XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO IV

MATEUS EDUARDO SIQUEIRA NUNES BERTONCINI

THIAGO ALLISSON CARDOSO DE JESUS

CALEB SALOMÃO PEREIRA

D597

Direito penal, processo penal e constituição IV[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Mateus Eduardo Siqueira Nunes Bertoncini, Thiago Allisson Cardoso De Jesus, Caleb Salomão Pereira – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-315-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO IV

Apresentação

No âmbito da Universidade Mackenzie, aqui consolidou-se mais um sessão do GT DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO IV, valiosa reunião de pesquisadores/as das diversas regiões do Brasil, oriundos de distintos programas de pós-graduação, da Iniciação Científica e de experiências técnicas e intervenções diretas. Nesse giro, a autora Ana Luiza Morato apresentou o trabalho intitulado REFLEXÕES SOBRE O CASO DANIEL ALVES E O FUTURO DO DIREITO EM MATÉRIA DE GÊNERO. O trabalho investiga como o processo citado, julgado na Espanha, seria analisado pela Justiça brasileira à luz de um protocolo de julgamento com perspectiva de gênero. A autora dialoga com a doutrina (Robalo e Taruffo, e.g.) para demonstrar que, mesmo com a aplicação de tais protocolos, o resultado não seria, a priori, diverso do original, pois eles não se sobrepõem às garantias constitucionais, tais como a presunção de inocência e o devido processo legal. O estudo aponta que a controvérsia central residiu nas narrativas sobre consentimento e que a palavra da vítima, embora relevante, não pode operar como presunção absoluta de vitimização sem corroboração por outros elementos probatórios. Conclui-se que os protocolos de gênero são ferramentas de proteção e de depuração de vieses, úteis para orientar investigações, mas que não constituem regras de julgamento aptas a afastar os standards probatórios em matéria penal.

Na sequência, o artigo elaborado por Pollyana Pereira da Cruz, Alfredo Ribeiro da Cunha Lobo, Willian Tosta Pereira de Oliveira, cujo título é CADEIA DE CUSTÓDIA COMO MECANISMO EPISTÊMICO: OMISSÃO NA LEGISLAÇÃO E A IMPORTÂNCIA DA PROVA DIGITAL NO PROCESSO PENAL BRASILEIRO. O artigo analisa a integridade da cadeia de custódia como mecanismo epistêmico no processo penal brasileiro, crucial para garantir a confiabilidade e validade das provas digitais. A pesquisa destaca que a Lei nº 13.964/2019 trouxe mudanças significativas, mas se omitiu sobre o tratamento da prova digital na cadeia de custódia. O artigo argumenta que, mesmo sem previsão legal expressa para a prova digital, sua validade depende da observância da cadeia de custódia para garantir a idoneidade e inviolabilidade do vestígio digital. Conclui que a ausência de regulamentação específica sobre a prova digital na cadeia de custódia não impede a validação da prova, mas reforça a necessidade de sua observância rigorosa para proteger os direitos de defesa e a integridade do sistema legal, mitigando o risco de informações falseadas. Na sequencia, o artigo elaborado por Felipe dos Santos Gasparoto, Carlos Henrique Gasparoto cujo título é PROVAS DIGITAIS E DEEPFAKES NO PROCESSO PENAL: DESAFIOS

CONSTITUCIONAIS E GARANTIAS FUNDAMENTAIS. O trabalho enfrenta os desafios que as provas digitais, em especial as deepfakes, trazem ao processo penal brasileiro. O estudo aponta que, embora o uso de arquivos digitais seja crescente, sua vulnerabilidade à manipulação exige critérios rigorosos de autenticidade. As deepfakes representam uma ameaça inédita, pois podem fabricar falsas incriminações ou desacreditar provas legítimas (liar's dividend), comprometendo princípios constitucionais como a presunção de inocência e o devido processo legal. A resposta a essa crise de autenticidade deve ser basear em três eixos essenciais: (i) preservação da cadeia de custódia (para garantir a integridade do vestígio); (ii) metodologias periciais auditáveis; e (iii) gatekeeping judicial (verificação prévia de confiabilidade). Conclui-se que protocolos técnicos padronizados e certificação digital robusta são indispensáveis para equilibrar inovação e garantias fundamentais.

Ainda, Maria Fernanda Lima Oka e Rosberg de Souza Crozara apresentaram a pesquisa AÇÃO DE ANTECIPAÇÃO DE PROVAS PARA TESTEMUNHAS EM CRIMES SEXUAIS CONTRA CRIANÇAS E ADOLESCENTES: AS CONTRIBUIÇÕES PARA O BEM-ESTAR DA VÍTIMA E PARA O CONJUNTO PROBATÓRIO e analisaram a necessidade de estender a prerrogativa da antecipação de provas (Lei nº 13.431/2017, depoimento especial), também às testemunhas adultas em crimes sexuais contra crianças e adolescentes. O estudo argumenta que a demora na coleta desses depoimentos compromete a prova oral, que é perecível e falível, e impõe à família o encargo de reter na memória práticas delitivas, o que configura sofrimento partilhado e revitimização. Defende-se que a antecipação de provas não é apenas uma questão de celeridade processual, mas de dignidade humana, sendo fundamental para proteger a integridade física e psíquica dessas testemunhas adultas. Conclui-se que a extensão desse benefício contribui para a integridade da prova e para que as testemunhas iniciem seu processo de cura, garantindo a eficácia integral do Sistema de Garantia de Direitos (SGD).

Na sequencia, o artigo elaborado por Mayara de Carvalho Siqueira, Mariana Esteves Masagué e Vitor Bross cujo título é DA SOCIEDADE QUE CUIDA À SOCIEDADE QUE FERE: UMA ANÁLISE DA VIOLÊNCIA ESTRUTURAL CONTRA JOVENS AUTORES DE ATOS INFRACIONAIS. O trabalho propõe uma reflexão crítica sobre a responsabilização de adolescentes autores de atos infracionais no Brasil, confrontando o punitivismo à Doutrina da Proteção Integral (CF/88). O estudo aponta a persistência da visão do jovem como desviante, notadamente entre jovens negros e de classes baixas, que são alvos da violência estrutural. Critica-se que instituições como a Fundação Casa simbolizam uma abordagem punitiva que, na prática, reduz o conceito de socioeducação — um direito inerente — a meras medidas infracionais, ignorando falhas estatais. Essa lógica confunde o tratamento do jovem com o de adultos. O artigo busca caminhos para consolidar um sistema

que promova a proteção integral e o reconheça como sujeito de direitos, superando a lógica que transforma a sociedade que cuida na sociedade que fere.

