XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

GUSTAVO NORONHA DE AVILA

ROGERIO LUIZ NERY DA SILVA

D597

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

Coordenadores: Gustavo Noronha de Avila, Rogerio Luiz Nery Da Silva – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-319-0
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

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO I

Apresentação

Tivemos a oportunidade de coordenar a apresentação dos excelentes trabalhos do GT Direito Penal, Processo Penal e Constituição I. Novamente, foi possível identificar o estado da arte da dogmática penal sendo discutidos por pesquisadores de Norte a Sul do país.

Inicialmente, Beatriz Azevedo e Giovanna Souza apresentaram texto sobre crimes de resultado e imputação objetiva no caso do Boeing 737 Max. A partir da categoria dos riscos proibidos, presente na referida teoria, defendem a possibilidade da imputação objetiva ainda em que atividades remotas, especialmente em contextos corporativos.

Sebastian Mello e Beatriz Azevedo discutiram os relatórios de inteligência financeira do COAF (Conselho de Controle de Atividades Financeiras) e a (i)legalidade de sua utilização. São trabalhadas a jurisprudência dos Tribunais Superiores, bem como a constitucionalidade de relatórios obtidos na informalidade.

O persistente tema da corrupção é discutido por Camila Costa e Sebastian Mello. Os autores trazem diferenciação entre as corrupções cotidianas e os esquemas de corrupção que normalmente ganham as manchetes midiáticas. São trazidas as diferenciações legais, além da discussão de casos paradigmáticos julgados no âmbito do Supremo Tribunal Federal.

As práticas laborais abusivas e sua criminalização, no âmbito internacional, são discutidas por Alexander Rodrigues de Castro, Pedro Henrique Facco , João Marcos Mariani Junior. São tratados, além do tema da política criminal, os reflexos das práticas no tocante aos direitos da personalidade e dos direitos humanos das vítimas.

A seguir, os mesmos autores, trabalham o atual tema do direito ao esquecimento, normalmente tratado de forma restrita ao direito constitucional, é analisado também em termos dos processos de criminalização. São identificados o direito à honra e intimidade como forma de prevenir futuros processos de estigmatização. Desta forma, está violada não apenas a dignidade humana do sujeito criminalizado, assim como a de seus familiares.

Tema também contemporâneo é o da lavagem de dinheiro e dos jogos de azar "online", analisado por Roberto Carvalho Veloso, Wendelson Pereira Pessoa e Monique Leray Costa. Os autores trabalham, em perspectiva comparada, com as regulamentações da Colômbia

(pioneira em normatizar a questão na América Latina) e a brasileira. Os autores defendem que, para além de regulação administrativa, é importante também a criminalização da conduta como forma de atenuar o problema.

O persistente problema do sistema prisional é discutido por Roberta Karina Cabral Kanzler , Wendelson Pereira Pessoa , Camila Kanzler Catunda da Silva. É debatida a questão da reinserção social enquanto (im)possibilidade de finalidade da pena, bem como trazida a teoria crítica da pena de Zaffaroni para o diálogo.

Os mesmos autores discutem o acordo de não persecução penal não apenas em termos dogmáticos, mas também na perspectiva político-criminal. Ao trabalhar o instituto, trazem o desenho legislativo previsto na Lei 13/964/2019 e problematizam a questão a partir do binômio eficiência x eficácia das garantias constitucionais fundamentais.

O trabalho, intitulado "PROCESSO DE CRIMINALIZAÇÃO QUATERNÁRIA: DADOS E REALIDADE SOBRE A (IN)TRANSCENDÊNCIA DA PENA PRIVATIVA DE LIBERDADE NO SISTEMA DE JUSTIÇA CRIMINAL EM IJUÍ", de autoria de Thiago dos Santos da Silva, Emmanuelle de Araujo Malgarim e Nelci Lurdes Gayeski Meneguzzi, tem como objetivo geral apresentar o papel da pesquisa acadêmica em direito sobre temas complexos, a partir da análise das condições de vulnerabilidade social e criminalização, explicitando as diversas violações dos princípios da dignidade humana e da personalidade da pena sofridas por familiares de pessoas encarceradas. A pesquisa qualitativa e exploratória questiona a efetividade do princípio da personalidade da pena no sistema carcerário brasileiro, focando em como a pena transcende o corpo do condenado, atingindo seus familiares.

A seguir, foi apresentado o texto intitulado "DESAFIOS E POSSIBILIDADES DE REINTEGRAÇÃO PELA LEITURA: UMA ANÁLISE A PARTIR DO PROJETO DE EXTENSÃO “LEITURA E EXISTÊNCIA” DA UNIJUÍ", de autoria de Thiago dos Santos da Silva, Patrícia Borges Moura e Patricia Marques Oliveski, tem como objetivo geral apresentar o projeto “Leitura e Existência” e o papel do letramento literário na reinserção social de apenados, como reforço ao direito à remição pela leitura, com foco na PMEI. O estudo analisa o papel da universidade na implementação da remição pela leitura, confirmando a hipótese de que o letramento literário fortalece a reinserção social e garante a dignidade das pessoas privadas de liberdade.

O objetivo do artigo "O CRIME DE ROUBO PRATICADO NO PERÍODO NOTURNO COMO CIRCUNSTÂNCIA JUDICIAL NEGATIVA E A ANÁLISE DA

JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA" é analisar criticamente a possibilidade de majorar a pena-base do roubo apenas pelo horário noturno. Os autores, Yuri Anderson Pereira Jurubeba, Bruna Patricia Ferreira Pinto e Fernanda Matos Fernandes de Oliveira Jurubeba, concluem que a jurisprudência do STJ rechaça essa majoração isolada, exigindo fundamentação específica para evitar violação ao princípio da legalidade estrita e aos direitos fundamentais do acusado.

Os mesmos pesquisadores examinam os desafios processuais da Lei nº 15.123/2025, que aumentou a pena para crimes de violência psicológica contra a mulher com uso de IA. O artigo conclui que é premente a instituição de protocolos específicos de cadeia de custódia para prova digital, visando garantir a autenticidade e integridade da prova e a segurança jurídica.

André Vecchi e José Luiz de Moura Faleiros Júnior são os autores do ensaio "RESPONSABILIDADE PENAL DOS SISTEMAS AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL: REFLEXÕES E PERSPECTIVAS JURÍDICAS FRENTE À DOGMÁTICA DO DELITO". O objetivo do trabalho é tentar vislumbrar a possibilidade de atribuir responsabilidade penal a sistemas inteligentes que causem lesões a bens jurídicos relevantes. O ensaio aborda as dificuldades de responsabilização das máquinas frente à dogmática penal atual, que se vê desafiada pelo surgimento da Inteligência Artificial.

A seguir, André Vecchi e Luciano Santos Lopes trabalham soluções para a aferição da tipicidade subjetiva no crime de lavagem de capitais, analisando se sua prática é possível apenas na modalidade dolo direto ou se também é admissível o dolo eventual. O artigo “A Imputação Subjetiva no Crime de Lavagem de Capitais” busca fixar parâmetros dogmáticos e propor soluções para as dificuldades probatórias da imputação subjetiva no processo penal.

José Guimarães Mendes Neto, Lucas Rafael Chaves de Sousa e Thiago França Sousa são os autores do trabalho "TEORIA DA PROVA NO PROCESSO PENAL E VEDAÇÃO À REVITIMIZAÇÃO: ANÁLISE DA ADPF 1107 E DOS PROTOCOLOS DO CNJ PARA JULGAMENTO COM PERSPECTIVA DE GÊNERO". O objetivo do estudo é investigar como a ADPF 1107 e os Protocolos do CNJ ressignificam a teoria da prova no processo penal, a partir da vedação à revitimização. O trabalho conclui que a tutela da dignidade da vítima se torna um novo pilar da dogmática probatória, exigindo reforma cultural dos operadores do Direito.

