

A (IN)SEGURANÇA DA PROVA NA ERA DA INTELIGÊNCIA ARTIFICIAL: DESAFIOS À VERACIDADE PROBATÓRIA NA TUTELA DOS DIREITOS DA PERSONALIDADE DA CRIANÇA

THE (IN)SECURITY OF EVIDENCE IN THE ERA OF ARTIFICIAL INTELLIGENCE: CHALLENGES TO EVIDENTIARY VERACITY IN THE PROTECTION OF CHILDREN'S PERSONALITY RIGHTS

Marcelo Negri Soares¹
Valéria Silva Galdino Cardin²
Leticia Mayumi Almeida Takeshita³
Laura Leal Carvalho⁴

RESUMO: O presente artigo analisa os riscos que a inteligência artificial generativa representa para a veracidade probatória e para a efetividade da tutela dos direitos da personalidade da criança no ordenamento jurídico brasileiro. Parte-se da premissa de que a presunção relativa de veracidade historicamente atribuída à prova digital foi construída sobre pressupostos técnicos hoje superados pela sofisticação dos *deepfakes*, conteúdos sintéticos tecnicamente indistinguíveis do real. Metodologicamente, adotou-se abordagem qualitativa, jurídico-dogmática, com pesquisa bibliográfica e documental. Os resultados indicam dupla vulnerabilidade: de um lado, a legislação penal pressupõe vítima real fotografada, revelando vazio de tipicidade quanto ao CSAM sintético; de outro, a fragilidade pericial favorece tanto a incriminação indevida quanto o fenômeno do "dividendo do mentiroso", que desacredita provas autênticas. Conclui-se que se impõe arranjo normativo e institucional multinível, articulando regulação da inteligência artificial, tipificação penal autônoma, forense de mídia sintética e cooperação internacional, para assegurar a efetividade da Doutrina da Proteção Integral na era digital.

Palavras-chave: Inteligência artificial. Prova judicial. *Deepfake*. Direitos da personalidade. Proteção da criança.

¹ Orientador de Mestrado, Doutorado e Pós-Doutorado. Advogado e contabilista. Pesquisador ICETI, Next Seti e FAPESP. Editor da Springer Journal para E-Law, renomada revista europeia (2019). Editor da Revista Brasileira de Direito da Personalidade. Professor Visitante Coventry University (UK), no PPG em Direito, Administração e Negócios (2019). Professor Permanente do Programa de Mestrado e Doutorado em Direito UniCesumar, na linha Efetividade da Justiça e Direitos da Personalidade. Avaliador presencial de seminários SIAC/UFRJ (desde 2018). Professor da UEM - Universidade Estadual de Maringá.

² Pós-Doutora em Direito pela Universidade de Lisboa. Doutora e Mestre em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Docente da Universidade Estadual de Maringá (UEM) e no Doutorado e Mestrado do Programa de Pós-Graduação em Ciências Jurídicas do Centro Universitário de Maringá (UNICESUMAR). Pesquisadora pelo Instituto Cesumar de Ciência, tecnologia e Inovação (ICETI). Advogada no Paraná.

³ Doutoranda e Mestre em Direito Unicesumar.

⁴ Mestranda em Ciências Jurídicas pelo Centro de Ensino Superior de Maringá (Unicesumar), vinculada à linha de pesquisa sobre o Sistema Constitucional de Garantia dos Direitos da Personalidade. Possui especialização em Direito do Trabalho e Previdenciário pelo Centro Universitário Unifatecie e graduação em Direito pela Universidade Paranaense (UNIPAR). Atualmente, é advogada no escritório Rolanski Leal Advocacia e Consultoria Jurídica e atua como docente de Pós-Graduação no Centro Universitário Unifatecie. Integra o grupo de pesquisa coordenado pelo Dr. Marcelo Negri Soares, com foco em temas como Direitos da Personalidade, proteção de dados e os impactos da tecnologia nas relações jurídicas. Possui produção bibliográfica que inclui livros, capítulos e artigos em periódicos qualificados, além de experiência em orientações de iniciação científica e trabalhos de conclusão de curso, e participação em bancas examinadoras e eventos científicos.