Também nesse GT, o artigo A BUSCA POLICIAL EM LIXO EXTERNO E OS STANDARDS DE VALIDADE DA PROVA OBTIDA realiza uma análise crítica da busca policial em lixo externo, tendo como eixo a decisão paradigma do STJ (Informativo 821). A autora contrapõe o entendimento de que o lixo descartado carece de expectativa de privacidade, argumentando que essa interpretação literal ignora direitos de personalidade e garantias fundamentais. A pesquisa destaca um caso da CIDH (Corte Interamericana de Direitos Humanos) em que a busca em lixo gerou responsabilidade Estatal, reforçando a cautela necessária. Demonstra-se que a apreensão de lixo, especialmente de dados pessoais, exige justificativa clara, pois a ausência de rigor pode violar princípios constitucionais e configurar pesca probatória. O estudo conclui que os critérios atuais dos tribunais superiores brasileiros são insuficientes para garantir a licitude da prova e o respeito às garantias da pessoa acusada, contrastando com os preceitos de Direito Internacional.

O artigo elaborado por Sidney Soares Filho e Amanda Magalhães Xavier de Lima, com o título "DA PUNIÇÃO AO DIÁLOGO: A EXPERIÊNCIA RESTAURATIVA NO JUIZADO ESPECIAL CRIMINAL", teve como objetivo central analisar a estrutura do Juizado Especial Criminal (JECrim), instituído pela Lei nº 9.099/95, e sua vocação para a aplicação de práticas de Justiça Restaurativa (JR). O artigo fundamenta a grande convergência entre os modelos, destacando que a natureza consensual, célere e informal do JECrim se alinha aos princípios restaurativos, que priorizam o diálogo, a reparação do dano e a reintegração social. O estudo demonstra como os institutos despenalizadores (composição civil, transação penal e suspensão condicional do processo) podem ser articulados com a JR. A pesquisa analisa experiências nacionais que comprovam a eficácia, como a satisfação das vítimas e a redução da reincidência. Apesar disso, são apontados desafios estruturais e a resistência cultural de operadores do direito. Conclui-se que a inserção da Justiça Restaurativa no âmbito do JECrim é um caminho promissor para construir um sistema de justiça mais humanizado, participativo e eficiente.

De autoria de Viviane Freitas Perdigão Lima e Willian Freire da Silva Ramos, o artigo ENTRE A NORMA E A PRÁTICA: DESAFIOS DO JUIZ DAS GARANTIAS NO MARANHÃO analisa os desafios estruturais, logísticos e institucionais da implementação do Juiz das Garantias no Tribunal de Justiça do Maranhão (TJMA). A pesquisa adota uma abordagem normativa, empírica e propositiva para identificar os entraves à plena adoção do modelo, especialmente nas comarcas de entrância inicial, visando garantir a imparcialidade judicial no processo penal. O referencial teórico contextualiza o instituto como um fenômeno

político e institucional, além de jurídico. Os autores propõem um modelo híbrido, escalonado e regionalizado para o TJMA, que combina especialização e rodízio funcional. A proposta busca assegurar a racionalidade administrativa e a efetividade da tutela penal, concluindo que a implementação representa uma oportunidade de modernização institucional e de fortalecimento do processo penal democrático no Maranhão.

Vanessa Alves Gera Cintra, Manoel Ilson Cordeiro Rocha e Luiz Fernando Peres Curia foram os autores de POLÍTICA PÚBLICA: ADMISSÃO DO CONTRADITÓRIO E AMPLA DEFESA NO INQUÉRITO POLICIAL e discutiram a aplicabilidade dos princípios do contraditório e da ampla defesa no inquérito policial, um procedimento marcado pelo caráter inquisitivo defendido pela maioria da doutrina brasileira. O artigo argumenta que, embora o Inquérito não seja um processo judicial com acusação formal, ele configura um procedimento administrativo sui generis onde já existe controvérsia (autoria e materialidade delitiva) e no qual o Estado adota medidas restritivas contra o suspeito. Desse modo, a não observância das garantias fundamentais nessa fase preliminar (onde muitos confessam crimes sob pressão) gera uma abordagem incompleta da persecução criminal e frustra os valores incorporados pela Constituição de 1988. Conclui-se que o respeito a esses princípios na fase policial é a única solução para resguardar os direitos dos cidadãos e a higidez do processo judicial subsequente.

Daniela Carvalho Almeida da Costa e Caio Poderoso Bispo da Mota apresentaram o artigo INTELIGÊNCIA ARTIFICIAL NO JUDICIÁRIO PODE AMEAÇAR O PRINCÍPIO DA PRESUNÇÃO DE INOCÊNCIA? que analisa os riscos da aplicação da inteligência artificial (IA) no âmbito do Judiciário criminal, questionando se essa tecnologia pode ameaçar a efetivação do princípio da presunção de inocência. O estudo discute o conceito do princípio dentro do modelo retributivo e, em seguida, aborda como as IAs, baseadas em algoritmos de aprendizado de máquina, podem tomar decisões enviesadas. A pesquisa analisa o sistema COMPAS, aplicado no Judiciário estadunidense para formular sentenças, e seus reflexos para o sistema brasileiro. O artigo conclui que a aplicação da IA, ao utilizar bancos de dados históricos dos tribunais, tem o potencial de perpetuar comportamentos discriminatórios no sistema retributivo e, consequentemente, comprometer as garantias fundamentais.

Na sequencia, foram apresentados os textos A BIOÉTICA E O INFANTICÍDIO NO ORDENAMENTO JURÍDICO GUINEENSE: ENTRE A NORMA PENAL E A REALIDADE SOCIOCULTURAL, de Zito Djata e Tagore Trajano De Almeida Silva, demarcando discussões e marcos teóricos-metodológicos específicos para a reconstrução da dogmática jurídico penal; e o texto ESTELIONATO VIRTUAL E O GOLPE DO FALSO ADVOGADO: DESAFIOS JURÍDICOS NA ERA DIGITAL, de Alberto Castelo Branco

Filho e Lidia Regina Rodrigues, trazendo novos entraves e desafios para a preservação de direitos em um contexto de sociedade da informação.