Wanderson Carlos Medeiros Abreu, Thiago França Sousa e Lucas Rafael Chaves de Sousa são os autores do trabalho "A ATIPICIDADE DO LINCHAMENTO NO DIREITO PENAL

BRASILEIRO: INCONGRUÊNCIAS DOGMÁTICAS E POLÍTICO-CRIMINAIS E CAMINHOS PARA O ENFRENTAMENTO INSTITUCIONAL". O objetivo do trabalho é identificar as incongruências dogmáticas e falhas político-criminais decorrentes da ausência de um tipo penal próprio para o linchamento no Brasil. O artigo propõe a reformulação do direito penal, com a criação de um tipo penal específico ou qualificadora, para oferecer uma resposta institucional mais proporcional a esse fenômeno de violência coletiva.

Em seguida foi apresentado o trabalho "A ARQUITETURA LEGISLATIVA DA PUNIÇÃO: COALIZÕES, NECROPOLÍTICA E A PRODUÇÃO SELETIVA DA POLÍTICA CRIMINAL NO CONGRESSO NACIONAL BRASILEIRO PÓS-1988", de autoria de Kennedy Da Nobrega Martins, Alexandre Manuel Lopes Rodrigues e Lucas Victtor De Carvalho Gomes .O objetivo é analisar como o Congresso Nacional, pós-1988, produziu e consolidou um modelo de política criminal seletiva, atravessado por coalizões e uma racionalidade necropolítica. O artigo conclui que a seletividade penal é uma escolha política que esvazia a promessa constitucional de cidadania universal.

João Pedro Rêgo Balata, Emanoelle de Alencar Pereira e Wanderson Carlos Medeiros Abreu são os autores do artigo "A AMEAÇA DO CARÁTER SUBJETIVO DO DEPOIMENTO ESPECIAL ÀS GARANTIAS PROCESSUAIS EM CASOS DE VIOLÊNCIA SEXUAL INFANTO-JUVENIL". O objetivo é examinar como o caráter subjetivo do depoimento especial (Lei n.º 13.431/2017) tensiona garantias processuais como o contraditório e a ampla defesa. O trabalho busca evidenciar os dilemas do instituto e a necessidade de maior rigor metodológico e parâmetros claros de confiabilidade, sem perder sua função protetiva.

Deise Neves Nazaré Rios Brito e Alexandre Manuel Lopes Rodrigues Investigam como a midiatização interfere na distinção entre dolo eventual e culpa consciente em casos de grande repercussão social no Brasil a partir de 2010, examinando fundamentos teóricos e propondo diretrizes de mitigação. O trabalho utiliza metodologia qualitativa com análise de casos paradigmáticos (Boate Kiss, Mariana, Brumadinho, Nardoni e Mariana Ferrer), demonstrando que a cobertura midiática dilui fronteiras dogmáticas entre institutos penais, favorece responsabilização pelo resultado e fragiliza presunção de inocência e devido processo legal, comprometendo imparcialidade judicial e segurança jurídica.

Por fim, Lucas Nacur Almeida Ricardo, Ana Carolina Letayf Campos e Luciano Santos Lopes analisam a diferenciação entre atos de preparação (impuníveis) e atos de execução (puníveis como tentativa) no iter criminis, propondo critérios interpretativos para o conceito de "iniciada a execução" mediante precedente vinculante. O artigo analisa o art. 14, II, do Código Penal, expõe teorias justificadoras da punição da tentativa, examina jurisprudência do

STJ que adota a teoria objetivo-formal e problematiza esse posicionamento por potencialmente gerar decisões desproporcionais e proteção penal insuficiente, considerando as obrigações processuais positivas do Estado de proteger bens jurídicos e vítimas, buscando equilíbrio entre legalidade e tutela efetiva.

Foi um privilégio poder acompanhar tantas discussões de excepcional nível acadêmico. Que venham os próximos encontros e debates!

São Paulo, Primavera de 2025.

Gustavo Noronha de Ávila

Rogerio Luiz Nery Da Silva

INTELIGÊNCIA ARTIFICIAL, PROVA DIGITAL E PROCESSO PENAL: DESAFIOS DA LEI 15.123/2025 E A URGÊNCIA DE NOVOS PROTOCOLOS DE CADEIA DE CUSTÓDIA

ARTIFICIAL INTELLIGENCE, DIGITAL EVIDENCE AND CRIMINAL PROCEDURE: CHALLENGES OF LAW NO. 15,123/2025 AND THE URGENCY OF NEW CHAIN OF CUSTODY PROTOCOLS

Yuri Anderson Pereira Jurubeba
Fernanda Matos Fernandes de Oliveira Jurubeba
Bruna Patricia Ferreira Pinto

Resumo

O presente artigo examina os desafios processuais decorrentes da Lei nº 15.123, de 24 de abril de 2025, a qual instituiu causa de aumento de pena para crimes de violência psicológica contra a mulher praticados mediante utilização de inteligência artificial. Embora se trate de diploma de natureza penal-material, sua aplicação pressupõe a produção de prova digital, circunstância que projeta efeitos diretos no processo penal. Analisa-se, nesse contexto, a necessidade de assegurar a autenticidade, a integridade e a rastreabilidade das provas, especialmente diante da suscetibilidade de manipulação de conteúdos gerados por inteligência artificial. A investigação, fundamentada em abordagem doutrinária, jurisprudencial e comparativa, com respaldo em fontes primárias e em padrões técnicos verificáveis, demonstra que a eficácia da nova legislação depende não apenas da dimensão substancial da norma, mas sobretudo da implementação de garantias processuais sólidas, ancoradas em fluxos operacionais auditáveis e em padrões internacionais de segurança. Conclui-se que é premente a instituição de protocolos técnicos e jurídicos específicos para delitos que envolvam o uso de inteligência artificial, sob pena de comprometimento da segurança jurídica e da tutela efetiva dos direitos fundamentais.

Palavras-chave: Lei 15.123/2025, Cadeia de custódia, Prova digital, Inteligência artificial, Deepfake

Abstract/Resumen/Résumé

This article examines the procedural challenges arising from Law No. 15,123, enacted on April 24, 2025, which established a penalty enhancement for crimes of psychological violence against women committed through the use of artificial intelligence. Although the law is primarily substantive in nature, its enforcement fundamentally relies on digital evidence, which directly impacts criminal procedure. Within this framework, the study addresses the need to ensure the authenticity, integrity, and traceability of such evidence, particularly given the risks of manipulation associated with AI-generated content. Based on doctrinal, jurisprudential, and comparative analysis, supported by primary sources and verifiable technical standards, the research demonstrates that the effectiveness of the new

legislation depends not only on its substantive application but also on the establishment of robust procedural safeguards grounded in auditable operational flows and international technical standards. The study concludes that the urgent development of specific technical and legal protocols for crimes involving artificial intelligence is indispensable to guarantee legal certainty and the protection of fundamental rights.

Keywords/Palabras-claves/Mots-clés: Law 15.123/2025, Chain of custody, Digital evidence, Artificial intelligence, Deepfake

1 INTRODUÇÃO

A promulgação da Lei nº 15.123, de 24 de abril de 2025, constitui marco relevante no ordenamento jurídico brasileiro, ao introduzir inovação legislativa voltada ao enfrentamento da violência psicológica contra a mulher perpetrada mediante o uso de recursos tecnológicos avançados (BRASIL, 2025a). O diploma alterou o artigo 147-B do Código Penal, estabelecendo causa de aumento de pena quando a conduta criminosa é praticada mediante emprego de inteligência artificial ou de outro recurso tecnológico apto a alterar a imagem ou o som da vítima.