ABSTRACT: This article analyzes the risks that generative artificial intelligence poses to evidentiary veracity and to the effective protection of children's personality rights in the Brazilian legal system. It starts from the premise that the relative presumption of veracity historically attributed to digital evidence rests on technical assumptions now overcome by the sophistication of deepfakes, synthetic content technically indistinguishable from reality. Adopting a qualitative, juridical-dogmatic methodology based on bibliographical and documentary research, the study reveals a twofold vulnerability: Brazilian criminal legislation presupposes a real photographed victim, creating a gap in typification regarding synthetically generated Child Sexual Abuse Material (CSAM); meanwhile, forensic fragility fosters both wrongful incrimination and the so-called "liar's dividend", whereby genuine evidence is discredited. It is concluded that a multi-level normative and institutional framework is required — combining AI regulation, autonomous criminal typification, synthetic media forensics and international cooperation — to ensure the effectiveness of the Doctrine of Integral Protection in the digital era.

Keywords: Artificial intelligence. Judicial evidence. Deepfake. Personality rights. Child protection.

INTRODUÇÃO

A prova constitui o eixo estrutural sobre o qual se assenta a legitimidade da função jurisdicional, na medida em que é por meio dela que o julgador reconstrói, dentro dos limites do possível, os fatos relevantes para a solução da controvérsia. Historicamente, a admissibilidade de documentos, imagens, áudios e vídeos digitais ampliou as possibilidades de demonstração da verdade dos fatos, conferindo maior acessibilidade e celeridade à instrução processual (DIDIER JR.; BRAGA; OLIVEIRA, 2020). Entretanto, o mesmo avanço tecnológico que multiplicou os meios de prova também engendrou um fenômeno de sentido inverso: a possibilidade de fabricação de evidências sintéticas tecnicamente indistinguíveis do real, mediante o emprego de sistemas de inteligência artificial (IA) generativa.

Nesse cenário, ganham centralidade os chamados *deepfakes* — conteúdos audiovisuais manipulados ou integralmente gerados por algoritmos de aprendizado profundo, capazes de reproduzir com verossimilhança perturbadora a voz, a imagem e os gestos de uma pessoa real. O problema transcende a mera curiosidade tecnológica: compromete a própria epistemologia da prova, colocando em xeque a presunção relativa de veracidade historicamente atribuída à prova digital (NIEVA-FENOLL, 2018). Como adverte a doutrina, a autenticidade documental, antes aferível por rastros técnicos relativamente estáveis, passa a depender de perícia forense cada vez mais sofisticada e onerosa, nem sempre disponível às partes hipossuficientes ou aos órgãos de persecução penal (AMERINI et al., 2025).

A questão adquire contornos ainda mais graves quando a pessoa exposta à manipulação sintética é uma criança. O ordenamento jurídico brasileiro, sob a influência da Doutrina da

Proteção Integral consagrada no art 227 da Constituição da República e no Estatuto da Criança e do Adolescente (ECA), reconhece a criança como sujeito de direitos dotado de proteção jurídica qualificada, em razão de sua peculiar condição de pessoa em desenvolvimento (BRASIL, 1988; BRASIL, 1990). Os direitos da personalidade — imagem, honra, intimidade, identidade e dignidade sexual — recebem, nesse contexto, tutela reforçada, cuja efetividade depende, em grande medida, da confiabilidade dos elementos probatórios levados a juízo.

Ocorre que a multiplicação de *deepfakes* sexuais infantis, popularmente identificados pela sigla CSAM (*Child Sexual Abuse Material*) quando gerados sinteticamente por IA, revela uma dupla insegurança: de um lado, a possibilidade de que crianças reais tenham sua imagem indevidamente utilizada para treinar modelos ou compor materiais sintéticos; de outro, a dificuldade de o sistema de justiça distinguir, para fins probatórios, o que é fabricado do que é autêntico, dificultando tanto a responsabilização de agressores quanto a defesa de pessoas falsamente incriminadas (FUZIGER; FERNANDES, 2025). Relatórios de organizações internacionais e nacionais apontam crescimento expressivo de denúncias de materiais de abuso gerados por inteligência artificial, evidenciando que o fenômeno já não é hipotético, mas empiricamente verificável (CONJUR, 2026).