Ainda, o trabalho ACORDOS SEM CULPA? O DILEMA DA RESPONSABILIZAÇÃO PENAL EM DESASTRES DE MASSA, de Ana Clara Almeida De Abreu coloca na pauta a construção de acordos, o Direito Penal contemporâneo e as discussões em matéria ambiental; a obra A BANALIZAÇÃO DO INQUÉRITO POLICIAL MILITAR DIANTE DA AUDIÊNCIA DE CUSTÓDIA, de João Pedro Prestes Mietz, demarcando os fundamentos e a aplicabilidade da persecução criminal; e a A NATUREZA JURÍDICA DAS MEDIDAS PROTETIVAS DE URGÊNCIA PREVISTAS NA LEI MARIA DA PENHA: UMA REVISÃO SISTEMÁTICA DE LITERATURA, de Giovanna Aguiar Silva, Lívia Mattar Silva Oliveira e Fernando Laércio Alves da Silva, sistematizando uma base teórica conceitual interessante e necessária.

Por fim, a pesquisa intitulada O ENQUADRAMENTO DA HOMOFOBIA E DA TRANSFOBIA COMO CRIMES DE RACISMO E A TENSÃO ENTRE A LEGALIDADE PENAL E O ATIVISMO JUDICIAL, de Lilian Benchimol Ferreira , Maria Cristina Almeida Pinheiro de Lemos e Narliane Alves De Souza E Sousa, trazendo à pauta as discussões e os limites do ativismo judicial; e A APLICAÇÃO DO JUIZ DE GARANTIAS NO TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ: A RESOLUÇÃO Nº 9, DE 13 DE AGOSTO DE 2025, de Verena Holanda de Mendonça Alves, retratando uma pesquisa sobre a operabilidade e efetividade do sistema de justiça criminal no norte do país.

Após as apresentações, notou-se a riqueza da produção acadêmica acima nominada e a grande relevância de mais esse CONPEDI, a atrair pesquisadores/as de todos o país – e do exterior –, em conformidade com o tema central do encontro: “Os caminhos da internacionalização e o futuro do Direito”.

Uma boa leitura desses trabalhos e dessa grande coletânea que reúne a propriedade intelectual de tantos e tantas que fazem pesquisa nesse país. Parabéns à pesquisadores/as e debatedores/as do GT DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO IV.

São Paulo, dezembro de 2025.

Prof. Dr. Caleb Salomão Pereira, da Universidade Presbiteriana Mackenzie.

Prof. Dr. Thiago Allisson Cardoso de Jesus, das Universidades CEUMA, UEMA e UFMA.

Prof. Dr. Mateus Eduardo Siqueira Nunes Bertoncini, do Centro Universitário Curitiba.

PROVAS DIGITAIS E DEEPFAKES NO PROCESSO PENAL: DESAFIOS CONSTITUCIONAIS E GARANTIAS FUNDAMENTAIS

DIGITAL EVIDENCE AND DEEPFAKES IN CRIMINAL PROCEEDINGS: CONSTITUTIONAL CHALLENGES AND FUNDAMENTAL GUARANTEES

Felipe dos Santos Gasparoto
Carlos Henrique Gasparoto

Resumo

O artigo examina os desafios que as provas digitais, especialmente as deepfakes, trazem ao processo penal brasileiro. A transformação digital ampliou o uso de mensagens, áudios, vídeos e metadados como elementos probatórios, mas a vulnerabilidade desses arquivos a manipulações exige critérios técnicos rigorosos para garantir autenticidade e integridade. As deepfakes, por sua vez, representam uma ameaça inédita, pois podem gerar falsas incriminações, desacreditar provas legítimas (liar's dividend) e comprometer princípios constitucionais como a presunção de inocência, a ampla defesa e o devido processo legal. O estudo defende três eixos essenciais: (I) preservação da cadeia de custódia, conforme os arts. 158-A a 158-F do CPP; (II) metodologias periciais auditáveis, baseadas em hash codes, metadados e análise forense; e (III) gatekeeping judicial, com verificação prévia da confiabilidade da prova. A análise jurisprudencial brasileira e comparada revela convergência internacional em torno da licitude, integridade e contraditório. O texto conclui que a adoção de protocolos técnicos padronizados, certificação digital robusta e cooperação internacional são medidas indispensáveis para equilibrar inovação tecnológica e garantias fundamentais, evitando nulidades e injustiças no processo penal

Palavras-chave: Provas digitais, Deepfake, Processo penal, Cadeia de custódia, Direitos fundamentais

Abstract/Resumen/Résumé

The article examines the challenges that digital evidence, especially deepfakes, pose to the Brazilian criminal process. Digital transformation has expanded the use of messages, audios, videos, and metadata as evidentiary elements, but the vulnerability of these files to manipulation requires strict technical criteria to ensure authenticity and integrity. Deepfakes, in turn, represent an unprecedented threat, as they can generate false incriminations, discredit legitimate evidence (liar's dividend), and undermine constitutional principles such as the presumption of innocence, the right to a full defense, and due process of law. The study advocates three essential pillars: (I) preservation of the chain of custody, in accordance with Articles 158-A to 158-F of the Code of Criminal Procedure; (II) auditable forensic methodologies, based on hash codes, metadata, and forensic analysis; and (III) judicial gatekeeping, with prior verification of the reliability of the evidence. The Brazilian and

comparative jurisprudential analysis reveals international convergence around legality, integrity, and adversarial proceedings. The text concludes that the adoption of standardized technical protocols, robust digital certification, and international cooperation are indispensable measures to balance technological innovation with fundamental guarantees, thus avoiding nullities and injustices in the criminal process

Keywords/Palabras-claves/Mots-clés: Digital evidence, Deepfake, Criminal procedure, Chain of custody, Fundamental rights

1.Introdução

A transformação digital intensificada nas últimas décadas consolidou a internet e as tecnologias da informação como elementos centrais da vida social e econômica. Essa evolução trouxe benefícios inegáveis, mas também fomentou o crescimento exponencial dos crimes digitais, como fraudes eletrônicas, invasões de sistemas, estelionatos cibernéticos e a manipulação avançada de conteúdos multimídia. No Brasil, o legislador reagiu com alterações relevantes, a exemplo da Lei n.º 14.155/2021, que agravou as penas para crimes cometidos por meios digitais, e da introdução dos arts. 158-A a 158-F no Código de Processo Penal (CPP) pela Lei n.º 13.964/2019, que estabeleceu regras para a cadeia de custódia das provas digitais.

