IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

VIVIANNE RIGOLDI

JÉSSICA FACHIN

ROSANE TERESINHA PORTO

Copyright © 2026 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Educação Jurídica
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR
Prof. Dr. Rubens Beçak - USP - SP
Profa. Dra. Livia Gaigher Bosio Campello – UFMS – MS
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial
Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ
Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB
Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG
Prof. Dr. Rogério Borba - UNIFACVEST - SC

D598

Direito, governança e novas tecnologias V [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Vivianne Rigoldi; Jéssica Fachin; Rosane Teresinha Porto – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-589-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



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

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

Apresentação

O Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), referência na difusão de pesquisas que abordam os novos fenômenos envolvendo o Direito, firma-se como espaço qualificado para apresentação de pesquisas produzidas na área das novas tecnologias em face do Direito.

O tema, recorrente nos artigos apresentados - o uso da inteligência artificial no âmbito jurídico, demonstra que a maior sociedade científica na área jurídica do Brasil se mantém atenta às inovações tecnológicas, ao avanço de diversas tecnologias, novas experiências no judiciário e nos escritórios de advocacia. Artigos, de alta relevância acadêmica e científica, destacam que o Direito não está imune a essas transformações e reiteram a necessidade de atenção aos desafios regulatórios do uso da inteligência artificial no mundo jurídico.

Diferentes pesquisas, apresentadas no Grupo de Trabalho 'Direito, Governança e Novas Tecnologias V', alertam para os efeitos deletérios da opacidade algorítmica,

referindo-se à falta de transparência sobre como sistemas de inteligência artificial e seus algoritmos produzem decisões, dentro e fora do judiciário. Nos textos, a governança

digital é debatida, com rigorosa visão científica, objetivando garantir o uso estratégico de tecnologias de informação e comunicação para gerir serviços, promover a segurança

de dados e integrar processos, de forma transparente, eficiente, com foco na participação ativa do cidadão na tomada de decisões.

algorítmico e tecnológico do sistema de justiça, englobando a investigação de cibercrimes, a digitalização de procedimentos policiais e judiciais, provas digitais e a

regulação de plataformas para combater conteúdos ilícitos.

Destarte, os artigos apresentados e os debates produzidos no Grupo de Trabalho ‘Direito, Governança e Novas Tecnologias V’ são essenciais para o

fortalecimento das diretrizes nacionais de regulação das novas tecnologias, pela formação de parâmetros normativos e procedimentais adequados à proteção dos

direitos humanos e fundamentais, à garantia da segurança da informação, à gestão de riscos e ao fortalecimento da transparência e do alinhamento legal no uso das novas

tecnologias no âmbito jurídico.

Por essas razões, as coordenadoras do GT convidam para a leitura do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Vivianne Rigoldi/Jéssica Fachin/Rosane Porto

DEEPFAKES E PROTEÇÃO JURÍDICA DA PERSONALIDADE NA ERA DA INTELIGÊNCIA ARTIFICIAL GENERATIVA: PROVA DIGITAL, RESPONSABILIDADE E CONTROLE CIBERNÉTICO

DEEPFAKES AND THE LEGAL PROTECTION OF PERSONALITY IN THE AGE OF GENERATIVE ARTIFICIAL INTELLIGENCE: DIGITAL EVIDENCE, LIABILITY AND CYBERNETIC CONTROL

Stephanie Ferreira Vaz [1]
Emerson Wendt [2]

Resumo

O artigo analisa em que medida o ordenamento jurídico brasileiro dispõe de mecanismos normativos, probatórios e institucionais capazes de enfrentar as violações aos direitos da personalidade produzidas por deepfakes, especialmente contra a imagem, a intimidade e a identidade pessoal. Parte-se da hipótese de que os instrumentos atualmente disponíveis são relevantes, mas fragmentários, pois não respondem integralmente à natureza sistêmica, informacional e cibernética da manipulação algorítmica de rostos, vozes e comportamentos. A pesquisa adota abordagem qualitativa, de natureza teórico-documental, com método predominantemente dedutivo, revisão bibliográfica e análise documental de legislação, jurisprudência e direito comparado. O referencial teórico apoia-se na teoria cibernética de Norbert Wiener, articulada aos conceitos de hiper-realidade, pós-verdade e direitos da personalidade. O estudo demonstra que os deepfakes introduzem ruído nos fluxos comunicacionais, elevam a entropia informacional, comprometem a confiabilidade da prova audiovisual e ampliam os riscos de danos à honra, à intimidade e à identidade pessoal. Conclui-se que a tutela jurídica brasileira exige resposta coordenada em três eixos: aprimoramento normativo da regulação da inteligência artificial e da responsabilidade de plataformas; consolidação de critérios jurisprudenciais para prova digital e distribuição dinâmica do ônus probatório; e fortalecimento da infraestrutura de perícia forense digital, rastreabilidade e autenticação de conteúdos sintéticos.

Palavras-chave: Deepfakes, Direitos da personalidade, Prova digital, Inteligência artificial generativa, Responsabilidade das plataformas

Abstract/Resumen/Résumé

---

1 Graduanda em Direito pela Universidade La Salle Canoas-RS. E-mail: stephanie.202211501@unilasalle.edu.br. Lattes: http://lattes.cnpq.br/9993147985302041.