Diante desse quadro, o presente artigo tem como problema de pesquisa a seguinte indagação: em que medida a inteligência artificial fragiliza a veracidade da prova no processo judicial brasileiro e quais os reflexos dessa fragilização sobre a efetividade da tutela dos direitos da personalidade da criança? Como hipótese, sustenta-se que a legislação processual e a legislação de proteção à infância, concebidas em contexto tecnológico anterior à IA generativa, revelam-se insuficientes para assegurar, de modo pleno, tanto a autenticidade probatória quanto a proteção da personalidade infantil, exigindo-se um arranjo normativo e institucional multinível, que combine regulação da IA, aprimoramento da cadeia de custódia digital e fortalecimento da Doutrina da Proteção Integral.

O objetivo geral do trabalho consiste em analisar os desafios impostos pela inteligência artificial à veracidade da prova judicial e seus impactos sobre a tutela dos direitos da personalidade da criança no ordenamento jurídico brasileiro. Como objetivos específicos, busca-se: (i) examinar o regime jurídico da prova digital e o papel da IA no sistema de justiça; (ii) investigar o fenômeno dos *deepfakes* e seus efeitos sobre a autenticidade probatória; (iii) analisar

o arcabouço normativo de proteção aos direitos da personalidade da criança; e (iv) propor caminhos normativos, técnicos e institucionais de mitigação dos riscos identificados.

A relevância do tema justifica-se, ainda, pela convergência entre duas agendas normalmente tratadas de forma apartada pela doutrina jurídica: de um lado, o direito processual e a teoria da prova, tradicionalmente concentrados em questões de admissibilidade, ônus probatório e valoração; de outro, o direito da criança e do adolescente, centrado na Doutrina da Proteção Integral e nos direitos da personalidade. A inteligência artificial generativa impõe a essas duas agendas um ponto de contato inescapável, na medida em que compromete simultaneamente a confiabilidade do instrumento processual (a prova) e a integridade do bem jurídico tutelado (a personalidade infantil), exigindo tratamento interdisciplinar que este artigo busca, na medida do possível, concluir.

Metodologicamente, adota-se abordagem qualitativa, de natureza jurídico-dogmática e exploratória, valendo-se de pesquisa bibliográfica e documental, com exame da doutrina processual civil e penal, da legislação de proteção à infância e à adolescência, da Lei Geral de Proteção de Dados Pessoais (LGPD) e de projetos legislativos em tramitação sobre a regulação da inteligência artificial, além de literatura técnica sobre forense digital. O artigo estrutura-se em cinco seções, além desta introdução e da conclusão: a primeira trata da prova e da inteligência artificial no processo judicial brasileiro; a segunda examina os *deepfakes* e a crise da autenticidade probatória; a terceira analisa os direitos da personalidade da criança; a quarta articula a insegurança probatória com os riscos à personalidade infantil; e a quinta apresenta propostas de mitigação normativa, técnica e institucional.

4

I Da inteligência artificial e da prova no processo judicial brasileiro

A prova, em sentido processual, pode ser compreendida como o conjunto de meios e atividades destinados a formar a convicção do julgador acerca da existência ou inexistência dos fatos relevantes para o litígio (CINTRA; GRINOVER; DINAMARCO, 2015). Trata-se de instrumento voltado não à demonstração de uma verdade absoluta e ontológica, inatingível pela razão humana, mas de uma verdade processualmente construída, sujeita a *standards* de convencimento e a regras de distribuição do ônus probatório (TARUFFO, 2016). Nesse sentido, Taruffo (2016) sublinha que a busca pela verdade no processo é uma "aproximação racional aos fatos", jamais uma reconstrução perfeita da realidade.

O Código de Processo Civil brasileiro, ao disciplinar o sistema de provas, consagra a livre apreciação motivada, segundo a qual o juiz aprecia a prova constante dos autos, indicando na decisão as razões da formação de seu convencimento (BRASIL, 2015). Tal sistema pressupõe, contudo, a integridade e a autenticidade dos elementos probatórios submetidos à apreciação judicial. A doutrina processualista reconhece que a prova digital — mensagens eletrônicas, registros de aplicativos de mensagens, fotografias e vídeos — passou a integrar rotineiramente a instrução processual, tanto na esfera cível quanto na criminal, beneficiando-se de presunção relativa de veracidade, que pode ser afastada por impugnação fundamentada da parte contrária (DIDIER JR.; BRAGA; OLIVEIRA, 2020).