No entanto, a ascensão da inteligência artificial generativa potencializou um novo desafio: as deepfakes. Trata-se de conteúdos sintéticos hiper-realistas, produzidos por redes neurais avançadas, capazes de criar vídeos, áudios e imagens praticamente indistinguíveis da realidade. No contexto do processo penal, esses elementos inauguram uma crise paradigmática sobre a autenticidade, integridade e confiabilidade das provas, pois podem tanto fabricar falsas incriminações quanto desacreditar provas lícitas por mera alegação de manipulação — fenômeno conhecido como liar's dividend.

Os impactos sobre os direitos fundamentais são igualmente significativos. A manipulação de conteúdos digitais e a coleta de dados pessoais para instrução processual envolvem direitos à intimidade, à vida privada e à proteção de dados (art. 5º, X e XII, da Constituição Federal), disciplinados por normas como a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet. Nesse cenário, o processo penal precisa se equilibrar entre a eficiência da persecução penal e a tutela das garantias constitucionais do contraditório, da ampla defesa e da vedação de provas ilícitas (art. 5º, LVI, CF/88).

Mesmo em outros ramos do Direito, como o eleitoral, já se observa a preocupação normativa com os efeitos das deepfakes. O Tribunal Superior Eleitoral (TSE), por exemplo, proibiu expressamente o uso dessas tecnologias em propagandas e determinou alertas obrigatórios quando houver manipulação digital. Essa tendência regulatória reforça a necessidade de padrões claros também para o processo penal.

Diante da possibilidade de que áudios, vídeos e imagens apresentados no processo penal sejam potencialmente sintetizados por inteligência artificial, quais padrões técnico-jurídicos devem orientar a admissibilidade, a produção e a valoração da prova digital para compatibilizar a busca pela verdade real com a proteção das garantias constitucionais, evitando, de um lado, condenações injustas baseadas em conteúdos falsificados e, de outro, a nulidade de processos por ausência de autenticidade ou quebra de cadeia de custódia?

Parte-se da hipótese de que é possível compatibilizar o uso responsável de provas digitais potencialmente manipuláveis com a preservação dos direitos e garantias fundamentais, desde que sejam observados três eixos principais:

Reforço da cadeia de custódia — aplicação rigorosa dos arts. 158-A a 158-F do CPP, com registro detalhado de integridade, armazenamento, logs de acesso e hash codes;

Metodologias periciais auditáveis — adoção de protocolos científicos replicáveis e validação cruzada de resultados;

Gatekeeping judicial — análise prévia da confiabilidade do material digital antes de sua exposição em juízo, com verificação técnica de autenticidade, preservando o contraditório substancial e evitando prejuízo à defesa.

A discussão possui relevância científica e prática. Sob o aspecto científico, o estudo atualiza categorias dogmáticas da teoria da prova, confrontando conceitos clássicos de autenticidade e integridade com o cenário de conteúdos sintéticos de alta complexidade técnica. Sob o aspecto prático, a consolidação de parâmetros objetivos para provas digitais fortalece a segurança jurídica, evita nulidades processuais e garante a efetividade dos direitos fundamentais. Além disso, contribui para orientar a atuação de autoridades policiais, Ministério Público, advocacia e magistratura diante de um cenário tecnológico em constante evolução.

A pesquisa se delimita ao estudo do processo penal brasileiro, examinando os impactos das deepfakes e de outras provas digitais sobre a admissibilidade, produção e valoração da prova. São objetivos específicos:

Analisar o marco normativo vigente (CPP, CF/88, LGPD e Marco Civil da Internet);

Avaliar a jurisprudência recente sobre provas digitais e cadeia de custódia;

Propor diretrizes técnico-jurídicas para mitigação dos riscos de condenações indevidas e nulidades processuais;

Sugerir um modelo de governança probatória adequado à era das deepfakes.

2.Provas Digitais no Processo Penal

A vida em sociedade migrou de forma intensa para o ambiente digital, o que transformou também a forma de investigar e julgar crimes. Hoje, provas como mensagens em aplicativos, registros de geolocalização, vídeos e metadados são cada vez mais comuns e relevantes no processo penal. O grande desafio é assegurar que esse tipo de elemento seja utilizado sem comprometer direitos fundamentais, como a privacidade, a ampla defesa e a presunção de inocência.

A doutrina entende que prova digital não é apenas o dado em si, mas todo o processo que envolve sua coleta, preservação e apresentação. Nesse ponto, Bittar (2023) destaca que a confiabilidade depende da forma como o vestígio é manipulado desde a origem até o momento em que chega ao juiz. Assim, não se trata de aceitar ou rejeitar tecnologias, mas de estabelecer critérios claros que deem segurança ao processo.

O primeiro requisito é a licitude da obtenção. Dados privados, como mensagens e registros de navegação, só podem ser acessados com autorização judicial. Do contrário, o material deve ser considerado nulo. O Supremo Tribunal Federal já consolidou esse entendimento: no HC 91.867/PA, a Corte declarou ilícita a interceptação de e-mails sem ordem judicial, reforçando que a intimidade digital está protegida pelos mesmos princípios que resguardam a comunicação telefônica.

Outro ponto central é a integridade da prova, garantida pela chamada cadeia de custódia. Esse procedimento documenta cada passo do caminho percorrido pelo vestígio digital: quem coletou, onde foi armazenado, como foi transportado e quais análises foram feitas. A Lei nº 13.964/2019 trouxe regras claras nesse sentido, tornando o controle obrigatório. Sem esse registro, a prova perde valor. O Superior Tribunal de Justiça confirmou essa exigência no RHC 77.836/SP, em que considerou inadmissíveis prints de conversas sem documentação metodológica adequada, justamente porque não havia garantia de que o conteúdo não fora manipulado.

Por fim, a validade das provas digitais depende de sua auditabilidade. É preciso que a defesa tenha acesso aos mesmos elementos técnicos que sustentam a acusação, como metadados, hash codes e relatórios periciais. Só assim é possível exercer o contraditório de forma efetiva, com a possibilidade de realizar perícias independentes. Um caso que ilustra essa preocupação é o AgRg no REsp 1.889.579/SP, em que o STJ reconheceu o direito da defesa de contestar a integridade do material e exigir verificação técnica, mesmo diante de falhas não consideradas suficientes para nulidade automática.