2 Doutor e Mestre em Direito (Unilasalle – Canoas/RS). Professor do PPGD e líder do GP Teorias Sociais do Direito. Delegado de Polícia Civil/RS. Lattes: http://lattes.cnpq.br/9475388941521093.

This article examines the extent to which the Brazilian legal system provides normative, evidentiary and institutional mechanisms capable of addressing violations of personality rights caused by deepfakes, especially violations of image, privacy and personal identity. It starts from the hypothesis that the currently available legal instruments are relevant but fragmented, since they do not fully respond to the systemic, informational and cybernetic nature of the algorithmic manipulation of faces, voices and behaviours. The research adopts a qualitative, theoretical-documentary approach, with a predominantly deductive method, bibliographic review and documentary analysis of legislation, case law and comparative law. The theoretical framework is grounded in Norbert Wiener's cybernetic theory, articulated with the concepts of hyperreality, post-truth and personality rights. The study demonstrates that deepfakes introduce noise into communicational flows, increase informational entropy, undermine the reliability of audiovisual evidence and intensify the risks of harm to honour, privacy and personal identity. It concludes that Brazilian legal protection requires a coordinated response along three axes: normative improvement of artificial intelligence regulation and platform liability; jurisprudential consolidation of criteria for digital evidence and dynamic allocation of the burden of proof; and strengthening of digital forensic infrastructure, traceability and authentication of synthetic content.

Keywords/Palabras-claves/Mots-clés: Deepfakes, Personality rights, Digital evidence, Generative artificial intelligence, Plataform liability

1 INTRODUÇÃO

A relação entre imagem e verdade fática constitui uma tensão permanente na história das sociedades modernas, tensão que se aprofunda exponencialmente com o advento da inteligência artificial generativa. Desde o surgimento da fotografia no século XIX, o registro visual assumiu função probatória e documental de grande relevância social e jurídica. Contudo, o desenvolvimento tecnológico recente representa uma ruptura qualitativa sem precedentes: a passagem da mera edição da realidade para a síntese de uma nova realidade, algoritmicamente fabricada e praticamente indistinguível do autêntico.

Essa transformação é evidenciada por dados alarmantes. Segundo projeções de empresas especializadas em cibersegurança, como DeepMedia[1] e Sensity AI[2], o volume de vídeos sintéticos saltou de aproximadamente 500 mil para 8 milhões entre 2024 e o biênio 2025/2026. No Brasil, o uso de inteligência artificial em conteúdos de desinformação triplicou em apenas um ano (Dantas, 2026), com o país concentrando cerca de 40% dos casos na América Latina.

Os *deepfake*s — mídias sintéticas produzidas por técnicas de aprendizado profundo capazes de simular rostos, vozes e comportamentos com elevado grau de realismo — constituem o epicentro dessa crise. Suas aplicações maliciosas abrangem desde a criação de pornografia não consensual e fraudes financeiras até a manipulação política e a difusão de desinformação eleitoral, gerando danos de difícil reparação à honra, à intimidade e à identidade de suas vítimas.

O presente artigo examina o seguinte problema de pesquisa: em que medida o ordenamento jurídico brasileiro dispõe de mecanismos normativos, probatórios e institucionais capazes de controlar, em termos cibernéticos, as perturbações informacionais produzidas por *deepfake*s contra os direitos da personalidade, especialmente a imagem, a intimidade e a identidade pessoal?

Parte-se da hipótese de que o ordenamento jurídico brasileiro dispõe de instrumentos fragmentários para a tutela dos direitos da personalidade diante dos *deepfake*s, mas ainda carece de uma arquitetura normativa, probatória e institucional capaz de responder à natureza sistêmica, informacional e cibernética da manipulação algorítmica da imagem, da voz e da identidade pessoal.

1 DeepMedia: https://deepmedia.ai. Acesso em: 10 abr. 2026.
2 Sensity AI: https://sensity.ai. Acesso em: 10 abr. 2026.

A pesquisa adota abordagem qualitativa, de natureza teórico-documental, com método predominantemente dedutivo. Utiliza procedimento bibliográfico, mediante revisão de literatura sobre *deepfake*s, direitos da personalidade, prova digital, hiper-realidade, pós-verdade e cibernética, e procedimento documental, por meio da análise de legislação, projetos legislativos, precedentes judiciais e atos regulatórios nacionais e estrangeiros. A análise jurídico-comparada contempla Estados Unidos, União Europeia, Reino Unido e China, selecionados pela diversidade de respostas regulatórias ao fenômeno: responsabilização civil, obrigações de transparência, criminalização setorial e marcação técnica de conteúdos sintéticos.

O trabalho está organizado em três seções. A primeira reconstrói a evolução da manipulação de imagens e os fundamentos técnicos da tecnologia *deepfake*. A segunda examina o arcabouço normativo brasileiro aplicável, analisando os regimes de responsabilidade civil, penal e dos provedores, bem como os desafios probatórios decorrentes da chamada "defesa *deepfake*". A terceira identifica as lacunas normativas existentes, traça um panorama do direito comparado e aponta caminhos para o aprimoramento da tutela jurídica no Brasil.