Tal inovação decorre do crescimento expressivo de práticas ilícitas relacionadas a deepfakes e outras formas de manipulação digital que têm sido instrumentalizadas como mecanismos de violência de gênero. Chesney e Citron (2019) ressaltam que a inteligência artificial tem sido utilizada de modo criminoso na criação de conteúdos falsos capazes de gerar danos psicológicos significativos às vítimas, sobretudo por meio da produção de imagens, vídeos ou áudios simulando situações comprometedoras ou vexatórias.

O enfoque do presente estudo encontra fundamento na natureza peculiar da Lei nº 15.123/2025, que, embora se caracterize como norma de direito penal material, demanda, para sua efetiva aplicação, a produção e a adequada valoração da prova digital em sede processual. A dependência de instrumentos probatórios dessa natureza revela desafios que ultrapassam a mera tipificação legal, exigindo reflexão aprofundada acerca dos mecanismos de aferição de autenticidade, integridade e rastreabilidade da prova digital.

O problema central delineia-se a partir de questionamentos múltiplos: de que forma assegurar a confiabilidade da prova digital em crimes que envolvem a utilização de inteligência artificial, considerando o risco crescente de manipulação de conteúdos gerados por tais tecnologias? A complexidade da questão é ampliada pelo fato de que os próprios meios empregados para a prática delitiva — como deepfakes, clonagem de voz e manipulação de imagens — têm como objetivo produzir material falso de difícil distinção em relação ao real.

Nesse cenário, a cadeia de custódia da prova digital, regulamentada pelos artigos 158-A a 158-F do Código de Processo Penal por intermédio da Lei nº 13.964, de 24 de dezembro de 2019, adquire especial relevância (BRASIL, 2019). Todavia, os protocolos até então estabelecidos foram concebidos para provas digitais convencionais, não

contemplando as especificidades introduzidas pelos crimes mediados por inteligência artificial.

Pesquisas recentes reforçam que a manipulação de conteúdos digitais mediante IA representa ameaça concreta à credibilidade da prova no processo judicial. Verdoliva (2020) argumenta que a sofisticação crescente das técnicas de deepfake desafia os métodos tradicionais de autenticação, impondo a necessidade de desenvolvimento de novos protocolos técnicos e jurídicos compatíveis com padrões internacionais auditáveis.

A relevância da investigação ora proposta extrapola o campo acadêmico, alcançando implicações práticas para magistrados, membros do Ministério Público, defensores, peritos criminais e formuladores de políticas públicas. A inexistência de protocolos específicos voltados a crimes com uso de IA pode conduzir à ineficácia da Lei nº 15.123/2025, comprometendo a proteção das vítimas e a própria segurança jurídica dos acusados.

O artigo organiza-se em cinco eixos centrais, além da introdução e das considerações finais. Inicialmente, examina-se o contexto normativo da cadeia de custódia no processo penal brasileiro e sua correlação com a nova lei. Em seguida, abordam-se a natureza e as peculiaridades da prova digital em delitos envolvendo inteligência artificial. Na terceira seção, discute-se a vulnerabilidade da cadeia de custódia diante dos riscos específicos desses crimes. A quarta seção é dedicada à análise crítica das lacunas normativas nacionais em cotejo com experiências internacionais. Por fim, a quinta seção apresenta propostas de aperfeiçoamento do sistema probatório brasileiro, mediante a definição de fluxos operacionais detalhados e padrões técnicos auditáveis.

A metodologia adotada fundamenta-se em pesquisa bibliográfica e documental, com análise da legislação, da doutrina, da jurisprudência e de estudos comparativos. A abordagem é qualitativa, com ênfase crítica na avaliação da adequação das normas processuais vigentes frente aos desafios impostos pela nova realidade tecnológica. Para tanto, recorre-se a padrões técnicos internacionalmente reconhecidos, como a ABNT NBR ISO/IEC 27037:2013, as diretrizes do Scientific Working Group on Digital Evidence (SWGDE) e as especificações do National Institute of Standards and Technology (NIST).

2 CONTEXTO NORMATIVO E FLUXO OPERACIONAL DA CADEIA DE CUSTÓDIA

A cadeia de custódia da prova no processo penal brasileiro passou a contar com regulamentação formal a partir da Lei nº 13.964, de 24 de dezembro de 2019, conhecida como "Pacote Anticrime", que introduziu os artigos 158-A a 158-F no Código de Processo Penal (BRASIL, 2019). Essa inovação normativa consolidou, pela primeira vez no ordenamento jurídico nacional, um conceito legal específico de cadeia de custódia, representando marco relevante na sistematização dos procedimentos probatórios.

O artigo 158-A do CPP define cadeia de custódia como o conjunto de procedimentos destinados a manter e documentar a história cronológica do vestígio coletado em locais de crime ou em vítimas, possibilitando o rastreamento de sua posse e manuseio desde o reconhecimento até o descarte (BRASIL, 1941). A amplitude dessa definição estabelece os alicerces de um sistema probatório mais rigoroso e confiável, aspecto particularmente relevante diante do avanço da digitalização das evidências criminais.

A normatização brasileira alinhou-se à tendência internacional verificada em diversos sistemas jurídicos, influenciada, em especial, pelas diretrizes técnicas elaboradas pelo National Institute of Standards and Technology (NIST), nos Estados Unidos, e pelas práticas consolidadas no âmbito da Convenção de Budapeste sobre Cibercrime (COUNCIL OF EUROPE, 2001). Tais instrumentos ressaltam a necessidade de preservação da integridade probatória em um cenário de crescente sofisticação tecnológica e circulação transnacional de provas digitais.

Nos termos do artigo 158-B do CPP, a cadeia de custódia compreende dez etapas fundamentais: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte (BRASIL, 1941). Cada uma dessas fases deve ser documentada de forma contínua e ininterrupta, de modo a constituir registro cronológico íntegro que assegure o rastreamento completo do vestígio, desde sua identificação inicial até sua destinação final.

Nos crimes que envolvem a utilização de inteligência artificial, a cadeia de custódia exige um fluxo operacional especializado, capaz de contemplar as especificidades técnicas dessa categoria de evidência. O modelo proposto baseia-se nas diretrizes da ABNT NBR ISO/IEC 27037:2013 e nas melhores práticas desenvolvidas pelo Scientific Working Group on Digital Evidence (SWGDE), de modo a assegurar rastreabilidade, integridade e confiabilidade probatória.

A primeira etapa refere-se ao reconhecimento e à identificação inicial da evidência digital. O responsável deve documentar a natureza do material e verificar

indícios de manipulação por inteligência artificial. Essa fase compreende o registro fotográfico do estado original dos dispositivos, a identificação de eventuais aplicativos de geração de IA instalados, a verificação de credenciais de autenticidade como C2PA/CAI quando existentes, a documentação dos metadados visíveis e o registro da data, da hora do sistema e das configurações de rede.

A segunda etapa consiste no isolamento e na preservação do estado original. Nessa fase, busca-se impedir qualquer alteração da evidência durante a coleta. Os procedimentos necessários incluem a desconexão dos dispositivos de redes para evitar sincronizações automáticas, a preservação do estado de energia, o bloqueio de escrita em mídias de armazenamento, a documentação de todos os dispositivos conectados e a coleta de dados voláteis, como a memória RAM, quando viável tecnicamente.