Em resumo, as provas digitais só podem ser admitidas quando atendem a três eixos básicos: (I) obtenção lícita, respeitando a privacidade e os limites constitucionais; (II) preservação íntegra, assegurada por uma cadeia de custódia bem documentada; e (III) auditabilidade plena, para garantir contraditório e ampla defesa. A doutrina e a jurisprudência convergem no sentido de que não basta a existência de dados digitais — é preciso que sejam confiáveis, autênticos e passíveis de debate técnico em juízo.

Esse rigor tende a crescer com a sofisticação das manipulações, como as deepfakes. Assim, o processo penal brasileiro caminha para um modelo em que a tecnologia e os direitos fundamentais precisam coexistir: de um lado, permitindo a eficiência da investigação; de outro, impedindo condenações baseadas em provas frágeis ou adulteradas.

3. Deepfakes e Manipulação Digital no Processo Penal

A evolução da inteligência artificial generativa permitiu o desenvolvimento de tecnologias capazes de criar conteúdos sintéticos extremamente realistas, conhecidos como deepfakes. Essas técnicas utilizam redes neurais de aprendizado profundo para gerar imagens, áudios e vídeos que simulam falas, comportamentos e aparências de pessoas com altíssimo grau de verossimilhança.

No contexto do processo penal, as deepfakes inauguram um novo paradigma probatório, pois desafiam diretamente a autenticidade, a integridade e a confiabilidade das provas digitais. A possibilidade de manipulação praticamente imperceptível de conteúdos multimídia impõe riscos significativos à formação da convicção judicial, podendo comprometer o devido processo legal e a presunção de inocência.

O uso de provas digitais no processo penal já exige cuidados especiais, dada a vulnerabilidade dos arquivos eletrônicos a alterações. Com a introdução das deepfakes, porém, o problema assume proporções inéditas, pois se torna cada vez mais difícil distinguir conteúdos genuínos de manipulações sofisticadas.

Dentre os principais impactos na produção probatória, destacam-se:

Dificuldade de verificação da autenticidade – Áudios e vídeos podem ser adulterados com tamanha precisão que mesmo perícias tradicionais falham na detecção de manipulações;

Risco de falsas incriminações – Um acusado pode ser colocado digitalmente em uma cena de crime, "dizendo" ou "fazendo" algo que jamais ocorreu;

Contaminação da prova legítima – O simples argumento de que determinada gravação pode ter sido manipulada pode gerar dúvida sobre conteúdos autênticos, fenômeno conhecido como liar's dividend;

Sobrecarga da perícia forense – A análise técnica para identificação de deepfakes exige softwares e conhecimentos altamente especializados, o que aumenta custos, prazos e riscos de erros.

Com isso, a cadeia de custódia e a metodologia pericial assumem papel central para garantir a integridade dos elementos de prova. A ausência de hash codes, metadados e relatórios técnicos completos tende a inviabilizar a aceitação de mídias digitais como evidências válidas.

Os impactos das deepfakes não se restringem à esfera técnica: há profundas implicações para os direitos fundamentais assegurados pela Constituição Federal e pela Convenção Americana de Direitos Humanos. Destacam-se quatro riscos principais:

a) Violação da presunção de inocência

A criação e circulação de conteúdos digitais falsos podem induzir o julgador a erro, invertendo o ônus probatório e fragilizando o princípio da presunção de inocência (art. 5º, LVII, CF/88). O risco se intensifica diante da pressão social e midiática, na qual conteúdos manipulados podem se espalhar rapidamente, afetando a imparcialidade do juízo.

b) Comprometimento do devido processo legal

O devido processo legal (art. 5º, LIV, CF/88) exige que as provas sejam obtidas, preservadas e analisadas segundo procedimentos previamente estabelecidos. A manipulação digital não detectada compromete não apenas a validade da prova, mas também a própria legitimidade do processo penal.

c) Risco à ampla defesa e ao contraditório

O contraditório substancial, previsto no art. 5º, LV, CF/88, pressupõe que a defesa tenha acesso pleno aos elementos probatórios e possa questionar sua autenticidade por meio de perícias independentes. No entanto, quando a tecnologia empregada na manipulação é mais sofisticada do que a disponível nos órgãos periciais oficiais, a defesa pode se ver impossibilitada de contestar adequadamente o conteúdo apresentado.

d) Proteção da intimidade e dos dados pessoais

As deepfakes podem violar o direito à intimidade e à vida privada (art. 5º, X, CF/88), além de conflitar com os princípios da Lei Geral de Proteção de Dados (LGPD), que impõe requisitos para coleta, tratamento e uso de dados pessoais. O risco aumenta quando conteúdos íntimos são criados ou expostos de forma ilícita para constranger ou manipular o acusado.

O cenário de proliferação das deepfakes impõe desafios urgentes ao sistema de justiça criminal:

Atualização de protocolos periciais – É necessário criar normas técnicas padronizadas para detecção de manipulações digitais, com utilização de algoritmos de verificação, análise de metadados e certificação por hash codes;

Capacitação institucional – Juízes, promotores, defensores e peritos precisam de formação continuada para compreender a dinâmica das deepfakes e seus impactos jurídicos;

Criação de parâmetros normativos específicos – Atualmente, o ordenamento brasileiro não dispõe de legislação própria para regular deepfakes, o que demanda projetos de lei voltados à responsabilização de criadores e plataformas;

Cooperação internacional – Dada a natureza transnacional da tecnologia, é necessário fomentar acordos multilaterais para rastrear origens, responsabilizar agentes e compartilhar técnicas de detecção.

As deepfakes representam um dos maiores desafios contemporâneos para a produção de provas digitais e para a efetividade das garantias constitucionais no processo penal. A dificuldade de verificar a autenticidade de conteúdos manipulados coloca em risco a confiabilidade do sistema probatório, a imparcialidade judicial e os direitos fundamentais do acusado.

Diante desse cenário, torna-se imperativo investir na criação de protocolos periciais robustos, na atualização legislativa e na capacitação dos operadores do direito, para que a evolução tecnológica não se converta em instrumento de injustiças processuais.

A crescente utilização de provas digitais no processo penal — como vídeos, áudios, mensagens, metadados e documentos eletrônicos — ampliou a necessidade de procedimentos técnicos robustos para verificar sua autenticidade e integridade. Esse cenário tornou-se ainda mais complexo com o surgimento das deepfakes, que utilizam inteligência artificial generativa para criar conteúdos sintéticos altamente realistas, desafiando as metodologias tradicionais de perícia forense.