Essa presunção relativa, todavia, foi historicamente construída sobre um pressuposto tecnológico que hoje se mostra frágil: o de que a falsificação de documentos digitais deixaria rastros técnicos detectáveis por perícia relativamente simples, como metadados inconsistentes ou artefatos de edição perceptíveis. A ascensão da inteligência artificial generativa rompe esse pressuposto, na medida em que passa a ser tecnicamente viável produzir conteúdo sintético de alta verossimilhança, sem os sinais de manipulação tradicionalmente empregados pela perícia documental (AMERINI et al., 2025). Como resultado, a distribuição do ônus da prova impugnativa — que tradicionalmente recaía sobre quem alegasse a falsidade — tende a se tornar cada vez mais onerosa e tecnicamente inviável para a parte hipossuficiente.

1.1 Da ascensão da inteligência artificial no sistema de justiça: avanços e riscos

O Poder Judiciário brasileiro tem incorporado ferramentas de inteligência artificial em diferentes graus de sofisticação, com o propósito declarado de conferir maior eficiência, celeridade e uniformidade à prestação jurisdicional. Exemplos notórios incluem o sistema Victor, do Supremo Tribunal Federal, voltado à triagem de processos com repercussão geral, e o projeto Sócrates, do Superior Tribunal de Justiça, destinado à elaboração de relatórios automatizados de processos. O Conselho Nacional de Justiça, por meio da Resolução nº 332/2020, estabeleceu diretrizes éticas para o uso de IA no Poder Judiciário, fixando como objetivos a promoção do bem-estar dos jurisdicionados e a prestação equitativa da jurisdição (CNJ, 2020).

Não obstante os ganhos de eficiência, a doutrina alerta para riscos relevantes associados à opacidade algorítmica e à reprodução de vieses discriminatórios nos sistemas de apoio à

decisão judicial. Nunes e Marques (2018), ao tratarem da necessidade de transparência algorítmica como garantia do devido processo constitucional, sustentam ser indispensável a "necessária possibilidade de oferta de clareza no iter que gerou a resposta" produzida pelo sistema. Tal exigência de rastreabilidade e auditabilidade humana da decisão algorítmica projeta-se, com ainda maior intensidade, sobre o uso da IA na produção e na análise de prova, pois, se a origem e o processamento dos dados que subsidiam a decisão judicial não forem passíveis de verificação, comprometem-se tanto a legitimidade da decisão quanto a segurança jurídica das partes.

Some-se a isso o episódio amplamente noticiado de decisão judicial fundamentada em precedentes inexistentes, produzidos por sistema de IA generativa e submetidos sem a devida checagem, o que ensejou a instauração de procedimento disciplinar pelo Conselho Nacional de Justiça (CONSULTOR JURÍDICO, 2023 apud REVISTA POLÍTICAS PÚBLICAS & CIDADES, 2024). O episódio ilustra, de forma paradigmática, o risco de contaminação da própria atividade jurisdicional pela chamada "alucinação" algorítmica, fenômeno em que sistemas de IA generativa produzem conteúdo plausível, mas factualmente incorreto ou inexistente. Se tal risco já se manifesta na elaboração de peças e decisões, ele se agrava exponencialmente no campo da prova, em que a IA pode ser empregada tanto para auxiliar sua análise quanto para fabricá-la deliberadamente.

6

Verifica-se, portanto, uma ambivalência estrutural: a mesma tecnologia que promete otimizar a gestão processual e ampliar o acesso à justiça é também instrumento apto a corroer a confiabilidade dos elementos que sustentam a própria decisão judicial. Essa ambivalência impõe ao sistema de justiça brasileiro o desafio de desenvolver, simultaneamente, capacidade técnica de detecção de fraudes probatórias e arcabouço normativo apto a disciplinar o uso responsável da IA, tema que será retomado na quinta seção deste trabalho.

1.2 Do contraditório sobre a prova produzida ou analisada por inteligência artificial

A incorporação de sistemas de inteligência artificial à instrução processual — seja como instrumento de análise de grandes volumes de dados, seja como ferramenta de apoio à perícia técnica — impõe releitura do princípio do contraditório, que deve ser compreendido não apenas como direito de manifestação sobre o conteúdo da prova, mas também como direito de conhecer e de impugnar o próprio método pelo qual a prova foi produzida ou analisada. Quando um laudo

pericial se vale de ferramenta de inteligência artificial para identificar padrões de manipulação em conteúdo audiovisual, é imprescindível que a metodologia empregada, os parâmetros de confiabilidade do sistema e a margem de erro estatística sejam disponibilizados às partes, sob pena de se criar uma "caixa-preta probatória" inacessível ao escrutínio processual.

