduos negros em sistemas de reconhecimento facial, como no caso em que um algoritmo do Facebook identificou erroneamente pessoas negras como "primatas". Isso não apenas reflete uma deficiência técnica, mas também um problema ético, pois tais sistemas são cada vez mais utilizados em processos judiciais e policiais. Quando esses algoritmos são empregados sem treinamento, apoio ou supervisão significativa, as injustiças e erros cometidos tornam-se ainda mais graves (Cataleta, 2023).

VI. Caminhos a Seguir

A crescente conscientização sobre as limitações dessas tecnologias ressalta a importância de utilizá-las com cautela e em conjunto com outras evidências. Os avanços em DNA e IA têm potencial para auxiliar investigações, mas não devem ser supervalorizados nos tribunais. É fundamental implementar regulamentações rigorosas para o uso dessas tecnologias, exigindo protocolos de validação científica e transparência. Além disso, a necessidade de supervisão humana e treinamento adequado para interpretar corretamente as análises tecnológicas se faz urgente, a fim de evitar erros judiciais e promover a justiça de forma imparcial.

VII. Desafiando a proporcionalidade com confiabilidade

A partir da análise até agora, pode-se ver que o uso da tecnologia pode auxiliar em cada etapa do processo de investigação, mas obscurece as linhas

entre prevenção e investigação de crimes e pode infringir os direitos de suspeitos, grupos de pessoas ou da sociedade como um todo.

Leis de proteção de dados aumentaram a rigidez do princípio da proporcionalidade em relação às medidas de investigação digital, como coleta de dados sobre contatos e associados (ou seja, sobre pessoas não suspeitas de envolvimento em um crime específico ou de representar uma ameaça), a coleta de informações por meios intrusivos e secretos (interceptação telefônicas e de *e-mails*), e o uso de técnicas de 'perfilamento', e de fato a policiamento 'preventivo' em geral, deve ser submetido a um teste de necessidade e proporcionalidade particularmente aprofundado(Kizza e Migga Kizza, 2011).

A Lei Geral de Proteção de Dados (LGPD) no Brasil, instituída pela Lei nº 13.709/2018(Brasil, 2018), estabeleceu diretrizes rigorosas para a coleta, armazenamento e tratamento de dados pessoais, reforçando a necessidade de proporcionalidade e necessidade nas práticas investigativas.

A LGPD determina que o tratamento de dados deve ser limitado ao mínimo necessário para a realização de suas finalidades, restringindo o acesso a dados sensíveis e impondo sanções severas para o uso inadequado dessas informações (Brasil, 2018).

Sob o prisma da presunção de inocência embora a LGPD imponha restrições à coleta e ao tratamento de dados, ela não estabelece diretrizes claras sobre como essas restrições devem ser aplicadas em contextos investigativos, deixando espaço para interpretações que podem prejudicar os investigados.

Por fim, a LGPD não contempla suficientemente as particularidades das provas digitais e as complexidades associadas ao seu uso em processos judiciais. A lei trata os dados pessoais de forma geral, sem considerar as especificidades das provas digitais, como a necessidade de preservar a cadeia de custódia e garantir a autenticidade e integridade das informações.

1. *O juiz pode influenciar a perícia, não o perito*

Com a devida vênia das magnificas palavras do Geraldo Padro (2005, p. 279):

> Não há dúvida de que o acusado tem a temer pela tendenciosidade precocemente demonstrada pelo juiz, antes mesmo da dedução da ação penal. Dizia-se com razão, na Idade Média, que aquele que tem um juiz por acusador, precisa de Deus como defensor. E, às vezes, isso não é suficiente.

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

Este magnifico brocardo da idade média, aquele que tem um juiz como acusador, precisa de Deus como defensor, diga-se de passagem por estas plagas nem Ele parece ser o suficiente ante ao corporativismo monolítico de uma corte sem nenhuma amalgama dissonante (RSP, 2024).