O marco teórico central do artigo apoia-se na teoria cibernética de Norbert Wiener (1970), especialmente na compreensão da sociedade como ambiente atravessado por processos de comunicação, controle e retroalimentação. Nessa perspectiva, os *deepfake*s não constituem apenas falsificações visuais, mas perturbações informacionais que introduzem ruído no sistema social, degradam a confiabilidade dos sinais audiovisuais e exigem mecanismos institucionais de feedback capazes de restaurar a distinção entre autenticidade e manipulação. A esse eixo articulam-se os conceitos de hiper-realidade, em Baudrillard (1994), e de pós-verdade, em Santaella (2020), que auxiliam a compreender os efeitos culturais da substituição do real por simulações persuasivas, bem como a teoria civil-constitucional dos direitos da personalidade, especialmente nas contribuições de Schreiber (2023) e Bittar (2015).

2 DA MANIPULAÇÃO ANALÓGICA À SÍNTESE ALGORÍTMICA: A GÊNESE DA CRISE DA AUTENTICIDADE

Esta seção estabelece o panorama tecnológico e histórico que fundamenta a análise jurídica desenvolvida nas seções seguintes. Inicialmente, reconstrói a trajetória da manipulação de imagens — da fotografia analógica à síntese algorítmica —, identificando as rupturas qualitativas que culminaram na tecnologia *deepfake*. Em seguida, examina os fundamentos técnicos dessa tecnologia e seus principais impactos sociais contemporâneos, com especial

atenção às modalidades de uso malicioso que desafiam o ordenamento jurídico brasileiro e a integridade do processo democrático.

2.1 Evolução histórica da manipulação de imagens

A história da manipulação de imagens antecede em muito o ambiente digital. Desde o surgimento da fotografia, a imagem técnica foi investida de um estatuto de verdade que, embora socialmente aceito, sempre conviveu com práticas de intervenção e alteração. Como observa Vilém Flusser, a fotografia não é uma mera reprodução do real, mas um produto de um aparelho que opera segundo programas e escolhas humanas, o que implica que toda imagem técnica já nasce mediada e interpretada (Flusser, 1985).

O uso político da manipulação imagética alcançou seu ápice durante os regimes totalitários do século XX. O caso soviético é paradigmático: opositores eram sistematicamente removidos de fotografias oficiais, reconfigurando a memória coletiva em favor do poder. Como documenta David King, figuras como Leon Trótski e Nikolai Iejov foram apagadas de registros históricos para reforçar a autoridade de Stalin (King, 2004). A manipulação visual convertia-se, assim, em instrumento de engenharia social e controle da narrativa histórica.

A transição para o ambiente digital, consolidada no final do século XX, representou uma ruptura paradigmática. Com a popularização de softwares como o Photoshop (lançado em 1990) e, posteriormente, de aplicativos acessíveis a qualquer usuário, a manipulação de imagens deixou de ser prática restrita a especialistas. Como observa Lev Manovich, o digital transformou a imagem em um objeto maleável, sujeito a intervenções ilimitadas (Manovich, 2001). A internet e as redes sociais aceleraram sua circulação em escala global, permitindo que conteúdos manipulados se disseminem em segundos, antes de qualquer verificação possível.

2.2 A tecnologia *deepfake*: fundamentos técnicos e impactos sociais

Os *deepfake*s representam o estágio mais sofisticado da manipulação digital contemporânea. O termo resulta da combinação de *deep learning* (aprendizado profundo) com *fake* (falso), indicando a utilização de modelos generativos capazes de sintetizar conteúdos audiovisuais com aparência de autenticidade. Esses modelos aprendem padrões faciais, vocais e corporais a partir de grandes bases de dados, reproduzindo expressões, movimentos e timbres com elevado grau de precisão (Goodfellow *et al.,* 2014).

Grande parte dos *deepfake*s é produzida por meio das Redes Adversariais Generativas (*Generative Adversarial Networks — GANs*), introduzidas por Ian Goodfellow em 2014. As GANs operam com dois modelos em constante competição: o gerador, responsável por criar imagens sintéticas, e o discriminador, encarregado de avaliar se essas imagens são reais ou falsas. Essa dinâmica adversarial aperfeiçoa continuamente ambos os modelos, até que o gerador seja capaz de produzir conteúdos praticamente indistinguíveis de registros autênticos (Goodfellow *et al.*, 2014).

Nos últimos anos, modelos de difusão ampliaram ainda mais o realismo dos *deepfake*s, incorporando nuances de iluminação, textura de pele, microexpressões e sincronização labial quase perfeita (Ramesh et al., 2022). A combinação de *deepfake*s com técnicas de *voice cloning* e *real-time rendering* inaugura um cenário em que a simulação pode ocorrer em tempo real, ampliando significativamente o potencial de dano (Kumar; Zhang, 2023).

A gravidade desse cenário é ilustrada por casos concretos. Em 2024, um funcionário de uma multinacional transferiu 25 milhões de dólares após participar de videoconferência com quem acreditava ser o diretor financeiro da empresa — o criminoso utilizou *deepfake* em tempo real para simular sua aparência e voz. No Brasil, em março de 2026, a Polícia Civil do Rio Grande do Sul instaurou inquérito para investigar *deepfake*s envolvendo alunas do Colégio de Aplicação da UFRGS (Oliveira; Trindade, 2026). Um levantamento nacional identificou 173 vítimas de *deepfake*s sexuais em ambientes escolares apenas em fevereiro de 2026 (Rodrigues, 2026).