Essa exigência de transparência metodológica dialoga diretamente com a garantia constitucional da ampla defesa e com o dever de motivação das decisões judiciais, na medida em que a mera invocação de um resultado algorítmico, desacompanhada da exposição do raciocínio técnico subjacente, não satisfaz o padrão de fundamentação exigido pelo devido processo legal. A doutrina que trata da transparência algorítmica no âmbito da própria decisão judicial (NUNES; MARQUES, 2018) aplica-se, por identidade de razões, à prova pericial informatizada, de modo que também os peritos judiciais que se valham de ferramentas de IA devem estar aptos a explicitar, em linguagem acessível, os fundamentos técnicos de suas conclusões, permitindo à parte contrária eventual contraprova ou perícia divergente.

A ausência de regulamentação específica sobre os requisitos mínimos de validação científica de ferramentas de IA empregadas em perícia judicial constitui lacuna relevante do direito probatório brasileiro, que poderia ser resolvida por resoluções do Conselho Nacional de Justiça ou por normas técnicas elaboradas em conjunto com os institutos de criminalística,

7

2 Das deepfakes e da crise da autenticidade probatória

O termo *deepfake* resulta da justaposição dos vocábulos "deep learning" e "fake", designando conteúdos audiovisuais sintéticos produzidos por redes neurais profundas, notadamente por meio de arquiteturas de redes adversariais generativas (GANs) e, mais recentemente, de modelos de difusão. Tais sistemas permitem substituir rostos, sincronizar movimentos labiais a áudios artificiais e clonar timbres de voz com grau de fidelidade que, para o observador leigo, é praticamente indistinguível da gravação autêntica (AMERINI et al., 2025). A literatura técnica costuma diferenciar subcategorias conforme o objeto manipulado: "deepvoice", quando a manipulação recai sobre o áudio; e "deepnude", quando o conteúdo

sintético envolve nudez ou conotação sexual, categoria de particular gravidade quando aplicada a menores de idade.

A dimensão jurídica do problema não é inteiramente nova: a manipulação da realidade por meio de testemunhos falsos, documentos forjados e provas fisicamente adulteradas sempre foi um risco inerente à atividade probatória. O que a inteligência artificial generativa acrescenta é a escala, a acessibilidade e o grau de sofisticação técnica da fraude, tornando-a exequível por qualquer pessoa com acesso a ferramentas de uso público, sem conhecimento técnico especializado (ROITMAN, 2026 apud LEXLEGAL, 2026). Essa democratização da capacidade de fraude documental é o elemento verdadeiramente disruptivo, pois desloca o problema da autenticidade de um cenário de risco excepcional para um cenário de risco sistêmico e cotidiano.

No plano civil, o art 11 do Código Civil brasileiro estabelece que os direitos da personalidade são intransmissíveis e irrenunciáveis, ao passo que o art 20 do mesmo diploma veda, a requerimento do interessado, a divulgação da imagem de pessoa quando atinja sua honra, boa fama ou respeitabilidade (BRASIL, 2002). A imagem e a voz, como emanções diretas da personalidade humana, gozam de proteção autônoma e fundamento constitucional, de modo que sua apropriação não autorizada para a criação de conteúdo sintético configura, em tese, violação a um direito da personalidade, independentemente da configuração de dano patrimonial, na esteira do entendimento consolidado na Súmula 403 do Superior Tribunal de Justiça (BRASIL. STJ, 2009).

8

Do ponto de vista técnico, convém ainda distinguir os *deepfakes* das demais formas de edição digital de imagem, historicamente já conhecidas pelo direito, como a montagem fotográfica tradicional ou a edição de vídeo por corte e colagem. Enquanto essas técnicas convencionais costumam deixar vestígios identificáveis por perícia relativamente simples — descontinuidades de iluminação, inconsistências de compressão, alterações abruptas de quadro —, os modelos de inteligência artificial generativa são treinados justamente para minimizar tais vestígios, otimizando o resultado final segundo métricas de verossimilhança perceptual. Esse traço técnico distintivo é o que confere ao fenômeno dos *deepfakes* um caráter qualitativamente novo, e não apenas uma variação quantitativa de um problema já conhecido pela perícia documental tradicional, circunstância que justifica o tratamento jurídico e pericial diferenciado.