A imparcialidade e autonomia do perito são pilares fundamentais para garantir a legitimidade da prova pericial no processo judicial. O papel do juiz, como garantidor do devido processo legal, inclui a possibilidade de indeferir uma perícia quando ela não se mostra necessária, mas não de modificar ou direcionar o conteúdo técnico produzido pelo perito.

Quando o magistrado intervém diretamente na produção da prova pericial, ele compromete a isenção e integridade da investigação, prejudicando o princípio do contraditório e da ampla defesa. Recentes revelações envolvendo o ministro Alexandre de Moraes, que trataremos a frente, levantam preocupações sobre até que ponto essa interferência pode ocorrer, abordando a questão da independência do perito e o limite da atuação judicial.

A. *A Importância da Independência do Perito*

Vejamos o artigo 159 do Código de Processo Penal:

> *Art. 159. O exame de corpo de delito e outras perícias serão realizados por* perito oficial, portador de diploma de curso superior.(Redação dada pela Lei nº 11.690, de 2008)
> § 1o Na falta de perito oficial, o exame será realizado por 2 (duas) pessoas idôneas, portadoras de diploma de curso superior preferencialmente na área específica, dentre as que tiverem habilitação técnica relacionada com a natureza do exame. (Redação dada pela Lei nº 11.690, de 2008)
> § 2o Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo. (Redação dada pela Lei nº 11.690, de 2008)
> § 3o Serão facultadas ao Ministério Público, ao assistente de acusação, ao ofendido, ao querelante e ao acusado a formulação de quesitos e indicação de assistente técnico. (Incluído pela Lei nº 11.690, de 2008)
> § 4o O assistente técnico atuará a partir de sua admissão pelo juiz e após a conclusão dos exames e elaboração do laudo pelos peritos oficiais, sendo as partes intimadas desta decisão. (Incluído pela Lei nº 11.690, de 2008)
> § 5o Durante o curso do processo judicial, é permitido às partes, quanto à perícia: (Incluído pela Lei nº 11.690, de 2008)

> I – requerer a oitiva dos peritos para esclarecerem a prova ou para responderem a quesitos, desde que o mandado de intimação e os quesitos ou questões a serem esclarecidas sejam encaminhados com antecedência mínima de 10 (dez) dias, podendo apresentar as respostas em laudo complementar; (Incluído pela Lei nº 11.690, de 2008)
> II – indicar assistentes técnicos que poderão apresentar pareceres em prazo a ser fixado pelo juiz ou ser inquiridos em audiência. (Incluído pela Lei nº 11.690, de 2008)
> § 6o Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação. (Incluído pela Lei nº 11.690, de 2008)
> § 7o Tratando-se de perícia complexa que abranja mais de uma área de conhecimento especializado, poder-se-á designar a atuação de mais de um perito oficial, e a parte indicar mais de um assistente técnico. (Incluído pela Lei nº 11.690, de 2008)

Este artigo estabelece que a perícia deve ser conduzida por peritos oficiais, que possuem conhecimento técnico e científico suficiente para esclarecer questões que fogem à competência do magistrado e das partes, ressalta ainda que a perícia deve ser imparcial, ou seja, os peritos devem ter liberdade técnica para produzir suas conclusões sem pressões externas, sejam elas das partes envolvidas ou do próprio juiz. A Lei deixa claro que, para garantir a lisura do processo, os laudos periciais devem ser baseados exclusivamente em critérios científicos, sem qualquer viés ou influência externa.

O Código de Processo Civil (CPC), no artigo 473, também aborda a independência do perito, determinando que o laudo deve ser realizado com base em metodologia científica, cabendo ao juiz, na análise final da prova, indicar os motivos pelos quais acolhe ou rejeita o parecer do perito. Isso reforça que a apreciação da prova pericial é um direito do juiz, mas a sua modificação não.