No contexto do processo penal brasileiro, a perícia digital assume papel fundamental para atestar a validade da prova, evitando condenações baseadas em conteúdos falsificados e preservando direitos fundamentais, como o devido processo legal, o contraditório e a ampla defesa (art. 5º, LIV e LV, CF/88). Para que um vestígio digital seja considerado confiável, é necessário comprovar sua origem, integridade e autenticidade, por meio de técnicas científicas auditáveis e transparentes.

A perícia digital é o conjunto de procedimentos técnicos voltados à coleta, preservação, análise e validação de vestígios eletrônicos, assegurando que o material apresentado ao juízo corresponda fielmente ao arquivo original.

No Brasil, a Lei nº 13.964/2019 inseriu os arts. 158-A a 158-F no Código de Processo Penal (CPP), disciplinando a cadeia de custódia e estabelecendo a obrigatoriedade da

documentação minuciosa de todas as etapas relacionadas à prova digital. Isso inclui a identificação de quem acessou, manipulou e analisou o arquivo, garantindo a rastreabilidade dos procedimentos.

Segundo Badaró (2022), “não basta que a prova digital seja apresentada: é necessário demonstrar que foi coletada e preservada de forma íntegra, mediante procedimentos científicos verificáveis”. Assim, a perícia digital atua como garantia processual e elemento de proteção da confiabilidade do sistema probatório.

Para atestar a autenticidade e a integridade das provas digitais, a ciência forense desenvolveu um conjunto de técnicas avançadas, combinando análise de metadados, algoritmos de hash e metodologias de detecção de manipulações. Entre as principais técnicas, destacam-se:

a) Códigos hash e assinatura digital

O uso de hash codes — funções criptográficas que geram um identificador único para cada arquivo — permite verificar se um documento, vídeo, áudio ou imagem foi alterado. Caso o hash gerado no momento da coleta seja diferente do apresentado em juízo, presume-se que houve adulteração.

Além disso, a assinatura digital baseada em criptografia assimétrica possibilita confirmar a autoria e a integridade do conteúdo, sendo especialmente útil para documentos processuais e registros oficiais.

b) Análise de metadados e logs

Os metadados contêm informações técnicas sobre arquivos digitais, como data de criação, local de captura, dispositivo utilizado e histórico de alterações. Sua análise permite detectar incongruências e manipulações, auxiliando na validação de vídeos, áudios e imagens apresentados como prova.

Além dos metadados, o rastreamento de logs de acesso em servidores, aplicativos de mensagens e plataformas de armazenamento é essencial para identificar tentativas de alteração ou exclusão de dados.

c) Perícia em imagens, áudios e vídeos

A análise forense de conteúdos multimídia utiliza algoritmos capazes de identificar manipulações sutis. Entre os principais métodos, destacam-se:

Detecção de inconsistências visuais: análise de sombras, iluminação, reflexos e bordas para identificar adulterações;

Perícia de áudio: avaliação espectral para detectar cortes, sobreposições e edição de voz;

Análise frame a frame: verificação detalhada da sequência de imagens para identificar sobreposições artificiais;

Detecção de artefatos digitais: uso de inteligência artificial para encontrar padrões anômalos em vídeos potencialmente manipulados.

d) Ferramentas de detecção de deepfakes

Com o avanço das deepfakes, surgiram ferramentas baseadas em aprendizado de máquina capazes de analisar microexpressões faciais, padrões de piscamento e inconsistências na sincronização de áudio e vídeo. Plataformas como Microsoft Video Authenticator e Deepware Scanner exemplificam os esforços para acompanhar a evolução das técnicas de falsificação.

Apesar dos avanços, a perícia digital enfrenta diversos desafios para lidar com conteúdos sintéticos sofisticados:

Corrida tecnológica – As técnicas de criação de deepfakes evoluem mais rapidamente do que os métodos de detecção, tornando a validação probatória cada vez mais complexa;

Falta de padronização – Não há, no Brasil, protocolos técnicos unificados para análise e autenticação de provas digitais, o que gera insegurança jurídica;

Limitações estruturais – Muitos órgãos periciais não dispõem de softwares atualizados e de pessoal qualificado para enfrentar manipulações avançadas;

Dificuldade de auditoria independente – A defesa nem sempre tem acesso a todos os dados técnicos necessários para replicar perícias, o que fragiliza o contraditório e a ampla defesa;

Risco de falsos positivos e negativos – Tanto a aceitação de provas manipuladas quanto o descarte indevido de provas legítimas podem comprometer a busca da verdade real e a efetividade do processo penal.

A perícia digital é elemento indispensável para a autenticação das evidências eletrônicas e a proteção dos direitos fundamentais no processo penal. As técnicas de verificação, como hash codes, assinatura digital, análise de metadados e algoritmos de detecção de deepfakes, oferecem um caminho sólido para preservar a confiabilidade das provas.

Entretanto, o avanço acelerado das tecnologias de manipulação digital impõe ao sistema de justiça brasileiro o desafio de criar protocolos periciais padronizados, investir na capacitação institucional e promover a cooperação internacional para enfrentar ameaças à autenticidade probatória.

Sem essas medidas, o processo penal corre o risco de se tornar vulnerável a condenações injustas e nulidades processuais diante de conteúdos digitais potencialmente adulterados.

4. Análise Jurisprudencial

A crescente presença de provas digitais nos processos criminais impôs ao Judiciário brasileiro e internacional a tarefa de definir parâmetros claros para sua admissibilidade. A vulnerabilidade desses elementos — ainda mais intensa com o avanço das deepfakes — exige uma postura de maior rigor técnico, sem perder de vista a proteção de direitos fundamentais como privacidade, ampla defesa e contraditório.

O STF vem sendo decisivo na construção das bases constitucionais que cercam a coleta e utilização de dados digitais. Dois julgados se destacam:

HC 91.867/PA (2010) – A Primeira Turma declarou ilícita a obtenção de mensagens eletrônicas sem ordem judicial, equiparando a proteção da privacidade digital à das comunicações telefônicas. Esse precedente foi um marco no reconhecimento da inviolabilidade das comunicações eletrônicas.

RE 1.155.361/SP (2021, Tema 977 da Repercussão Geral) – O Plenário fixou a tese de que a apreensão de dispositivos eletrônicos não autoriza, por si só, o acesso ao conteúdo neles

armazenado. Somente decisão judicial fundamentada pode permitir a quebra de sigilo, reforçando a centralidade da intimidade digital como direito fundamental.