2.1 Cadeia de custódia, perícia forense e ônus da prova

A cadeia de custódia digital — conjunto de procedimentos destinados a preservar a integridade e a rastreabilidade da prova desde sua obtenção até sua apresentação em juízo — foi expressamente disciplinada no processo penal brasileiro pela Lei nº 13.964/2019, conhecida como "Pacote Anticrime" (BRASIL, 2019). O regramento buscou assegurar que a prova digital, uma vez colhida, não sofresse alterações capazes de comprometer sua idoneidade probatória. Contudo, a disciplina legal foi concebida em contexto no qual a principal ameaça à integridade da prova era a manipulação posterior à sua coleta, e não a fabricação integral do conteúdo antes mesmo de sua apreensão, hipótese em que a cadeia de custódia, por mais rigorosa que seja em sua aplicação, é incapaz de atestar a autenticidade originária do material.

Diante desse cenário, a perícia técnica assume papel decisivo, e cada vez mais insubstituível, na aferição da autenticidade de conteúdos audiovisuais suspeitos de manipulação por IA. A autenticação de um arquivo de áudio ou vídeo deve envolver a análise de metadados, do espectro sonoro e de artefatos neurais residuais deixados pelos próprios modelos generativos, elementos que somente peritos com formação específica em forense digital são capazes de identificar (SOARES, 2025 apud DECISOR BRASIL, 2026). Ocorre que a perícia especializada em detecção de *deepfakes* ainda ocupa posição marginal na rotina probatória brasileira, em razão

9

do custo elevado, da escassez de profissionais qualificados e do desconhecimento, por parte de operadores do direito, sobre a formulação de quesitos técnicos adequados (ANÁLISE, 2026). Esse quadro produz um deslocamento silencioso, mas relevante, do ônus da prova. Embora o sistema processual brasileiro, em regra, atribua a quem alega a falsidade documental o encargo de demonstrá-la, a alta complexidade técnica das fraudes por IA pode justificar a mitigação desse ônus, autorizando o juiz a determinar, de ofício, a realização de perícia, sob pena de decidir com base em prova de idoneidade duvidosa (GALÍCIA EDUCAÇÃO, 2025). Trata-se de aplicação do poder instrutório do magistrado, orientado pelos princípios da busca da verdade possível e da cooperação processual, para reequilibrar uma disparidade técnica que, de outro modo, prejudicaria estruturalmente a parte sem recursos para custear perícia privada.

Na ausência de tipificação penal autônoma e específica para a generalidade das condutas envolvendo *deepfakes* no direito brasileiro, a responsabilização criminal tem se valido de tipos penais preexistentes, como os crimes contra a honra, a falsidade ideológica e o estelionato, este

último especialmente fortalecido, no que se refere à modalidade eletrônica, pela Lei nº 14.155/2021. Recentemente, a Lei nº 15.123/2025 alterou o artigo 147-B do Código Penal para estabelecer causa de aumento de pena no crime de violência psicológica contra a mulher quando praticado mediante uso de inteligência artificial ou de outro recurso tecnológico apto a alterar imagem ou som da vítima (BRASIL, 2025).

No campo cível, a responsabilização por danos decorrentes de *deepfakes* fundamenta-se na cláusula geral de proteção aos direitos da personalidade e na responsabilidade civil por ato ilícito, sendo dispensável, segundo a jurisprudência consolidada, a prova de prejuízo material para a configuração do dano decorrente do uso não autorizado de imagem com fins ofensivos (BRASIL. STJ, 2009). A doutrina pondera, contudo, que a análise não pode prescindir da distinção entre conteúdo satírico ou paródico, amparado pela liberdade de expressão, e conteúdo deliberadamente elaborado para induzir o observador médio a erro, cuja ilicitude é mais evidente (LEGALE EDUCACIONAL, 2025).

Um obstáculo adicional à responsabilização, tanto cível quanto penal, reside na identificação do autor do conteúdo sintético, sobretudo quando produzido por meio de ferramentas de código aberto executadas localmente, sem registro em servidores de terceiros. Quando há rastros em servidores estrangeiros, a cooperação jurídica internacional, usualmente processada por meio de tratados de assistência mútua (MLAT), tende a ser lenta, podendo se estender por meses ou anos, lapso temporal muitas vezes suficiente para a consolidação do dano à vítima (DEBATE JURÍDICO, 2026). Esse descompasso entre a velocidade de disseminação digital e o tempo da resposta jurisdicional constitui um dos principais gargalos da tutela dos direitos da personalidade na era da inteligência artificial.