B. *O Caso do Ministro do STF Alexandre de Moraes e a Revista Oeste*

Mensagens vazadas revelaram uma prática preocupante em que o Ministro Alexandre de Moraes e seus auxiliares, por meio de canais informais, orientavam peritos a ajustar relatórios periciais. Um caso notório envolve a Re-

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

vista Oeste, quando, em dezembro de 2022, um juiz instrutor do gabinete de Moraes sugeriu ao perito responsável que "usasse sua criatividade" para incluir críticas mais ácidas contra o veículo, após não encontrar elementos substanciais que justificassem a inclusão da publicação em investigações sobre desinformação nas eleições de 2022, segue ipsis literis o texto de um grande jornal brasileiro divulgando estes fatos (DW, 2024; Ferreira, 2024):

> Em dezembro de 2022, Vieira enviou mensagem a Tagliaferro com um pedido específico. Segundo o jornal, o juiz instrutor de Moraes pediu ao técnico do TSE um levantada sobre "revistas golpistas para desmonetizar nas redes". A solicitação foi acompanhada de um link do X (antigo Twitter) da revista Oeste.
> No dia seguinte ao pedido, Tagliaferro reportou que encontrou apenas "publicações jornalísticas" na Oeste e questionou o auxiliar de Moraes sobre o que deveria colocar no documento. "Use a sua criatividade[...] rsrsrs", respondeu Vieira, orientando Tagliaferro a inserir no relatório "opiniões mais ácidas". "O Ministro [Alexandre de Moraes] entendeu que está extrapolando com base naquilo que enviou", completou [grifo nosso].

A mensagem trocada via WhatsApp orientava o perito a "desmonetizar revistas golpistas" e "inserir opiniões mais ácidas", indicando uma tentativa de manipulação da prova para fins que favorecessem a narrativa do magistrado (DW, 2024; Ferreira, 2024).

Essa interferência vai diretamente contra o que preconiza o CPP e o CPC. A atuação de Alexandre de Moraes e seus auxiliares, conforme descrito nas mensagens vazadas, extrapola o papel de um juiz na condução de investigações, afetando diretamente a credibilidade da perícia e, por extensão, a confiança no processo judicial. A situação em questão revela uma tentativa de personalizar o conteúdo técnico para justificar uma determinada postura jurídica, algo que fere a independência do perito.

C. *O Juiz Pode Indeferir a Perícia, Não Modificá-la*

O artigo 480 do CPC estabelece que o juiz pode indeferir a realização de uma perícia quando considerar que a prova não é necessária para o caso, seja por já existirem elementos suficientes no processo, seja porque a questão não exige conhecimento técnico especializado. No entanto, após a realização da perícia, o juiz não tem o poder de modificar o conteúdo do laudo. Ele pode discordar das conclusões do perito, mas deve fundamentar sua de-

cisão com base em outros elementos do processo, como testemunhos ou documentos que contradigam as conclusões técnicas.

D. *Apreciação da Prova Pericial e Limites da Influência Judicial*

O juiz tem o direito de apreciar a prova pericial com base no princípio do livre convencimento motivado, previsto no artigo 371 do CPC. Esse princípio dá ao magistrado a liberdade para formar sua convicção a partir das provas dos autos, incluindo a perícia. Contudo, essa liberdade não deve ser confundida com a possibilidade de direcionar o conteúdo técnico produzido pelos peritos. Qualquer tentativa de modificar a prova técnica compromete a integridade do processo e o princípio da imparcialidade.

No caso envolvendo a *Revista Oeste*, fica claro que o juiz auxiliar instruiu o perito a adaptar o relatório para adequar-se a uma narrativa previamente estabelecida, o que fere a independência da prova pericial e os princípios constitucionais do devido processo legal e da ampla defesa (DW, 2024; Ferreira, 2024).