Essas decisões consolidaram um entendimento: a prova digital, para ser válida, precisa respeitar o mesmo regime constitucional que protege dados pessoais e comunicações privadas.

O STJ assumiu protagonismo na definição de requisitos técnicos, com ênfase na cadeia de custódia e autenticidade. Dois casos são paradigmáticos:

RHC 77.836/SP (2023) – A Quinta Turma considerou inválidos prints de conversas obtidos em aplicativos sem acompanhamento técnico. A Corte destacou que, pela alta vulnerabilidade a manipulações, a prova digital deve vir acompanhada de relatório pericial que assegure sua integridade.

HC 598.051/SP (2021) – A mesma Turma declarou nulas provas extraídas de um celular sem observância da cadeia de custódia. O acórdão reforçou que a falta de documentação de metadados e hash codes compromete a confiabilidade do material.

Esses precedentes evidenciam o papel do STJ em estabelecer um padrão técnico mínimo para a aceitação das provas digitais, afastando conteúdos apresentados de forma desprovida de controle.

Entre os TRFs, destaca-se decisão do TRF-4 (Apelação Criminal 5002732-21.2021.4.04.7200), em que houve a anulação parcial de processo envolvendo fraudes eletrônicas por quebra da cadeia de custódia. O Tribunal concluiu que a ausência de registro cronológico das etapas de coleta e análise inviabilizou a comprovação da autenticidade do material, reforçando a exigência de documentação precisa mesmo fora dos tribunais superiores.

Nos EUA, a admissibilidade de provas digitais está diretamente ligada às Federal Rules of Evidence, especialmente à Rule 901, que exige demonstração da autenticidade. O caso mais ilustrativo é o United States v. Vayner (2014), no qual o Tribunal de Apelações do Segundo Circuito rejeitou uma captura de tela de rede social por falta de autenticação. O julgamento reforçou que não basta a apresentação do print: é necessário comprovar origem, autoria e integridade.

Na Europa, a abordagem é fortemente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR). O caso Digital Rights Ireland (TJUE, 2014) foi paradigmático ao declarar incompatível com o direito europeu a retenção indiscriminada de dados pessoais para fins de investigação penal. O Tribunal entendeu que a coleta de informações digitais deve respeitar a proporcionalidade e a necessidade, estabelecendo limites rígidos ao poder investigativo do Estado.

A análise comparada revela pontos de convergência entre Brasil, Estados Unidos e União Europeia:

Licitude – só são admitidas provas obtidas com respeito à legalidade e mediante ordem judicial quando houver restrição a direitos fundamentais.

Integridade – a cadeia de custódia e o uso de hash codes e metadados são indispensáveis para garantir a confiabilidade.

Contraditório – defesa e acusação devem ter igual acesso às informações técnicas que sustentam a prova.

Proteção de direitos fundamentais – privacidade e proporcionalidade orientam a atuação judicial, sob pena de nulidade.

A jurisprudência nacional e internacional converge no sentido de que a prova digital só pode ser aceita quando acompanhada de documentação rigorosa e metodologias auditáveis. O fenômeno das deepfakes agrava ainda mais a necessidade de parâmetros claros, pois ameaça não apenas a veracidade das provas, mas também a confiança no próprio processo penal.

O futuro aponta para a padronização de protocolos técnicos, investimento em perícia especializada e fortalecimento da cooperação internacional. Assim, será possível compatibilizar inovação tecnológica com preservação das garantias fundamentais, evitando tanto condenações injustas baseadas em manipulações digitais quanto nulidades processuais por ausência de confiabilidade probatória.

5. Diretrizes para Validação de Provas Digitais

O avanço das tecnologias digitais e o crescimento de manipulações sofisticadas — como as deepfakes — colocaram em xeque a forma como o processo penal lida com a produção e a

valoração das provas. Nesse cenário, tornou-se urgente a criação de diretrizes claras e unificadas que assegurem a confiabilidade das evidências eletrônicas sem abrir mão da proteção de direitos fundamentais.

Entre os critérios possíveis, três eixos se mostram indispensáveis: a preservação da cadeia de custódia, o uso de certificação digital e a adoção de padrões internacionais de perícia forense.

A prova digital é, por natureza, frágil. Arquivos podem ser copiados, manipulados ou adulterados de forma quase imperceptível. Por isso, a cadeia de custódia prevista nos arts. 158-A a 158-F do CPP tornou-se o alicerce da validade probatória.

Manter a rastreabilidade do vestígio significa registrar cada etapa: quem coletou, como armazenou, quando transportou e de que modo foi analisado. Boas práticas recomendam a geração de hash codes no momento da coleta, o isolamento da mídia original e a utilização de cópias forenses em análises posteriores.

Mais do que um procedimento técnico, a cadeia de custódia é uma garantia processual. Sem documentação clara, abre-se espaço para dúvidas, nulidades e injustiças. Em tempos de manipulações digitais quase indetectáveis, não há como prescindir de registros cronológicos detalhados que assegurem autenticidade e integridade.

Outro pilar essencial é a certificação digital, que fornece instrumentos técnicos para comprovar autoria, integridade e temporalidade de documentos eletrônicos.

No Brasil, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) dá respaldo jurídico às assinaturas digitais qualificadas, presumindo sua validade. Mas, diante da sofisticação das falsificações, recomenda-se ir além:

- utilização de assinaturas digitais com certificação cruzada;
- análise de metadados (data, local, dispositivo de origem);
- uso de carimbos do tempo (timestamping);
- incorporação de tecnologias como blockchain, que permitem registrar alterações de forma transparente e praticamente inviolável.

Esses mecanismos garantem que um documento, áudio ou vídeo apresentado em juízo corresponda exatamente ao original, fortalecendo o contraditório e evitando que a defesa se veja diante de provas insuscetíveis de contestação.

Por fim, a experiência internacional demonstra a necessidade de alinhar práticas nacionais a protocolos técnicos já consolidados. Entre os mais relevantes estão os padrões ISO/IEC voltados à perícia digital:

ISO/IEC 27037 – diretrizes para identificação, coleta e preservação de evidências digitais;

ISO/IEC 27041 – requisitos para validação e replicabilidade de perícias;

ISO/IEC 27042 – procedimentos de análise e interpretação de dados eletrônicos;

ISO/IEC 27043 – parâmetros para investigação de incidentes digitais.

Essas normas já são aplicadas em diversos países e asseguram que as perícias sejam replicáveis e auditáveis. Sua adoção no Brasil traria maior segurança jurídica e alinhamento às melhores práticas globais, sobretudo em casos em que deepfakes ou outras manipulações complexas colocam em dúvida a autenticidade das provas.