Na terceira etapa, de coleta e aquisição forense, é imprescindível empregar metodologia que preserve a integridade bit a bit da evidência. São medidas essenciais a criação de imagem forense completa mediante ferramentas validadas, a geração de hash criptográfico (preferencialmente SHA-256) do arquivo original, a aplicação de carimbo de tempo confiável nos termos da RFC 3161 ou de serviços TSA, a coleta de logs de sistema relevantes e a preservação de metadados estendidos e informações de proveniência.

A quarta etapa, de acondicionamento e documentação, exige que a evidência seja armazenada em contêiner com logs imutáveis. Esse processo envolve a preservação do arquivo fonte completo, a criação de cópias de trabalho verificadas, a documentação da cadeia de manuseio, o registro das ferramentas e versões utilizadas e a atribuição de identificador único para cada item.

A quinta etapa diz respeito ao transporte e ao recebimento da evidência. Deve-se assegurar que não ocorra alteração, corrupção ou perda de dados. Entre os controles necessários, incluem-se a verificação de integridade por meio de hash, a documentação de todos os manuseios, o registro de responsáveis e horários, a confirmação de recebimento e a atualização do sistema de controle de evidências.

Na sexta etapa, relativa ao processamento e à análise pericial, a avaliação deve ser realizada exclusivamente em cópias verificadas, preservando-se o original. A metodologia exige a checagem prévia da integridade do material, o uso de ferramentas validadas e auditáveis, a documentação minuciosa dos procedimentos aplicados, o registro de parâmetros e configurações utilizadas e a preservação dos resultados intermediários.

A sétima e última etapa refere-se à elaboração do laudo e à verificação por pares. O relatório pericial deve conter descrição completa da metodologia empregada, identificação das limitações e do grau de confiança, anexação de evidências de suporte, revisão por especialista independente quando se tratar de análises tecnicamente complexas e disponibilização de dados para eventual contraprova.

A efetiva implementação do fluxo operacional delineado requer o emprego de ferramentas e padrões técnicos auditáveis, capazes de garantir reprodutibilidade e verificabilidade dos procedimentos. Nesse sentido, as ferramentas devem atender aos critérios definidos pelo programa Computer Forensics Tool Testing (CFTT), do National Institute of Standards and Technology (NIST), e seguir as diretrizes da SWGDE para a análise de evidências digitais.

O uso do hash SHA-256, aliado ao registro em conformidade com a RFC 3161, configura requisito indispensável. A aplicação imediata do hash após a coleta, com registro em serviço de carimbo de tempo confiável, permite detectar qualquer alteração posterior e estabelecer marco temporal verificável para a integridade da evidência.

A preservação deve ocorrer em contêiner com logs imutáveis, apto a registrar automaticamente todos os acessos e operações realizadas. O sistema deve documentar a data e a hora de cada acesso, a identificação do usuário responsável, o tipo de operação, as ferramentas utilizadas e os resultados obtidos, garantindo rastreabilidade plena.

Outro requisito é a manutenção do denominado “original melhor”, isto é, a preservação do arquivo fonte na forma mais próxima possível do estado original. As análises devem ser realizadas exclusivamente em cópias verificadas, assegurando que o material original permaneça intocado e possa servir como referência em verificações posteriores.

Por fim, impõe-se que as ferramentas de análise aplicadas a evidências digitais associadas à inteligência artificial tenham sido submetidas a validação técnica, preferencialmente no âmbito do programa NIST CFTT ou equivalente. Essas ferramentas devem ser aptas a detectar indícios de manipulação artificial, preservar metadados originais, gerar relatórios auditáveis e possibilitar verificação independente dos resultados produzidos.

A promulgação da Lei nº 15.123, de 24 de abril de 2025, insere-se no contexto de enfrentamento aos desafios impostos pela evolução tecnológica no âmbito da violência de gênero. O diploma não criou tipo penal autônomo, mas introduziu qualificadora ao

delito de violência psicológica contra a mulher, já previsto no artigo 147-B do Código Penal.

De acordo com a redação conferida ao dispositivo legal, a pena será aumentada de metade quando a infração for praticada mediante uso de inteligência artificial ou de outro recurso tecnológico destinado a alterar a imagem ou o som da vítima (BRASIL, 2025a). Essa formulação legislativa evidencia a preocupação em coibir novas modalidades de agressão que utilizam tecnologias avançadas para potencializar o dano psicológico infligido às vítimas.

A justificativa para o agravamento da resposta penal encontra respaldo no reconhecimento de que a utilização de inteligência artificial amplia substancialmente o potencial lesivo da conduta criminosa. Chesney e Citron (2019) destacam que deepfakes e outras formas de manipulação digital possuem capacidade de gerar danos psicológicos duradouros e de comprometer de forma intensa a reputação e a dignidade da vítima, em grau superior ao verificado nas formas tradicionais de violência psicológica.

Embora a Lei nº 15.123/2025 seja, em sua essência, norma de direito penal material, sua efetividade depende da articulação com regras processuais de prova e com padrões técnicos internacionalmente reconhecidos. Essa interdependência revela-se especialmente no momento de comprovar, no curso do processo penal, que a conduta delitiva foi efetivamente praticada mediante uso de inteligência artificial ou de outro recurso tecnológico capaz de alterar a imagem ou o som da vítima.

A demonstração dessa circunstância qualificadora exige a produção de evidências digitais complexas, frequentemente submetidas a análises periciais sofisticadas destinadas a identificar sinais de manipulação artificial em conteúdos audiovisuais. Essa necessidade probatória expõe as limitações dos protocolos tradicionais de cadeia de custódia quando aplicados a evidências produzidas ou alteradas por inteligência artificial, cujo caráter intrinsecamente sintético desafia as metodologias convencionais de verificação de autenticidade.

A doutrina processual penal ressalta que a eficácia de normas cuja aplicação depende de prova técnica especializada está diretamente vinculada à qualidade e à confiabilidade dos procedimentos adotados, sobretudo quando estes observam padrões técnicos internacionais. No caso da Lei nº 15.123/2025, essa vinculação revela-se ainda mais sensível, dado que a própria dinâmica criminosa — baseada na manipulação digital por meio de IA — pode comprometer a credibilidade das evidências se não houver rigor metodológico na sua produção e conservação.

A integração de protocolos probatórios com padrões internacionais, como a ABNT NBR ISO/IEC 27037:2013, voltada ao tratamento de evidências digitais, e as diretrizes do Scientific Working Group on Digital Evidence (SWGDE), aplicáveis à análise forense de imagens e vídeos, constitui elemento indispensável para conferir legitimidade e confiabilidade às provas produzidas. Esses referenciais oferecem base sólida para o desenvolvimento de fluxos operacionais especializados que respondam adequadamente às exigências da nova legislação.

3 NATUREZA E PECULIARIDADES DA PROVA DIGITAL EM CRIMES COM INTELIGÊNCIA ARTIFICIAL

No processo penal brasileiro, a prova digital tradicional abrange mensagens eletrônicas, e-mails, fotografias digitais, registros de navegação e dados armazenados em dispositivos, submetidos a padrões consolidados de coleta, preservação e análise, orientados pela ABNT NBR ISO/IEC 27037:2013. Já a prova derivada de inteligência artificial possui características distintas, incluindo deepfakes, imagens sintéticas, textos produzidos por algoritmos e outras mídias geradas por machine learning e deep learning. Enquanto a prova tradicional registra eventos efetivamente ocorridos, a prova produzida por inteligência artificial pode consistir em simulações, impondo protocolos especializados baseados em padrões técnicos auditáveis.