O juiz pode indeferir uma perícia quando ela for desnecessária, pode discordar do laudo pericial com base em outros elementos dos autos, e pode desconsiderá-lo se houver provas que o contradigam. No entanto, o juiz não pode instruir o perito a modificar seu laudo, muito menos orientar o uso de "criatividade" na elaboração das provas, como revelado no caso de Alexandre de Moraes. Qualquer tentativa de influenciar diretamente o conteúdo técnico compromete a imparcialidade do processo, fragiliza a confiança nas instituições e coloca em risco o princípio da justiça.

VIII. Conclusão

A crescente utilização de provas digitais nos processos penais levanta preocupações sérias sobre a preservação dos princípios fundamentais do devido processo legal, em especial a *presunção de inocência* e a *equidade* no julgamento. À medida que as tecnologias avançam, a coleta, análise e apresentação de provas digitais se tornam cada vez mais comuns, mas a falta de regulamentação e validação científica robusta dessas evidências ainda representa uma ameaça significativa para a justiça.

Como observado, a falta de padronização legal para a coleta e verificação de provas digitais no Brasil é um problema que persiste e compromete

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

a integridade do processo penal. Embora a NBR ISO/IEC 27037 tenha sido introduzida para fornecer diretrizes sobre a identificação, coleta, aquisição e preservação de evidências digitais, ela ainda não é obrigatória por lei. A ausência de normas jurídicas vinculativas em relação às provas digitais permite que essas evidências sejam aceitas sem a devida verificação de sua autenticidade e integridade, o que, por sua vez, compromete os direitos dos acusados, em particular o direito de contestar as provas apresentadas.

As ameaças à *presunção de inocência* são amplamente exacerbadas pelo fenômeno da *dataficação*, em que aspectos da vida cotidiana são transformados em dados digitais. Como vimos, a coleta massiva de dados digitais pode levar a erros judiciais, onde os dados são interpretados fora de contexto, ou pior, mal utilizados para criar uma narrativa incriminatória contra o suspeito. Isso gera uma "visão em túnel", na qual os investigadores se concentram apenas nos dados que confirmam suas hipóteses iniciais, desconsiderando informações que poderiam fornecer uma visão mais equilibrada dos fatos. A utilização crescente de *inteligência artificial* e *algoritmos automatizados* também levanta preocupações sobre a imparcialidade e transparência desses processos, especialmente quando estudos demonstram que esses algoritmos podem conter vieses implícitos que afetam desproporcionalmente grupos minoritários.

Além disso, a confiabilidade das *provas digitais* é questionada devido à facilidade com que podem ser manipuladas, adulteradas ou mal interpretadas. As funções de *hash*, amplamente utilizadas para garantir a integridade dos dados, apresentam vulnerabilidades que podem ser exploradas para alterar ou ocultar evidências. Como discutido, as colisões de hash no MD5 e no SHA-1, embora raras, são possíveis e, quando ocorrem, comprometem a autenticidade das provas digitais, prejudicando o processo penal. A fragilidade da prova digital torna essencial a implementação de protocolos rigorosos para garantir sua integridade desde o momento da coleta até sua apresentação em tribunal.

O recente caso envolvendo o ministro Alexandre de Moraes e as mensagens vazadas que indicam uma interferência na produção de laudos periciais ilustra a gravidade do problema. A sugestão de que peritos "usem sua criatividade" para ajustar relatórios compromete a independência técnica dos peritos e, por consequência, a confiabilidade das provas produzidas. A tentativa de direcionar a prova pericial para apoiar uma narrativa específica viola diretamente os princípios da imparcialidade e da ampla defesa, colocando em risco o direito a um julgamento justo.

Este caso ressalta a importância de que o *juiz* exerça seu papel como *garantidor do devido processo legal*, respeitando a independência do perito e limitando sua atuação à apreciação das provas apresentadas. Como observado no *Código de Processo Penal* e no *Código de Processo Civil*, o juiz tem a prerrogativa de indeferir uma perícia quando não for necessária ou se houver outros elementos suficientes no processo. No entanto, uma vez realizada a perícia, o juiz não tem o poder de modificar o conteúdo do laudo pericial. Ele pode discordar das conclusões, desde que fundamente sua decisão com base em outros elementos dos autos, mas não pode instruir o perito a ajustar suas conclusões de acordo com uma narrativa previamente estabelecida.