A confiabilidade das provas digitais depende de três pilares: cadeia de custódia rigorosa, certificação digital robusta e alinhamento a padrões internacionais ISO. Sem esses elementos, o processo penal corre o risco de se tornar refém da insegurança tecnológica e de condenações baseadas em material adulterado.

Por outro lado, a implementação de protocolos claros fortalece o devido processo legal, assegura o contraditório e preserva a confiança no sistema de justiça. A integração entre Direito, ciência forense e tecnologia é o caminho para equilibrar inovação e garantias constitucionais, evitando que as provas digitais — em vez de servir à verdade real — se convertam em instrumentos de incerteza e injustiça.

6. Propostas para futuras pesquisas

O avanço exponencial das tecnologias digitais exige pesquisas interdisciplinares que unam direito, ciência da computação, engenharia de dados e cibersegurança. Algumas direções relevantes para estudos futuros incluem:

Protocolos nacionais de certificação digital — Desenvolvimento de um padrão brasileiro unificado de auditoria e validação de provas digitais, integrando ICP-Brasil, hash codes, blockchain e normas ISO internacionais.

Detecção automatizada de deepfakes — Criação de ferramentas baseadas em inteligência artificial capazes de identificar manipulações sutis em imagens, áudios e vídeos, com aplicação direta no âmbito pericial.

Governança probatória internacional — Investigação de modelos de cooperação global para a padronização de critérios técnicos e metodologias de autenticação, especialmente diante de crimes digitais transnacionais.

Responsabilidade civil e penal por manipulação digital — Estudo dos efeitos jurídicos relacionados à criação e disseminação de deepfakes, propondo modelos de responsabilização de indivíduos e plataformas digitais.

Privacidade e proteção de dados na era da IA — Análise dos impactos da inteligência artificial generativa sobre direitos fundamentais, equilibrando segurança pública, liberdade individual e proteção de dados pessoais.

A transformação digital trouxe consigo novas oportunidades e novos riscos para o processo penal. A crescente relevância das provas digitais exige protocolos padronizados, investimento em perícia especializada e integração normativa com padrões internacionais.

As deepfakes representam um dos maiores desafios probatórios contemporâneos, exigindo que operadores do direito dominem não apenas os conceitos jurídicos tradicionais, mas também as tecnologias emergentes envolvidas na produção, manipulação e autenticação das evidências.

Por fim, conclui-se que o fortalecimento da segurança digital no processo penal depende da articulação entre direito, tecnologia e ciência forense, garantindo a proteção dos direitos fundamentais, a busca da verdade real e a credibilidade do sistema de justiça.

Referências

ALMEIDA, Cláudia. Perícia forense e detecção de manipulações digitais. Rio de Janeiro: Lumen Juris, 2023.

BADARÓ, Gustavo Henrique. Provas ilícitas e cadeia de custódia. São Paulo: Revista dos Tribunais, 2022.

BITTAR, Eduardo. Prova digital no processo penal. 2. ed. São Paulo: RT, 2023.

BRASIL. Código de Processo Civil. Lei nº 13.105, de 16 de março de 2015. Disponível em: http://www.planalto.gov.br. Acesso em: 15 ago. 2025.

BRASIL. Código de Processo Penal. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Alterado pela Lei nº 13.964, de 24 de dezembro de 2019. Disponível em: http://www.planalto.gov.br. Acesso em: 10 ago. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br. Acesso em: 09 ago. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br. Acesso em: 05 ago. 2025.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Disponível em: http://www.planalto.gov.br. Acesso em: 15 ago. 2025.

CAPEZ, Fernando. Crimes Digitais e Provas Eletrônicas. São Paulo: Saraiva, 2022.

CHESNEY, Robert; CITRON, Danielle. Deep Fakes and the Liar's Dividend. California Law Review, v. 107, n. 2, 2019. Disponível em: https://papers.ssrn.com. Acesso em: 18 ago. 2025.

FONSECA, Rodrigo. Perícia digital e autenticação de arquivos. Porto Alegre: Bookman, 2021.

GALDINO, Gustavo. Deepfakes e o desafio probatório no processo penal comparado. Coimbra: Almedina, 2023.

GOMES, Anderson. Blockchain, certificação digital e provas eletrônicas. São Paulo: Saraiva, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition, and preservation of digital evidence. Geneva: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27041-27043:2015 — Information security incident investigation standards. Geneva: ISO, 2015.

LOPES JR., Aury. Direito Processual Penal. 19. ed. São Paulo: Saraiva, 2023.

MICROSOFT. Video Authenticator. Disponível em: https://www.microsoft.com. Acesso em: 10 ago. 2025.

NUCCI, Guilherme de Souza. Código de Processo Penal Comentado. 19. ed. Rio de Janeiro: Forense, 2023.

PACELLI, Eugênio. Curso de Processo Penal. 27. ed. Rio de Janeiro: Atlas, 2023.

ROSA, Alexandre Morais da. Provas Digitais e Processo Penal. São Paulo: RT, 2022.

SOUZA, Marcos Vinícius. Provas digitais e processo penal: desafios contemporâneos. São Paulo: Thomson Reuters, 2022.

UNITED STATES. Federal Rules of Evidence. Rule 901. Disponível em: https://www.law.cornell.edu/rules/fre/rule_901. Acesso em: 11 ago. 2025.

UNITED STATES. United States v. Browne, 834 F.3d 403 (3d Cir. 2016). Disponível em: https://casetext.com/case/united-states-v-browne. Acesso em: 11 ago. 2025.

UNITED STATES. United States v. Thomas, 327 F. Supp. 3d 1161 (E.D. Va. 2019). Disponível em: https://casetext.com/case/united-states-v-thomas-135. Acesso em: 11 ago. 2025.

UNITED STATES. United States v. Vayner, 769 F.3d 125 (2d Cir. 2014). Disponível em: https://casetext.com/case/united-states-v-vayner. Acesso em: 11 ago. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679. Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: . Acesso em: 15 ago. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Digital Rights Ireland Ltd v. Minister for Communications, C-293/12 e C-594/12, 2014. Disponível em: . Acesso em: 15 ago. 2025.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Benedik v. Slovenia. Application no. 62357/14. Julgado em 24 abr. 2018. Disponível em: https://hudoc.echr.coe.int. Acesso em: 28 ago. 2025.