A volatilidade dos dados digitais, já reconhecida como desafio da perícia tradicional, torna-se mais complexa nas evidências de inteligência artificial, pois os algoritmos modificam continuamente os dados, gerando versões inconsistentes. Para enfrentá-la, o Scientific Working Group on Digital Evidence (SWGDE) recomenda captura imediata do estado original com hash criptográfico, preferencialmente SHA-256, aplicação de carimbo de tempo conforme a RFC 3161, preservação de versões intermediárias, documentação do ambiente computacional e registros imutáveis de todas as operações. A autenticação de conteúdos derivados de inteligência artificial constitui desafio central, pois métodos tradicionais não bastam diante de mídias artificiais semelhantes a genuínas. Superar essa limitação requer múltiplas verificações, como análise temporal segundo a SWGDE, detecção de padrões de compressão, uso de algoritmos validados pelo CFTT do NIST, checagem de credenciais C2PA e análise cruzada por ferramentas independentes.

A preservação da integridade de evidências digitais relacionadas à inteligência artificial demanda protocolos mais sofisticados, incluindo informações sobre algoritmos, dados de treinamento e versões de software. Metadados devem indicar proveniência dos dados, técnicas de pré-processamento, hiperparâmetros, métricas de qualidade e, quando existentes, trilhas de auditoria criptográficas, indispensáveis para a reprodução e verificação independente dos resultados.

Os sistemas de detecção de deepfakes não estão imunes a falsos positivos, que classificam como artificiais conteúdos autênticos, comprometendo o processo penal. A mitigação exige protocolos de verificação cruzada, uso de múltiplas ferramentas validadas, análise manual de perito, revisão por pares e documentação do grau de confiança. Mais graves são os falsos negativos, quando conteúdos manipulados não são detectados, admitindo provas fraudulentas. A prevenção requer ferramentas constantemente atualizadas e validadas, metodologias complementares, verificação de credenciais, exame contextual e documentação transparente das limitações técnicas.

A análise de conteúdos manipulados por inteligência artificial deve seguir protocolos internacionais. Para deepfakes em vídeo, aplicam-se as SWGDE Best Practices for Digital Forensic Video Analysis (Versão 1.1, de 22 de março de 2024), que orientam preservação do arquivo nativo, análise de metadados estendidos, consistências temporais, detecção de artefatos de compressão e documentação completa. Para áudio, devem-se aplicar as diretrizes da SWGDE voltadas à análise espectral, padrões de respiração e prosódia, inconsistências na qualidade, artefatos de síntese e comparação com amostras de referência. Para imagens sintéticas, recomendam-se a análise de ruídos, verificação de iluminação e sombras, detecção de artefatos por algoritmos validados, exame de metadados EXIF e XMP e, quando aplicável, credenciais C2PA.

4 CADEIA DE CUSTÓDIA E RISCOS DE QUEBRA EM EVIDÊNCIAS COM INTELIGÊNCIA ARTIFICIAL

Os artigos 158-A a 158-F do Código de Processo Penal estabelecem protocolo rigoroso para preservar a integridade probatória, com dez etapas da cadeia de custódia: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte (BRASIL, 2019). No caso de evidências digitais derivadas de inteligência artificial, cada etapa deve seguir protocolos especializados previstos na ABNT NBR ISO/IEC 27037:2013 e nas diretrizes do

Scientific Working Group on Digital Evidence (SWGDE). O reconhecimento deve incluir análise preliminar de manipulação artificial, e a coleta exige preservação do ambiente computacional, coleta de logs, documentação de aplicativos, aplicação imediata de hash SHA-256 e carimbo de tempo conforme a RFC 3161.

A manipulação invisível constitui vulnerabilidade crítica, pois não deixa rastros perceptíveis por métodos tradicionais. Para enfrentá-la, recomendam-se análise com algoritmos validados pelo CFTT do NIST, verificação de compressão segundo a SWGDE, exame de metadados estendidos, uso de ferramentas independentes e checagem de credenciais C2PA. Outra fragilidade decorre da ausência de registros de origem em sistemas de geração artificial, mitigada pela coleta de logs, preservação de trilhas de auditoria, documentação do ambiente, recuperação de dados excluídos e manutenção de registros cronológicos imutáveis. O avanço de softwares de edição com inteligência artificial intensifica os riscos, exigindo contramedidas como análise espectral conforme a SWGDE, verificação temporal, análise de compressões múltiplas, checagem de iluminação e uso de machine learning para detecção de manipulações.

A jurisprudência do Superior Tribunal de Justiça exige rigor na preservação da cadeia de custódia em provas digitais. Em precedente paradigmático (AgRg no HC n. 828.054/RN, 23/04/2024, rel. Min. Joel Ilan Paciornik), a Quinta Turma considerou inadmissíveis provas extraídas de dispositivos móveis sem metodologia idônea (BRASIL, 2024). O acórdão destacou que a ausência de documentação detalhada configura quebra da cadeia de custódia, tornando a prova imprestável. Esses entendimentos aplicam-se integralmente às provas com inteligência artificial, exigindo documentação minuciosa, verificação com hash SHA-256 e registro temporal, preservação do arquivo nativo segundo a SWGDE, ferramentas validadas pelo NIST CFTT e documentação transparente do grau de confiança de cada análise.

A quebra da cadeia de custódia acarreta nulidade processual, comprometendo a persecução penal, sobretudo quando ausentes padrões técnicos reconhecidos. Nos crimes envolvendo inteligência artificial, a confiabilidade da prova demanda demonstração de conformidade com a ABNT NBR ISO/IEC 27037:2013, com as melhores práticas da SWGDE, ferramentas validadas pelo NIST CFTT e preservação de trilhas de auditoria. A falta de observância compromete a convicção judicial e a legitimidade do processo, podendo corroer a credibilidade do sistema de justiça criminal em um contexto de crescente digitalização das relações sociais.

5 ANÁLISE CRÍTICA E ALINHAMENTO COM PADRÕES INTERNACIONAIS

A análise do ordenamento jurídico brasileiro evidencia lacuna relevante no que se refere à regulamentação de protocolos específicos voltados ao tratamento de crimes relacionados ao uso de inteligência artificial. Embora a Lei nº 15.123, de 24 de abril de 2025, tenha introduzido previsão penal adequada ao estabelecer causa de aumento de pena para a violência psicológica contra a mulher praticada mediante recursos tecnológicos avançados, o sistema processual não dispõe de diretrizes técnicas especializadas para a coleta, preservação e análise de evidências digitais derivadas ou manipuladas por inteligência artificial.

Essa ausência de regulamentação contrasta com a complexidade técnica que caracteriza a manipulação digital contemporânea, em especial na produção de deepfakes e outras formas de conteúdo sintético. A aplicação de protocolos genéricos de cadeia de custódia a esse tipo de prova pode acarretar perda de informações cruciais ou mesmo comprometer a integridade do material probatório.

A experiência comparada demonstra que a regulação eficaz de delitos praticados com uso de inteligência artificial requer não apenas a tipificação penal, mas também a elaboração de protocolos técnicos específicos que contemplem as peculiaridades dessas evidências. A inexistência de tais protocolos no Brasil pode comprometer a efetividade da Lei nº 15.123/2025 e ocasionar disparidades na aplicação da justiça entre diferentes jurisdições nacionais.