Esse tipo de interferência não apenas compromete a confiabilidade das provas, mas também mina a confiança pública no sistema de justiça. A ideia de que o poder judiciário, que deveria ser imparcial, possa influenciar diretamente o conteúdo técnico das provas levanta questões sérias sobre a integridade do processo judicial. Quando o perito é pressionado a adaptar suas conclusões para atender a demandas externas, o sistema legal falha em garantir um julgamento justo, violando os direitos fundamentais dos acusados.

A *preservação da imparcialidade do perito* é crucial para garantir que as provas apresentadas em tribunal sejam confiáveis e justas. A independência técnica do perito deve ser respeitada em todas as etapas do processo judicial, desde a coleta de dados até a análise e apresentação das conclusões. Somente dessa forma o sistema de justiça pode assegurar que as provas digitais, que já são inerentemente complexas e suscetíveis a falhas, sejam tratadas com o rigor e a imparcialidade necessários para garantir um julgamento justo.

No entanto, além das questões técnicas e processuais, é fundamental que haja uma *intervenção legislativa* que estabeleça normas claras e obrigatórias para a coleta e análise de provas digitais. A legislação atual, embora tenha dado passos importantes com a implementação da Lei Geral de Proteção de Dados (LGPD), ainda carece de diretrizes específicas para as provas digitais no contexto do processo penal. A LGPD impõe restrições à coleta e ao tratamento de dados pessoais, mas não aborda diretamente as peculiaridades das provas digitais, como a necessidade de garantir a autenticidade e integridade dos dados durante todo o processo investigativo e judicial.

Uma *harmonização internacional* dos padrões forenses digitais também é essencial para garantir a justiça. À medida que as investigações criminais se tornam cada vez mais globais, com dados armazenados em servidores localizados em diferentes países e informações compartilhadas entre juris-

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

dições, é crucial que os padrões para a coleta e análise de provas digitais sejam uniformes em todo o mundo. Isso não apenas garantiria a confiabilidade das provas, mas também asseguraria que os direitos dos acusados sejam protegidos de maneira equitativa, independentemente da jurisdição em que o caso esteja sendo julgado.

Portanto, o uso de provas digitais no sistema judicial exige uma abordagem cuidadosa e rigorosa. Sem a devida regulamentação e validação científica dessas evidências, corremos o risco de comprometer a presunção de inocência e a equidade no julgamento. As tecnologias, embora poderosas, trazem consigo desafios éticos e legais que não podem ser ignorados. A confiabilidade das provas digitais deve ser garantida por meio de normas claras, procedimentos rigorosos e respeito à independência técnica dos peritos. Somente assim podemos assegurar que a justiça seja feita de maneira imparcial e que os direitos fundamentais dos acusados sejam devidamente protegidos.

A *urgência* de uma intervenção legislativa que regule adequadamente a utilização de provas digitais é evidente. O sistema de justiça precisa se adaptar às mudanças tecnológicas, mas sem comprometer os direitos dos cidadãos. A implementação de *padrões mínimos* para a coleta, preservação e análise de provas digitais, bem como a adoção de *procedimentos robustos* para a validação científica dessas evidências, são passos essenciais para garantir a integridade do processo penal.

Finalmente, a cooperação internacional e a harmonização dos padrões forenses digitais são fundamentais para garantir a justiça em um mundo cada vez mais interconectado. Ao padronizar as práticas forenses digitais e garantir que as provas digitais sejam tratadas com o rigor necessário, podemos assegurar que o *direito a um julgamento justo* seja respeitado em todas as jurisdições. As ameaças não resolvidas à presunção de inocência e à equidade no uso de provas digitais precisam ser enfrentadas com urgência, para que o sistema de justiça possa evoluir sem comprometer seus princípios fundamentais.