Do ponto de vista epistemológico, esse desenvolvimento culmina no que Jean Baudrillard (1994) denomina hiper-realidade: um estágio em que a representação não apenas imita o real, mas o substitui, tornando-se mais convincente do que os próprios fatos. Como analisa Lucia Santaella (2020), vivemos em um ecossistema de pós-verdade no qual a crença subjetiva frequentemente se sobrepõe ao fato objetivo. A imagem, historicamente âncora da prova e da memória coletiva, converte-se em objeto permanente de suspeita.

Sob a perspectiva cibernética, esse fenômeno pode ser compreendido como uma elevação da entropia comunicacional. A circulação de *deepfake*s reduz a capacidade dos sistemas sociais de distinguir sinais autênticos de sinais fabricados, afetando os processos de confiança, decisão e atribuição de responsabilidade. Se, em Wiener (1970), comunicação e controle são dimensões indissociáveis dos sistemas complexos, a manipulação algorítmica da imagem e da voz indica uma falha no circuito de feedback entre produção, circulação, verificação e correção da informação. Daí a necessidade de que o Direito atue não apenas

repressivamente, após o dano, mas também como instância de estabilização normativa dos fluxos informacionais.

3 TUTELA JURÍDICA DOS DIREITOS DA PERSONALIDADE FRENTE AOS *DEEPFAKE*S

A expansão da tecnologia *deepfake* impõe ao ordenamento jurídico brasileiro um duplo desafio: o de tutelar efetivamente os direitos da personalidade violados pela síntese artificial de identidade e o de preservar a integridade probatória do processo diante da possibilidade de fabricação e contestação algorítmica de evidências digitais.

Esta seção analisa a resposta que o Direito brasileiro oferece a esse fenômeno, examinando, em sequência: os fundamentos constitucionais e civis da proteção da imagem, da intimidade e da identidade pessoal; os regimes de responsabilidade civil, penal e dos provedores de internet; e os desafios específicos impostos pela crise de autenticidade digital ao sistema processual.

3.1 Fundamentos constitucionais e civis

Os direitos da personalidade constituem prerrogativas essenciais à dignidade humana, assegurando proteção contra interferências indevidas na esfera existencial do indivíduo. No Brasil, encontram fundamento constitucional no art. 1º, III, que consagra a dignidade da pessoa humana como princípio estruturante do Estado Democrático de Direito, e no art. 5º, incisos V e X, que garantem a inviolabilidade da intimidade, vida privada, honra e imagem, assegurando indenização pelo dano decorrente de sua violação.

No plano infraconstitucional, o Código Civil de 2002 dedica os arts. 11 a 21 à tutela dos direitos da personalidade, disciplinando expressamente a proteção à imagem (art. 20) e à vida privada (art. 21). Para Carlos Alberto Bittar, esses direitos são "essenciais ao desenvolvimento da pessoa humana, irrenunciáveis, intransmissíveis e imprescritíveis" (Bittar, 2015, p. 14). Para Maria Helena Diniz, constituem o "núcleo mínimo de proteção da dignidade" (Diniz, 2018, p. 136).

Para além dos tradicionais direitos à imagem e à intimidade, os *deepfake*s agridem uma dimensão que merece atenção dogmática autônoma: o direito à identidade pessoal. A tecnologia é capaz de atribuir a outrem pensamentos, declarações e atos que jamais ocorreram, subvertendo a própria narrativa de vida do indivíduo. Anderson Schreiber (2023, p. 189) defende que a

identidade pessoal é uma projeção da dignidade que compreende o direito de cada pessoa a ser reconhecida segundo sua real história, seus valores e suas escolhas de vida. O dano provocado pelo *deepfake* configura o que se pode denominar falso testemunho visual: a criação de evidência sintética sobre a existência de alguém que não corresponde a nenhuma realidade vivida.

O arcabouço normativo aplicável inclui, além dos dispositivos constitucionais e civis:

- A Lei 13.718/2018, que criminaliza a divulgação de cena de sexo ou pornografia sem consentimento (art. 218-C do CP), diretamente aplicável a *deepfake*s pornográficos;

- A Lei 13.772/2018, que acrescenta ao art. 216-B do CP o crime de registro não autorizado da intimidade sexual, incluindo montagens digitais manipuladas; o art. 241-C do ECA, que criminaliza a montagem ou adulteração de imagem envolvendo crianças e adolescentes;

- O Marco Civil da Internet (Lei 12.965/2014), que disciplina a responsabilidade de provedores e os procedimentos de remoção de conteúdo;

- A Resolução TSE nº 23.732/2024, que proíbe *deepfake*s em campanhas eleitorais e exige rotulagem destacada para todo conteúdo produzido ou manipulado por IA; e,

- A Lei nº 15.123/2025, que acrescentou parágrafo único ao art. 147-B do Código Penal para majorar a pena do crime de violência psicológica contra a mulher quando cometido mediante uso de inteligência artificial ou recurso tecnológico que altere imagem ou som da vítima.

3.2 Responsabilidade civil, penal e dos provedores

A responsabilidade civil por *deepfake*s pode ser construída a partir de múltiplos vetores normativos complementares: violação da imagem (art. 5º, V e X, CF; art. 20, CC); dano moral e material (arts. 186 e 927, CC); violação da identidade pessoal como extensão da dignidade (art. 1º, III, CF; art. 12, CC); e divulgação não consentida de conteúdo íntimo (Lei 13.718/2018; art. 21, MCI).