O Regulamento (UE) 2024/1689, conhecido como AI Act, estabelece obrigações detalhadas de rotulagem para conteúdos gerados ou manipulados por inteligência artificial, oferecendo modelo direto de implementação para o contexto brasileiro. O artigo 50 do referido regulamento determina que sistemas de IA que geram imagens, áudios ou vídeos assegurem que o material sintético seja marcado de forma detectável por máquina e identificado como artificialmente produzido ou manipulado (EUROPEAN UNION, 2024).

Essa obrigação de transparência facilita a identificação de evidências potencialmente problemáticas no processo penal, sobretudo quando associada a padrões técnicos como o Coalition for Content Provenance and Authenticity (C2PA). A rotulagem com credenciais verificáveis possibilita checagem automática de autenticidade já nas fases iniciais da investigação criminal.

O mesmo artigo estabelece ainda que os fornecedores de sistemas de inteligência artificial devem projetá-los de modo a garantir que os conteúdos sintéticos sejam claramente identificáveis pelos usuários. Essa exigência cria condições técnicas para a implementação de credenciais criptográficas aptas a serem verificadas durante a cadeia de custódia probatória.

A implementação prática das obrigações previstas no AI Act encontra fundamento técnico na especificação C2PA, em sua versão 2.2, que define credenciais criptográficas para rastreamento da proveniência de conteúdos digitais. Esse padrão permite a constituição de trilhas de auditoria que documentam origem, modificações e cadeia de custódia de arquivos por meio de assinaturas criptográficas e registros temporais confiáveis.

As credenciais C2PA contêm informações sobre a origem do conteúdo e o dispositivo de captura, o software empregado na criação ou edição, o histórico completo de modificações, as assinaturas criptográficas verificáveis e os respectivos carimbos de tempo. Esses elementos são essenciais para a preservação da cadeia de custódia em evidências relacionadas à inteligência artificial.

A Content Authenticity Initiative (CAI), em sua versão 2.1, complementa o padrão C2PA ao disponibilizar infraestrutura para verificação das credenciais e manutenção de registros confiáveis. A adoção combinada desses padrões no Brasil permitiria automatizar a verificação de autenticidade durante a coleta de provas, fortalecendo a efetividade da Lei nº 15.123/2025.

O artigo 12 do AI Act impõe requisitos específicos para a manutenção de registros detalhados de sistemas de inteligência artificial, incluindo dados de entrada, parâmetros de processamento e resultados produzidos. Esses requisitos, quando aplicados ao processo penal, tornam-se essenciais para a adequada preservação da cadeia de custódia em evidências envolvendo IA e podem ser implementados por meio de infraestruturas de chave pública (PKI) e protocolos de integridade baseados em hash criptográfico.

Os registros obrigatórios devem contemplar o histórico automático de todas as operações realizadas, a identificação dos dados de entrada, os parâmetros de configuração aplicados, os resultados intermediários e finais, além da fixação de carimbos de tempo verificáveis para cada operação. Essa documentação expandida possibilita a reconstrução completa do processo de geração ou manipulação do conteúdo, fortalecendo a confiabilidade da prova em ambiente judicial.

O documento NIST IR 8387 – Digital Evidence Preservation: Considerations for Evidence Handlers estabelece diretrizes específicas para a preservação de evidências digitais, aplicáveis de forma direta ao conteúdo produzido por inteligência artificial. O relatório reconhece que as provas envolvendo IA demandam procedimentos diferenciados, que ultrapassam os protocolos tradicionais de informática forense (NIST, 2023).

Entre as recomendações, destacam-se a necessidade de documentação dos algoritmos empregados na geração do conteúdo, a preservação de dados de treinamento sempre que tecnicamente viável, a verificação de integridade dos modelos de IA utilizados, a manutenção de trilhas de auditoria criptográficas e a adoção de múltiplas camadas de verificação.

Paralelamente, o programa NIST Computer Forensics Tool Testing (CFTT) define metodologias rigorosas para o teste e a validação de ferramentas forenses, inclusive aquelas voltadas à detecção de conteúdos sintéticos. As ferramentas validadas nesse programa oferecem garantia adicional de confiabilidade e de reprodutibilidade dos resultados periciais, elemento indispensável em processos penais que envolvem provas digitais de alta complexidade.

O Scientific Working Group on Digital Evidence (SWGDE) desenvolveu recomendações específicas para a análise forense de vídeo e imagem, diretamente aplicáveis a deepfakes e demais formas de conteúdo sintético. As Best Practices for Digital Forensic Video Analysis (Versão 1.1, de 22 de março de 2024) estabelecem metodologia sistemática para a preservação e análise de provas audiovisuais.

Essas diretrizes destacam a obrigatoriedade da preservação do arquivo nativo original, a documentação integral dos metadados estendidos, a aplicação de técnicas de verificação de integridade, a análise de consistências temporais e espaciais e a documentação transparente das limitações técnicas identificadas durante o exame.

Para a análise de imagens, a SWGDE recomenda protocolos voltados à detecção de artefatos de manipulação, à verificação de padrões de compressão, à análise de consistência de iluminação e sombras, ao exame de metadados EXIF e XMP e à aplicação de métodos de autenticação baseados em hash criptográfico. Tais procedimentos garantem maior robustez metodológica e mitigam riscos de falsos positivos ou negativos.

A inadequação dos protocolos atualmente utilizados para a cadeia de custódia de evidências digitais envolvendo inteligência artificial gera risco expressivo de nulidade processual. A jurisprudência do Superior Tribunal de Justiça tem consolidado posição no

sentido de que a ausência de documentação completa dos procedimentos de coleta e preservação compromete a confiabilidade da prova, tornando-a imprestável para fins processuais (BRASIL, 2024).

Esse entendimento assume especial relevância em crimes relacionados ao uso de inteligência artificial, nos quais a complexidade técnica das provas impõe a adoção de protocolos especializados baseados em padrões internacionais reconhecidos. A não observância de normas como a ABNT NBR ISO/IEC 27037:2013, das diretrizes da SWGDE e das especificações do NIST pode resultar na exclusão de elementos relevantes, comprometendo a persecução penal e, em casos de violência psicológica contra a mulher, aumentando o risco de impunidade dos agressores.

A crescente sofisticação dos crimes cometidos mediante o uso de inteligência artificial demanda maior integração entre os atores do sistema de justiça criminal, baseada em padrões técnicos comuns e em protocolos auditáveis. A eficácia das investigações depende da atuação coordenada entre polícia judiciária, Ministério Público e peritos criminais, cada qual contribuindo com expertise específica para assegurar a confiabilidade das provas.

À polícia judiciária cabe desenvolver capacidade técnica para o reconhecimento inicial de vestígios relacionados à IA, incluindo treinamento em padrões como C2PA/CAI e diretrizes da SWGDE. Essa capacitação é fundamental para garantir a preservação adequada das evidências desde os estágios iniciais da investigação.

O Ministério Público, por sua vez, necessita aprimorar a formulação de quesitos periciais fundamentados em padrões técnicos internacionalmente reconhecidos, além de desenvolver capacidade para interpretar laudos complexos envolvendo tecnologias de IA. A consistência da acusação em tais casos depende diretamente da compreensão das limitações e do grau de confiança das análises periciais.

Os peritos criminais devem contar com formação especializada em técnicas de análise de conteúdos gerados ou manipulados por IA, apoiada em referenciais internacionais. Isso inclui conhecimentos avançados sobre algoritmos de machine learning, utilização de ferramentas de detecção de deepfakes validadas pelo NIST CFTT e aplicação de metodologias de autenticação alinhadas às diretrizes da SWGDE. Tal especialização constitui requisito essencial para a produção de laudos periciais consistentes e confiáveis, aptos a subsidiar decisões judiciais seguras.