IX. Referências

Andrea, M., Ortega, C., Alberto, C., e Calderón, C. (2022). Artificial intelligence evidence: A proposal for evidence production from the perspective of scientific expert opinion in Colombia. *Civilizar Ciencias Sociales y Humanas*, *22*(42), e20220106.

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-89532022000100106&lng=en&nrm=iso&tlng=es

Associação Brasileira de Normas Técnicas (2023). *ABNT Catálogo*. https://www.abntcatalogo.com.br/pnm.aspx?Q=NDlLZHR1a1ZUajFjTy80SjIvNXphZnBrMFhuRHpnQmQxeXUrRnRIN3JYND0=

Bedigan, M. (2022). Amber Heard set for "meteoric rise" before Depp lawyer's "defamatory" comments. *The Independent*. https://www.independent.co.uk/news/uk/crime/amber-heard-kate-moss-jason-momoa-wonder-woman-james-wan-b2085768.html

Brasil. (2018). *LEI 13.709*. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Capanema, W. A. (2024). *Teoria e Prática*.

Cataleta, M. S. (2023). *East-West Center Humane Artificial Intelligence The Fragility of Human Rights Facing AI*. https://hal.science/hal-03289002

Chow-White, P. A. e Duster, T. (2011). Do Health and Forensic DNA Databases Increase Racial Disparities?. *PLoS Medicine*. *8*(10). /pmc/articles/PMC3186804/

Risinger, D. M. e Risinger, L. C. (2011). Innocence Is Different : Taking Innocence into Account in Reforming Criminal Procedure. *Reforming Criminal Procedure*. *56*(3), 869-909. https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=1663&context=nyls_law_review

Debenedictis, D. J. (1992). DNA Report Raises Concerns: Study Backs Genetic Evidence, But Questions Reliability of Labs, Statistics. *ABA Journal*, [*s. l.*], *78*(7), 20, https://www.jstor.org/stable/27830704?mag=-forensic-dna-evidence-can-lead-wrongful-convictions

Depp V. Heard - Wikipedia. (s. d.). https://en.wikipedia.org/wiki/Depp_v._Heard

Dias Moreira de Resende, C. E., Berkenbrock, G. E., O. Saboia Ribeiro, L. O., Dellape Gomes, M. (2023). Prova Digital No Processo Judicial. *Revista Judicial Brasileira*, *3*, 145-186. https://revistadaenfam.emnuvens.com.br/renfam/article/view/222

Dodd, V., Bowcott, O., Malik, S. (2012). Forensics firm investigated over DNA blunder in rape case | UK criminal justice. *The Guardian*. https://www.theguardian.com/law/2012/mar/09/forensics-firm-investigated-dna

DW. (2024). *Alexandre de Moraes: o que indicam as mensagens vazadas – DW – 14/08/2024*. https://www.dw.com/pt-br/alexandre-de-moraes-o-que-indicam-as-mensagens-vazadas/a-69936500

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396

Elster, N. (2017). *How Forensic DNA Evidence Can Lead to Wrongful Convictions*. https://daily.jstor.org/forensic-dna-evidence-can-lead-wrongful-convictions/

Exame. (2023). Peritos federais veem parcialidade e questionam isenção de relatório da PF no caso Moraes. *Exame*. https://exame.com/brasil/peritos-federais-veem-parcialidade-e-questionam-isencao-de-relatorio-da-pf-no-caso-moraes/

Ferreira, Z. (2024). *'Use sua criatividade', diz juiz auxiliar de Moraes ao pedir investigação contra revista Oeste - Estadão*. https://www.estadao.com.br/politica/use-criatividade-juiz-auxiliar-moraes-pedir-investigacao-contra-oeste-nprp/

Heffernan, L. (2008). Genetic Policing: The Use of DNA in Criminal Investigations. By Robin Williams and Paul Johnson (Willan Publishing). https://academic.oup.com/bjc/article-abstract/48/5/699/530474

Convenção Americana sobre Direitos Humanos (Assinada na Conferência Especializada Interamericana sobre). https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Kizza, J.e e Migga Kizza, F. (2011). *Digital Evidence and Computer Crime*. 2011.