A jurisprudência do Superior Tribunal de Justiça consolidou, por meio da Súmula 403 (Brasil, 2009), o entendimento de que "independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais", configurando o dano como presumido (*in re ipsa*). Esse entendimento é de fundamental importância para as vítimas de *deepfake*s, que frequentemente não conseguem quantificar ou

documentar todos os desdobramentos do dano sofrido. A violação da imagem pela síntese artificial é, em si, o fato gerador do dano - independentemente da demonstração de prejuízo concreto -, o que aproxima os *deepfake*s da hipótese consolidada na Súmula 403 e reforça o dever de reparação integral, incluindo danos morais, materiais e à identidade pessoal (Brasil 2009).

No campo penal, os *deepfake*s podem configurar tipos já existentes: calúnia, difamação e injúria (arts. 138-140, CP); falsidade ideológica (art. 299, CP); divulgação de cena de sexo sem consentimento (art. 218-C, CP); fraude eletrônica (art. 171, § 2º-A, CP); e crimes do ECA (art. 241-C). O principal desafio penal é a prova da autoria, dado que a cadeia de produção de *deepfake*s pode envolver ferramentas automatizadas, servidores em múltiplas jurisdições e perfis anônimos. A ausência de tipo penal específico para *deepfake*s de cunho reputacional, político e de fraude de identidade cria lacuna grave, pois a adequação típica analógica encontra limitações estruturais.

O Marco Civil da Internet (Lei 12.965/2014) estabelece um regime escalonado de responsabilidade para os provedores. A regra geral (art. 18) afasta a responsabilidade objetiva pelo conteúdo gerado por terceiros. O art. 19 prevê responsabilização após descumprimento de ordem judicial específica. O art. 21, porém, estabelece regime especial para conteúdo íntimo: o provedor responde subsidiariamente se não agir diligentemente após notificação da vítima, dispensando-se a ordem judicial. *Deepfake*s pornográficos enquadram-se nesse regime, permitindo à vítima acionar diretamente a plataforma para remoção imediata (Brasil, 2014). No julgamento do Tema 987 pelo Supremo Tribunal Federal (RE 1.037.396/SP, j. 26/06/2025), a Corte declarou a inconstitucionalidade parcial e progressiva do art. 19 do MCI, abrindo caminho para que as plataformas respondam por danos decorrentes de conteúdos manifestamente ilícitos mesmo sem ordem judicial específica (Brasil, 2025).

3.3 A crise probatória: a defesa *deepfake* e a cadeia de custódia

O fenômeno mais perturbador que os *deepfake*s introduzem no campo processual não é apenas a possibilidade de criar provas falsas, mas também o efeito inverso: a possibilidade de invalidar provas legítimas por meio da simples alegação de manipulação digital — estratégia denominada pela doutrina estrangeira de *deepfake defense.* O processo penal enfrenta, assim, dois riscos simultâneos: a condenação com base em *deepfake* apresentado como prova verdadeira; e a absolvição por insuficiência de prova, quando o acusado suscita, sem fundamento técnico, que evidência autêntica seria manipulada. Como alerta Guilherme Nucci,

"a dúvida razoável, pilar do *in dubio pro reo*, pode ser artificialmente gerada pela alegação infundada de manipulação digital" (Nucci, 2024, p. 421).

A resposta jurídica central a esse dilema é o instituto da cadeia de custódia, disciplinada nos arts. 158-A a 158-F do Código de Processo Penal, inseridos pelo Pacote Anticrime (Lei 13.964/2019). O art. 158-A define cadeia de custódia como o conjunto de procedimentos para manter e documentar a história cronológica do vestígio coletado, desde o local do fato até o laudo pericial. Para mídias digitais, isso implica: registro de *hash* criptográfico no momento da coleta; armazenamento em ambiente isolado e auditável; documentação de cada acesso ao material; e laudo pericial atestando a integridade do arquivo.

O STJ tem consolidado que é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova digitais por ele apresentadas. No AgRg no RHC 143.169/RJ (Brasil, 2023), a Corte estabeleceu que são inadmissíveis as provas digitais sem os registros documentais sobre os procedimentos adotados para a preservação de sua integridade, autenticidade e confiabilidade. No mesmo sentido, o AgRg no HC 828.054/RN (Brasil, 2024) assentou que a ausência de metodologia forense adequada na extração de dados de dispositivos digitais - incluindo a geração de código *hash* e a documentação auditável de cada etapa - resulta na inadmissibilidade da prova. A robustez da cadeia de custódia é, portanto, a principal defesa do sistema de justiça tanto contra a prova falsificada quanto contra a alegação infundada de manipulação digital.

O desafio prático, contudo, é que a perícia forense especializada em detecção de *deepfake*s ainda é escassa no Brasil. Renato Brasileiro Lima (2023, p. 784) aponta que a modernização da estrutura pericial é condição indispensável para a efetividade do processo penal na era digital. Enquanto essa infraestrutura não se consolida, o Judiciário permanece dependente de peritos de escassa disponibilidade e de ferramentas que a própria evolução tecnológica dos *deepfake*s supera progressivamente.

A cadeia de custódia pode ser compreendida, em chave cibernética (Wiener, 1970), como mecanismo institucional de *feedback* destinado a reduzir a entropia probatória. Ao registrar *hash* criptográfico, documentar acessos, preservar metadados e submeter o arquivo à perícia, o sistema de justiça cria um circuito de verificação que retroalimenta a decisão judicial com informações sobre autenticidade, integridade e confiabilidade. Sem esse circuito, a prova audiovisual fica exposta simultaneamente ao risco da falsificação e ao risco da contestação oportunista pela chamada defesa *deepfake*.