6 PROPOSTAS BASEADAS EM PADRÕES TÉCNICOS AUDITÁVEIS

A primeira necessidade identificada refere-se à criação de protocolos nacionais específicos para a coleta e preservação de provas digitais em casos que envolvem inteligência artificial, elaborados a partir de padrões técnicos internacionais auditáveis. Tais protocolos devem ser fruto de colaboração entre o Conselho Nacional de Justiça, o Ministério da Justiça e Segurança Pública, instituições acadêmicas especializadas e entidades técnicas competentes.

A proposta é que esses protocolos definam procedimentos detalhados, fundamentados na ABNT NBR ISO/IEC 27037:2013, adaptados às peculiaridades de diferentes tipos de evidência produzida por IA, como deepfakes de vídeo e áudio, imagens sintéticas e outros conteúdos gerados por algoritmos de machine learning. Cada categoria demandaria procedimentos próprios de identificação, coleta, preservação e análise, em consonância com as diretrizes correspondentes da SWGDE.

No caso específico de deepfakes de vídeo, os protocolos deveriam adotar as Best Practices for Digital Forensic Video Analysis da SWGDE (Versão 1.1, de 22 de março de 2024), com exigência de preservação do arquivo nativo original, aplicação imediata de hash criptográfico SHA-256 acompanhado de carimbo de tempo em conformidade com a RFC 3161, coleta de metadados estendidos, verificação de credenciais C2PA quando disponíveis e documentação integral do ambiente em que ocorreu a coleta.

A segunda proposta consiste no desenvolvimento e integração de ferramentas de verificação de autenticidade que obedeçam aos critérios estabelecidos pelo programa NIST Computer Forensics Tool Testing (CFTT) e às diretrizes da SWGDE voltadas à validação de instrumentos forenses. Essas ferramentas devem permitir análises preliminares já nas primeiras etapas da investigação, fornecendo indícios iniciais de possível manipulação artificial.

As ferramentas idealizadas devem contemplar técnicas de detecção múltiplas e validadas, incluindo a análise de inconsistências temporais de acordo com a SWGDE, a verificação de padrões de compressão mediante algoritmos aprovados pelo NIST CFTT, a detecção de artefatos de geração baseados em machine learning, a verificação automática de credenciais C2PA/CAI e a análise de metadados estendidos.

A integração dessas ferramentas aos sistemas de informação da polícia judiciária e do Ministério Público deve possibilitar análises automatizadas com capacidade de alertar os investigadores sobre potenciais conteúdos sintéticos, sempre sujeitas à revisão pericial especializada. Além disso, as ferramentas devem incluir mecanismos de

documentação automática que registrem os parâmetros aplicados, os resultados obtidos e o grau de confiança das detecções, em conformidade com padrões de auditabilidade técnica.

Outra medida proposta, de caráter normativo, envolve alteração pontual do Código de Processo Penal, de forma a prever expressamente a adoção de procedimentos especializados para a manipulação de provas digitais complexas. A modificação buscaria complementar os dispositivos já existentes sobre cadeia de custódia, sem desfigurar a estrutura geral do sistema probatório.

A redação sugerida prevê a inclusão de um novo artigo 158-G, dispondo que a coleta, a preservação e a análise de vestígios digitais gerados ou manipulados por inteligência artificial observarão protocolos específicos fundamentados em padrões técnicos internacionais, a serem definidos por regulamentação do Conselho Nacional de Justiça. Prevê-se ainda a obrigatoriedade de documentação expandida, de modo que a cadeia de custódia desses vestígios contemple registro detalhado dos algoritmos, ferramentas validadas e metodologias empregadas em todas as etapas, assegurando reprodutibilidade e verificação independente dos resultados.

Propõe-se, de forma complementar, a implementação de padrões de autenticidade de conteúdo baseados em credenciais criptográficas, inspirados no artigo 50 do AI Act da União Europeia. Essa medida estimularia a adoção voluntária, no Brasil, de tecnologias como a Coalition for Content Provenance and Authenticity (C2PA) – Versão 2.2 – e a Content Authenticity Initiative (CAI) – Versão 2.1.

A adoção desses padrões permitiria que conteúdos digitais legítimos fossem automaticamente marcados com credenciais de proveniência verificáveis, facilitando a identificação de materiais manipulados já no início da cadeia de custódia. Essa abordagem preventiva complementaria os métodos tradicionais de detecção de deepfakes, criando um ambiente de maior confiabilidade para o processamento de provas digitais.

Além disso, tais padrões deveriam ser integrados aos protocolos de cadeia de custódia estabelecidos pela ABNT NBR ISO/IEC 27037:2013, possibilitando que evidências dotadas de credenciais válidas fossem processadas de modo mais célere, enquanto aquelas sem credenciais ou com credenciais suspeitas fossem submetidas a exame pericial mais rigoroso com ferramentas validadas pelo NIST CFTT.

Outra proposta envolve a criação de centros regionais especializados em perícia digital, com foco específico na análise de conteúdos gerados por inteligência artificial, devidamente equipados com infraestrutura técnica auditável segundo padrões

internacionais. Esses centros deveriam atender múltiplas jurisdições, otimizando recursos técnicos e humanos altamente especializados.

Os centros projetados devem dispor de equipamentos compatíveis com as especificações da SWGDE e do NIST, incluindo servidores de alto desempenho para processamento de algoritmos de IA validados, sistemas de armazenamento seguro com registros imutáveis, ferramentas de análise forense aprovadas pelo NIST CFTT, infraestrutura para verificação de credenciais C2PA/CAI e sistemas de backup e recuperação em conformidade com padrões de continuidade.

As equipes desses centros devem ser multidisciplinares e compostas por peritos certificados em padrões internacionais, com especialização em análise forense de vídeo conforme diretrizes da SWGDE, detecção de deepfakes por ferramentas validadas, verificação de credenciais criptográficas, análise de metadados técnicos e implementação de protocolos de cadeia de custódia segundo a ABNT NBR ISO/IEC 27037:2013.

A dimensão transnacional dos crimes praticados com uso de inteligência artificial torna indispensável a criação de parcerias internacionais voltadas ao compartilhamento de expertise técnica e à cooperação em investigações, sempre com base em padrões técnicos comuns e protocolos auditáveis.

Nesse contexto, a adesão do Brasil ao Segundo Protocolo Adicional da Convenção de Budapeste sobre Cibercrime deve ser considerada prioritária, por fornecer arcabouço jurídico para cooperação em casos que envolvem evidências digitais complexas. Essa adesão facilitaria o intercâmbio de informações técnicas baseadas em referenciais comuns e a coordenação de investigações em âmbito transnacional.

Além disso, parcerias estratégicas com organizações internacionais, como o NIST e a SWGDE, poderiam assegurar acesso a recursos técnicos avançados, metodologias validadas e programas de capacitação. Essa cooperação internacional seria particularmente relevante diante das limitações de recursos internos para o desenvolvimento de expertise altamente especializada.

7 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permite concluir que a efetividade da Lei nº 15.123, de 24 de abril de 2025, ultrapassa sua dimensão estritamente penal-material, estando condicionada à adequação dos procedimentos processuais de produção e valoração da prova digital, necessariamente fundamentados em padrões técnicos

internacionais auditáveis. A previsão de causa de aumento de pena para a violência psicológica contra a mulher praticada mediante uso de inteligência artificial representa avanço legislativo expressivo, mas sua concretização prática enfrenta desafios complexos vinculados à preservação da cadeia de custódia da prova digital.