2.2 Direito comparado: iniciativas regulatórias sobre deepfakes

O exame do direito comparado revela que diferentes ordenamentos jurídicos têm buscado respostas normativas específicas ao fenômeno dos *deepfakes*, ainda que de forma assistemática e heterogênea. Na Austrália, o Criminal Code Amendment (Deepfake Sexual Material) Act de 2024 tipificou de forma autônoma a criação e a distribuição de material sexual sintético não consentido, independentemente da existência de vítima fotografada em situação real, abordagem que se afasta do modelo brasileiro, ainda dependente da comprovação de manipulação de imagem preexistente (AUSTRALIAN GOVERNMENT, 2024). Trata-se de

solução legislativa que reconhece explicitamente a autonomia do bem jurídico tutelado — a dignidade sexual da pessoa retratada, real ou sinteticamente composta — em relação à técnica específica empregada na fabricação do conteúdo ilícito.

Na União Europeia, o Regulamento de Inteligência Artificial (AI Act) impõe obrigações de transparência a provedores de sistemas que gerem ou manipulem conteúdo de imagem, áudio ou vídeo que se assemelhe a pessoas, lugares ou eventos existentes, exigindo a rotulagem do conteúdo como artificialmente gerado ou manipulado, sob pena de sanções administrativas. Tal exigência de rotulagem, ainda ausente na legislação brasileira, poderia contribuir significativamente para a redução da assimetria informacional entre quem produz e quem recebe o conteúdo sintético, funcionando como mecanismo preventivo complementar à perícia forense a posteriori. A ausência de padronização internacional, contudo, permite que plataformas e desenvolvedores explorem lacunas regulatórias por meio da operação em jurisdições menos exigentes, o que reforça a necessidade de cooperação regulatória multilateral, tema retomado na quinta seção deste trabalho.

No que se refere especificamente à proteção da infância, verifica-se tendência internacional de ampliação do conceito legal de material de abuso sexual infantil para abranger expressamente o conteúdo sintético, independentemente da existência de vítima real identificável, orientação já adotada, com variações técnicas, em diplomas normativos de diversos países e recomendada por organismos internacionais dedicados à proteção da infância. O Brasil, ao manter a exigência de vítima real fotografada como elemento do tipo penal, permanece, nesse aspecto específico, em descompasso com a tendência regulatória internacional mais recente, o que reforça a urgência da revisão legislativa apontada por Fuziger e Fernandes (2025).

3 Os direitos da personalidade da criança no ordenamento jurídico brasileiro

A Constituição da República de 1988, em seu art 227, rompeu com o paradigma tutelar-repressivo anteriormente vigente, consagrando a Doutrina da Proteção Integral, segundo a qual é dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, os direitos à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade

e opressão (BRASIL, 1988). O Estatuto da Criança e do Adolescente, Lei nº 8.069/1990, regulamentou esse comando constitucional, estabelecendo em seu art 3º que a criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata a lei (BRASIL, 1990).

A Doutrina da Proteção Integral representa, nesse sentido, uma ruptura paradigmática em relação ao modelo anterior — identificado pela doutrina como "situação irregular" — que tratava a infância pobre ou em conflito com a lei como objeto de intervenção estatal, e não como sujeito de direitos (INSTITUTO ALANA, 2022). Sob a ótica civil-constitucional, Tepedino (2021) observa que a família contemporânea deve ser compreendida não como instituição previamente imposta por laços sanguíneos, mas como "comunidade instrumental ao pleno desenvolvimento da personalidade de seus integrantes", o que reforça a centralidade do desenvolvimento da personalidade como finalidade última da proteção jurídica conferida à infância.

O princípio do melhor interesse da criança, corolário da proteção integral e amplamente incorporado pela jurisprudência brasileira, exige que toda decisão administrativa ou judicial que afete a criança considere, prioritariamente, os efeitos da medida sobre seu desenvolvimento físico, psíquico e social. Trata-se de vetor hermenêutico que deve orientar, inclusive, a atividade probatória em processos que envolvam crianças, seja como vítimas, seja como partes ou testemunhas, impondo redobrada cautela na colheita, na análise e na valoração de provas capazes de expor sua imagem, sua intimidade ou sua identidade.