4 LACUNAS NORMATIVAS, DIREITO COMPARADO E CAMINHOS PARA O APRIMORAMENTO DA TUTELA

A análise do arcabouço normativo brasileiro, desenvolvida na seção anterior, permite identificar as insuficiências estruturais que persistem na tutela jurídica dos direitos da personalidade frente aos *deepfake*s.

Esta seção examina essas lacunas em perspectiva comparada e propõe caminhos para seu aprimoramento, organizando-se em três momentos: a identificação das principais lacunas normativas do ordenamento brasileiro; o exame do tratamento jurídico conferido ao tema pelas jurisdições selecionadas; e a formulação de eixos estratégicos para o aperfeiçoamento da tutela jurídica no Brasil.

4.1 Lacunas normativas no ordenamento brasileiro

O ordenamento jurídico brasileiro ainda carece de instrumentos normativos específicos para o enfrentamento abrangente dos *deepfake*s. As principais lacunas identificadas são: ausência de definição legal de *deepfake*, criando riscos de subinclusão e superinclusão; ausência de tipificação penal específica para *deepfake*s de cunho reputacional, político e de fraude de identidade fora de contexto sexual — o que o art. 147-B do CP, inserido em 2025, não supriu integralmente; ausência de protocolos forenses padronizados e investigativos nacionais para detecção, documentação e apresentação de *deepfake*s como evidência; e ausência de obrigações gerais de transparência algorítmica para plataformas, que identifiquem e rotulem conteúdo sintético independentemente de sua natureza.

A conexão entre *deepfake*s e a Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018) constitui um vetor normativo subutilizado. A imagem facial, a voz e outros atributos biométricos constituem dados pessoais sensíveis (art. 5º, II, c/c art. 11, LGPD), cujo tratamento sem consentimento é, em regra, vedado. A criação de um *deepfake* implica, necessariamente, o tratamento ilícito de tais dados, o que enseja a aplicação das sanções administrativas previstas no art. 52 da LGPD — multa de até 2% do faturamento da empresa, limitada a R$ 50 milhões por infração — independentemente da via civil ou penal (Brasil, 2017).

O Projeto de Lei nº 2.338/2023, Marco Legal da Inteligência Artificial[3] (Brasil, 2023), em tramitação no Congresso Nacional, representa a iniciativa mais abrangente para suprir essas lacunas. O PL propõe: obrigações de rotulagem visível de conteúdo sintético; responsabilidade civil objetiva dos provedores por conteúdo de IA não identificado; avaliação de impacto algorítmico para aplicações que utilizem síntese de identidade; e atribuição à ANPD de competência para fiscalizar o uso de dados pessoais na produção de *deepfake*s.

4.2 Panorama do direito comparado e a experiência europeia

A análise do direito comparado revela uma tendência global à regulação específica dos *deepfake*s. Nos Estados Unidos, o S.3696 — DEFIANCE Act of 2024, aprovado pelo Senado norte-americano e pendente de conclusão na Câmara[4] (Estados Unidos, 2024), criou causa de ação civil federal para vítimas de *deepfake*s sexuais não consentidos, com danos estatutários de até US$ 150.000 por violação. No âmbito estadual, Califórnia, Texas e Virgínia possuem leis específicas criminalizando *deepfake*s pornográficos e eleitorais. No Reino Unido, o *Online Safety Act 2023* foi emendado em 2024 para incluir a criminalização do compartilhamento de *deepfake*s íntimos sem consentimento, independentemente da intenção de causar dano.

A experiência mais estruturada, e que mais diretamente pode orientar o Brasil, é a europeia. O *AI Act* (Regulamento UE 2024/1689, de 13 de junho de 2024) impõe, em seu art. 50, obrigações de transparência para conteúdos gerados ou manipulados por IA, incluindo divulgação de *deepfake*s como artificialmente gerados ou manipulados, ou seja, de rotulagem visível e automática para todo conteúdo sintético gerado por IA, inclusive *deepfake*s, indicando claramente que o conteúdo foi gerado ou manipulado por inteligência artificial. A violação dessa obrigação sujeita o infrator a multas de até € 15 milhões ou 3% do faturamento global anual (União Europeia, 2024). A *Digital Services Act* (Regulamento UE 2022/2065) complementa esse regime, impondo às grandes plataformas obrigações de avaliação e mitigação de riscos sistêmicos associados à desinformação por conteúdo sintético (União Europeia, 2022).

A ausência de obrigação análoga ao art. 50 do *AI Act* no ordenamento brasileiro representa lacuna normativa crítica, pois permite que conteúdos sintéticos circulem sem

[3] O PL nº 2.338/2023 foi aprovado pelo Senado Federal e remetido à Câmara dos Deputados em 17 de março de 2025.

[4] Trâmite no Congresso Americano: https://www.congress.gov/bill/119th-congress/senate-bill/1837 (acesso em 10 maio 2026).

identificação, dificultando tanto a responsabilização de criadores quanto a proteção do público. A incorporação de regime equivalente no Marco Legal da IA brasileiro (PL 2.338/2023) é medida de harmonização regulatória urgente (Brasil, 2023). O Brasil, com sua tradição constitucional de tutela da dignidade humana e com os instrumentos normativos já existentes, tem as condições objetivas para avançar nessa direção.