Lima, U. D. M. R. dee e Venturin, E. V. D. F. (2020). O Incidente das Falsas Memórias no Processo Penal Frente ao Valor Probatório da Palavra da Vítima / The Incident of False Memories in the Criminal Process in Front of the Probatory Value of the Victim's Word. *ID on line Revista De Psicologia*. *14*(52), 855-878. https://www.jusbrasil.com.br/artigos/o-incidente-das-falsas-memorias-no-processo-penal-frente-ao-valor-probatorio-da-palavra-da-vitima/1114247883

Mariobo Franck, K., Vitorino Ferreira, R., Ji-Paraná, L., Ji-Paraná Av Engenheiro Manfredo Barata, C., e Aurélio Bernardes, B. (s.d.) Instruções preventivas contra crimes cybernéticos e orientações da perícia forense computacional. *jiparana.emnuvens.com.br*, 2023. https://jiparana.emnuvens.com.br/riacti/article/view/689

Padilha, R.; Theóphilo, A.; Andaló, F. A.; Vega-Oliveros, D. A.; Cardenuto, J. P.; Bertocco, G.; Nascimento, J.; Yang, J.; Rocha, A. (2021). A Inteligência Artificial e os desafios da Ciência Forense Digital no século XXI. *Estudos Avancados*, *35*(101), 111-138.

Prado, G. (2005). *Sistema Acusatório* (3oed.). Rio de Janeiro.

RSP, R. do S. P. (2024). Supremo Tribunal Federal. *Revista do Serviço Público*, *84*(1), 87-91. https://noticias.stf.jus.br/postsnoticias/stf-confirma-decisao-que-suspendeu-o-x-antigo-twitter-em-todo-o-pais/

Segata, J. e Sociais, T. R.-C.-R. de C. (2021). Digitalização e dataficação da vida. SciELO Brasil. https://www.scielo.br/j/civitas/a/DRHF8GbQTKw8Jt3rXBVJt9w/?lang=pt

Sterritt, D. (s.d.). *JSTOR*, 1006. https://www.jstor.org/stable/23639511?mag=forensic-dna-evidence-can-lead-wrongful-convictions

STJ (2024). *Julgamento Eletrônico*. https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=242041837&registro_numero=202301896150&peticao_numero=202300906480&publicacao_data=20240429&formato=PDF

Syndercombe, D. (2017). *Making Sense of Forensic Genetics – Sense about Science*. https://senseaboutscience.org/activities/making-sense-of-forensic-genetics/

Thamay, R. e Tamer, M. (2020). *Provas no Direito Digital: conceito da prova digital, procedimentos e provas digitais em espécie*.

Wallis, N. (s.d.). *Depp v Heard : the unreal story*. 305.

Yeung, Douglas; Khan, Inez; Kalra, Nidhi; Osoba, O. A. (2021). *Identifying Systemic Bias in the Acquisition of Machine Learning Decision Aids for Law Enforcement Applications*. https://www.jstor.org/stable/resrep29576

Cómo citar

IIJ-UNAM

Pereira Passos, João Pedro, "Provas digitais: ameaças não resolvidas à equidade e à presunção de inocência", *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, México, vol. 27, núm. 54, enero-junio de 2026, e19396. https://doi.org/10.22201/iij/24484881e.2026.54.19396

APA

Pereira Passos, J. P. (2026). Provas digitais: ameaças não resolvidas à equidade e à presunção de inocência, *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, *27*(54), e19396. https://doi.org/10.22201/iij/24484881e.2026.54.19396

e-ISSN: 2448-4881 | DOI: https://doi.org/10.22201/iij.24484881e.2026.54.19396