Constatou-se que as particularidades da prova derivada de inteligência artificial demandam protocolos especializados, distintos dos procedimentos tradicionais previstos nos artigos 158-A a 158-F do Código de Processo Penal. A possibilidade de criação de conteúdos sintéticos, muitas vezes indistinguíveis da realidade, por meio de deepfakes e outras técnicas de manipulação digital, constitui desafio inédito ao sistema probatório brasileiro, impondo adaptações relevantes nos métodos de coleta, preservação e análise de evidências.

A comparação com experiências internacionais revelou que jurisdições mais avançadas no enfrentamento de crimes envolvendo inteligência artificial estruturaram frameworks regulatórios abrangentes, combinando tipificação penal adequada com protocolos processuais técnicos e auditáveis. Nesse cenário, o AI Act da União Europeia, especialmente em seu artigo 50, que prevê obrigações de rotulagem e transparência para conteúdos sintéticos, oferece modelo de referência para aplicação no Brasil, mediante integração a padrões técnicos como C2PA e CAI.

As diretrizes da ABNT NBR ISO/IEC 27037:2013, as melhores práticas da SWGDE e as especificações do NIST constituem bases sólidas para a formulação de soluções nacionais adaptadas às peculiaridades do ordenamento jurídico brasileiro. A jurisprudência do Superior Tribunal de Justiça, ao adotar posicionamento cada vez mais rigoroso sobre a preservação da cadeia de custódia em evidências digitais, reforça a necessidade de implementação de protocolos específicos, devidamente alinhados a padrões técnicos internacionalmente reconhecidos.

As propostas apresentadas neste estudo visam suprir as lacunas identificadas a partir de uma abordagem multifacetada, que envolve a elaboração de protocolos técnicos nacionais baseados em padrões auditáveis, a capacitação profissional especializada, a integração de ferramentas tecnológicas validadas e a realização de ajustes legislativos com fundamento técnico sólido. A execução dessas medidas exige atuação coordenada entre diferentes atores do sistema de justiça e investimentos consistentes em infraestrutura técnica e formação qualificada.

A criação de protocolos nacionais específicos para evidências derivadas de inteligência artificial constitui prioridade absoluta, devendo ser resultado de cooperação

entre órgãos técnicos e validados por meio de testes rigorosos. Esses protocolos devem contemplar todas as modalidades de conteúdos sintéticos e estabelecer procedimentos detalhados para cada etapa da cadeia de custódia, em conformidade com padrões técnicos auditáveis.

A implementação de ferramentas de verificação de autenticidade, baseadas em especificações como C2PA e CAI e validadas pelo NIST CFTT, pode ampliar significativamente a eficiência das investigações. Contudo, tais instrumentos devem ser utilizados em conjunto com protocolos de verificação cruzada, sendo indispensável a análise pericial especializada orientada pelas diretrizes da SWGDE para a tomada de decisões processuais definitivas.

A proposta de alteração pontual do Código de Processo Penal, com a inserção de previsão expressa sobre procedimentos para prova digital complexa, fundamentada em padrões internacionais, representaria reforço normativo consistente, sem comprometer a estrutura geral do sistema probatório. Essa modificação deve ser suficientemente flexível para acompanhar a evolução tecnológica, mantendo sempre o respaldo em parâmetros auditáveis.

Sem uma cadeia de custódia robusta e adaptada às especificidades da prova digital produzida ou manipulada por inteligência artificial, apoiada em padrões internacionalmente reconhecidos, corre-se o risco concreto de que evidências cruciais sejam desconsideradas pelo Judiciário, comprometendo o processo penal e frustrando os objetivos de proteção previstos na Lei nº 15.123/2025. Esse cenário seria especialmente grave diante do caráter sofisticado da violência psicológica de gênero que a norma busca coibir.

A efetividade da Lei nº 15.123/2025 depende, portanto, não apenas de sua aplicação material, mas da construção de um sistema probatório robusto, sustentado em padrões técnicos auditáveis, que assegure a identificação, a preservação e a adequada valoração das evidências digitais complexas. Esse desafio impõe esforço coordenado de todos os atores do sistema de justiça e representa oportunidade estratégica para posicionar o Brasil na vanguarda do enfrentamento a crimes cometidos com uso de inteligência artificial.

Por fim, destaca-se que a proteção das vítimas de violência psicológica praticada por meio de inteligência artificial exige não apenas previsão normativa penal, mas igualmente garantias processuais consistentes, estruturadas sobre padrões técnicos verificáveis, capazes de assegurar a responsabilização efetiva dos agressores. A

construção desse sistema de garantias constitui responsabilidade coletiva, que ultrapassa fronteiras disciplinares e institucionais, demandando cooperação entre juristas, especialistas em tecnologia, formuladores de políticas públicas e sociedade civil, sempre orientada por fundamentos técnicos sólidos e auditáveis.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27037:2013: Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 13 ago. 2025.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 26 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 13 ago. 2025.

BRASIL. Lei nº 15.123, de 24 de abril de 2025. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena para o crime de violência psicológica contra a mulher cometido mediante uso de inteligência artificial. Diário Oficial da União, Brasília, DF, 25 abr. 2025a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm. Acesso em: 13 ago. 2025.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Quinta Turma. Agravo Regimental no Habeas Corpus nº 828.054/RN. Relator: Ministro Joel Ilan Paciornik. Julgado em: 23 abr. 2024. Diário da Justiça Eletrônico, 29 abr. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/02052024-Quinta-Turma-nao-aceita-como-provas-prints-de-celular-extraidos-sem-metodologia-adequada.aspx. Acesso em: 13 ago. 2025.

CHESNEY, Bobby; CITRON, Danielle K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, v. 107, n. 6, p. 1753-1819, 2019. DOI: 10.15779/Z38RV0D15J. Disponível em: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship. Acesso em: 13 ago. 2025.

COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY. C2PA Technical Specification. Version 2.2, 2024. Disponível em: https://spec.c2pa.org/specifications/specifications/2.2/specs/_attachments/C2PA_Specification.pdf. Acesso em: 13 ago. 2025.

CONTENT AUTHENTICITY INITIATIVE. CAI Technical Specification. Version 2.1. San Jose: Adobe, 2024. Disponível em: https://contentauthenticity.org/docs/. Acesso em: 13 ago. 2025.

COUNCIL OF EUROPE. Convention on Cybercrime. Budapest, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 13 ago. 2025.

COUNCIL OF EUROPE. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg, 12 mai. 2022. Disponível em: https://www.coe.int/en/web/cybercrime/second-additional-protocol. Acesso em: 13 ago. 2025.

EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 1689, 12 jul. 2024. CELEX: 32024R1689. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. Acesso em: 13 ago. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST IR 8387: Digital Evidence Preservation — Considerations for Evidence Handlers. Gaithersburg: NIST, 2022. DOI: 10.6028/NIST.IR.8387. Disponível em: https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers. Acesso em: 13 ago. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Forensics Tool Testing Program (CFTT). Gaithersburg: NIST, 2025. Disponível em: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt. Acesso em: 13 ago. 2025.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Best Practices for Digital Forensic Video Analysis. Version 1.1, 22 mar. 2024. Disponível em: https://www.swgde.org/wp-content/uploads/2024/04/2024-03-22-SWGDE-Best-Practices-for-Digital-Forensic-Video-Analysis-18-V-001-1.1.pdf. Acesso em: 13 ago. 2025.

VERDOLIVA, Luisa. Media Forensics and DeepFakes: An Overview. arXiv preprint, arXiv:2001.06564, 2020. DOI: 10.48550/arXiv.2001.06564. Disponível em: https://arxiv.org/abs/2001.06564. Acesso em: 13 ago. 2025.