4.3 Caminhos para o aprimoramento da tutela jurídica

Os caminhos para o aprimoramento da tutela jurídica convergem em três eixos complementares. No plano legislativo, são necessários: aprovação do PL 2.338/2023 com inclusão de obrigações de rotulagem e responsabilidade objetiva dos provedores; tipificação penal específica da criação e divulgação maliciosa de *deepfake*s, com agravantes para fins eleitorais, extorsivos e de violência de gênero digital; e definição técnico-jurídica de *deepfake* que permita segurança na aplicação dos tipos legais.

No plano jurisprudencial, a consolidação de precedentes que reconheçam a inversão do ônus da prova em situações de assimetria técnica entre criador de *deepfake* e vítima, bem como a aplicação extensiva do regime do art. 21 do Marco Civil da Internet a todas as modalidades de *deepfake* que envolvam síntese da identidade pessoal, representaria avanço significativo na proteção imediata dos afetados.

No plano institucional, o fortalecimento da capacidade pericial dos institutos de criminalística e dos laboratórios forenses digitais é condição *sine qua non* para a efetividade de qualquer resposta normativa. A adoção de padrões de certificação digital de conteúdo audiovisual — como os desenvolvidos pela *Coalition for Content Provenance and Authenticity* (C2PA) — e a implementação de programas de letramento midiático nas escolas completam o quadro de medidas necessárias para uma resposta socialmente efetiva ao fenômeno.

Rotulagem obrigatória, padrões de proveniência como C2PA, deveres de transparência algorítmica e fortalecimento pericial compõem uma arquitetura cibernética de controle da circulação de mídias sintéticas. Tais instrumentos não eliminam o risco dos *deepfake*s, mas introduzem feedback verificável no ecossistema informacional, permitindo que usuários, plataformas, órgãos públicos e tribunais identifiquem sinais manipulados, corrijam assimetrias informacionais e reduzam a propagação de conteúdos falsamente autênticos.

CONSIDERAÇÕES FINAIS

A presente pesquisa demonstrou que o ordenamento jurídico brasileiro dispõe de instrumentos relevantes para a tutela dos direitos da personalidade frente aos *deepfake*s — mas que esses instrumentos são estruturalmente insuficientes para enfrentar, com plenitude, a magnitude e a especificidade dos danos produzidos pela síntese de identidade por inteligência artificial generativa.

Três déficits estruturais comprometem a tutela efetiva. O primeiro é normativo: a ausência de definição legal de *deepfake*, de tipificação penal abrangente e de protocolos forenses padronizados cria zonas de impunidade que o esforço interpretativo não consegue suprir integralmente. O segundo é probatório: a crise de autenticidade gerada pelos *deepfake*s afeta simultaneamente a capacidade de usar mídias digitais como prova e a de desconstituí-las quando falsas, criando paradoxo que exige soluções técnicas e jurídicas combinadas. O terceiro é institucional: a infraestrutura de perícia forense digital no Brasil é insuficiente para a demanda atual e futura, comprometendo a resposta judicial a violações que dependem de análise técnica especializada.

A resposta a esses déficits exige atuação coordenada em três frentes. No plano legislativo, a aprovação do Marco Legal da IA com obrigações de rotulagem e responsabilidade objetiva dos provedores, inspirada no modelo do art. 50 do AI Act europeu, é medida urgente. No plano jurisprudencial, a consolidação dos precedentes do STJ sobre cadeia de custódia, dano presumido e inversão do ônus probatório deve ser aprofundada. No plano institucional, o investimento em capacitação pericial e em programas de letramento midiático é requisito de efetividade de qualquer resposta normativa.

Em última análise, os *deepfake*s revelam que a proteção jurídica da personalidade depende da capacidade do Direito de operar como sistema de controle normativo da entropia comunicacional. Na era da inteligência artificial generativa, preservar imagem, intimidade e identidade pessoal exige mais do que reparação posterior: exige circuitos institucionais de feedback, rastreabilidade, autenticação e responsabilização capazes de restaurar a confiança nos sinais que estruturam a comunicação social e a decisão jurídica.

REFERÊNCIAS

BAUDRILLARD, Jean. **Simulacra and Simulation**. Tradução de Sheila Faria Glaser. Ann Arbor: University of Michigan Press, 1994. Título original: Simulacres et Simulation (Paris: Galilée, 1981).

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 7. ed. São Paulo: Saraiva, 2015.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 maio 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 maio 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil. Brasília, DF, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Código Penal para tipificar os crimes de importunação sexual e de divulgação de cena de estupro ou de cena de sexo ou pornografia sem consentimento. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13718.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018**. Acrescenta o art. 216-B ao Decreto-Lei nº 2.848/1940. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13772.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Pacote Anticrime. Brasília, DF, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 10 maio 2026.

BRASIL. **Lei nº 15.123, de 24 de abril de 2025**. Acrescenta o art. 147-B ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar o crime de divulgação de conteúdo íntimo falso produzido por manipulação digital. Brasília, DF: Diário Oficial da

União, 27 mar. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15123.htm. Acesso em: 10 maio 2026.

BRASIL. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Senado Federal, Brasília, DF, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 10 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 403**. Independe de prova do prejuízo a indenização pela publicação não autoriza da de imagem de pessoa com fins econômicos ou comerciais. Brasília, DF: Superior Tribunal de Justiça, [2009]. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf. Acesso em: 10 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ**. PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. OPERAÇÃO OPEN DOORS. FURTO, ORGANIZAÇÃO CRIMINOSA E LAVAGEM DE DINHEIRO. [...]. Relator: Min. Ribeiro Dantas. Quinta Turma, 02 mar. 2023. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=176387491&tipo=3&nreg=202100573956&dt=20230302&formato=PDF&salvar=false. Acesso em: 10 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus nº 828.054/RN**. PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS. CAPTURA DE TELAS. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA DIGITAL. AGRAVO REGIMENTAL PROVIDO [...]. Rel. Min. Joel Ilan Paciornik. Quinta Turma, 29 abr. 2024. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:superior.tribunal.justica;turma.5:acordao;hc:2024-04-23;828054-2425050. Acesso em: 10 maio 2026.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.037.396/SP** (Tema 987). Rel. Min. Dias Toffoli. Tribunal Pleno, 30 jun. 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/RE1.037.396_SP.pdf Acesso em: 10 maio 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024**. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF: TSE, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 maio 2026.

BRASILEIRO, Renato Lima. **Manual de Processo Penal**. 9. ed. Salvador: JusPodivm, 2023.

DANTAS, Glenda. **Conteúdos falsos com IA triplicam e viram arma política no Brasil**. Salvador/BA: Desinformante, 6/02/2026. Disponível em: https://desinformante.com.br/conteudos-falsos-com-ia-triplicam-e-viram-arma-politica-no-brasil/. Acesso em: 15 mar. 2026.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: teoria geral do direito civil. 33. ed. São Paulo: Saraiva, 2018.

ESTADOS UNIDOS. Congresso. Senado. S.3696 — DEFIANCE Act of 2024 (Disrupt Explicit Forged Images and Non-Consensual Edits Act). 118th Congress. Washington, D.C., 2024. Disponível em: https://www.congress.gov/bill/118th-congress/senate-bill/3696. Acesso em: 10 maio 2026.

FLUSSER, Vilém. **Filosofia da Caixa Preta**: Ensaios para uma futura filosofia da fotografia. São Paulo: Hucitec, 1985.

GOODFELLOW, Ian et al. Generative Adversarial Nets. *In*: **ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS**, 27., 2014. Anais [...]. [S.l.]: NeurIPS, 2014. Disponível em: https://arxiv.org/abs/1406.2661. Acesso em: 10 maio 2026.

KING, David. **O comissário desaparece**: a falsificação de fotografias e de arte na Rússia de Stalin. São Paulo: Cosac & Naify, 2004.

KUMAR, Ranjeet; ZHANG, Wei. Real-time *deepfake*s: threats and countermeasures. IEEE **Transactions on Information Forensics and Security**, v. 18, p. 1423-1437, 2023. Disponível em: https://ieeexplore.ieee.org/document/10025544. Acesso em: 10 maio 2026.

MANOVICH, Lev. **The Language of New Media**. Cambridge: MIT Press, 2001.

NUCCI, Guilherme de Souza. **Código de Processo Penal Comentado**. 20. ed. Rio de Janeiro: Forense, 2024.

OLIVERIA, Pietro; TRINDADE, Pedro. Deepfake: Polícia apura suspeita de manipulação de imagens de alunas do Colégio de Aplicação da UFRGS. **G1**. 31 mar. 2026. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2026/03/31/deepfake-policia-apura-suspeita-de-manipulacao-de-imagens-de-alunas-do-colegio-de-aplicacao-da-ufrgs.ghtml. Acesso em: 10 maio, 2026.

RAMESH, Aditya et al. **Hierarchical Text-Conditional Image Generation with CLIP Latents**. arXiv, 2022. Disponível em: https://arxiv.org/abs/2204.06125. Acesso em: 10 mar. 2026.

REINO UNIDO. **Online Safety Act 2023**. Chapter 50. London: His Majesty's Stationery Office, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50/contents. Acesso em: 10 maio 2026.

RODRIGUES, Natália. Relatório aponta 173 vítimas de deepfakes sexuais em escolas brasileiras; crime também foi registrado em Pernambuco. 11 fev. 2026. **SaferNet Brasil**. Disponível em: https://cnf.net.br/2026/02/11/relatorio-aponta-173-vitimas-de-deepfakes-sexuais-em-escolas-brasileiras-crime-tambem-foi-registrado-em-pernambuco/. Acesso em: 10 maio 2026.

SANTAELLA, Lucia. A pós-verdade é verdadeira ou falsa? **TECCOGS**: Revista Digital de Tecnologias Cognitivas, São Paulo, n. 21, p. 16-30, jan./jun. 2020. Disponível em: https://revistas.pucsp.br/index.php/teccogs/article/view/48959. Acesso em: 10 maio 2026.

SCHREIBER, Anderson. **Direitos da Personalidade**. 5. ed. São Paulo: Atlas, 2023.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (Artificial Intelligence Act). **Jornal Oficial da União Europeia**, L, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689. Acesso em: 10 maio 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022 (Digital Services Act). **Jornal Oficial da União Europeia**, L 277, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022R2065. Acesso em: 10 maio 2026.

WIENER, Norbert. **Cibernética e sociedade**: o uso humano de seres humanos. São Paulo: Cultrix, 1970.