3.1 Direitos da personalidade: imagem, honra, intimidade e dignidade sexual

Os direitos da personalidade — categoria jurídica que abrange, entre outros, o direito à vida, à integridade física e psíquica, à honra, à imagem, à intimidade, à identidade e à dignidade sexual — são caracterizados pela intransmissibilidade, irrenunciabilidade e indisponibilidade relativa, nos termos do art 11 do Código Civil (BRASIL, 2002). Segundo Schreiber (2014), a tutela da personalidade humana no direito contemporâneo migra de uma lógica de rol taxativo de direitos nominados para uma cláusula geral de proteção, fundada na dignidade da pessoa humana, apta a alcançar novas formas de violação ainda não expressamente previstas em lei, como as decorrentes de tecnologias emergentes.

Quando a titular desses direitos é uma criança, a proteção assume contornos de especial reforço, na medida em que a pessoa em desenvolvimento não dispõe, em regra, de plena capacidade de discernimento para consentir com a exposição de sua imagem ou de sua intimidade, tampouco de instrumentos próprios para reagir a violações. Bodin de Moraes (2003) destaca que a dignidade da pessoa humana, fundamento maior da ordem constitucional, exige do sistema jurídico uma leitura civil-constitucional dos danos à pessoa, centrada na proteção da personalidade em suas múltiplas dimensões, e não apenas na reparação patrimonial. Essa leitura é especialmente relevante no caso da criança, cuja violação à imagem ou à dignidade sexual produz efeitos que transcendem o dano imediato, projetando-se sobre seu desenvolvimento psicossocial de longo prazo.

A dignidade sexual da criança recebe, no ordenamento brasileiro, proteção penal específica, notadamente por meio dos tipos previstos no Estatuto da Criança e do Adolescente relativos à produção, reprodução, venda e divulgação de material que retrate criança ou adolescente em cena de sexo explícito ou pornográfica, inclusive mediante adulteração ou montagem de fotografia ou vídeo (BRASIL, 1990). Trata-se de regime protetivo historicamente construído sobre a premissa de que a conduta ilícita pressupõe a existência de uma vítima real, cuja imagem tenha sido indevidamente utilizada — premissa que, como se examinará na seção seguinte, é diretamente desafiada pelo surgimento de conteúdos integralmente sintéticos, gerados por inteligência artificial sem que exista, necessariamente, uma criança real fotografada ou filmada na origem imediata do material.

3.2 Autonomia progressiva, consentimento e limites à exposição da imagem infantil

O reconhecimento da criança como sujeito de direitos não implica equipará-la, para todos os efeitos, ao adulto plenamente capaz, mas sim reconhecer-lhe autonomia progressiva, compatível com seu estágio de desenvolvimento, na condução dos aspectos existenciais de sua própria vida. O Código Civil brasileiro estabelece a incapacidade absoluta para os menores de dezesesseis anos e a incapacidade relativa entre dezesesseis e dezoito anos, regime que, transposto para o campo dos direitos da personalidade, impõe a necessidade de suprimento da vontade infantil pelos responsáveis legais no que se refere ao consentimento para a exposição de sua imagem, sem prejuízo do dever de considerar, na medida do possível, a opinião da própria criança, em atenção ao seu direito de participação (BRASIL, 2002; BRASIL, 1990).

Essa estrutura de consentimento por representação, adequada ao contexto de publicações pontuais em meios de comunicação tradicionais, revela-se insuficiente diante da prática contemporânea de exposição cotidiana e massiva da imagem infantil em redes sociais pelos próprios responsáveis legais, fenômeno conhecido como "sharenting". Tal prática, ainda que amparada no exercício do poder familiar, gera um acervo público e nem sempre removível de imagens infantis, que passa a constituir matéria-prima potencial para o treinamento de modelos de inteligência artificial generativa e para a fabricação de conteúdo sintético, inclusive de natureza sexual, sem que a criança, tampouco seus responsáveis, tenham qualquer controle sobre esse uso posterior e não autorizado.

A tensão entre o exercício do poder familiar — que inclui, em tese, a prerrogativa de decidir sobre a exposição da imagem do filho — e a proteção autônoma da personalidade em formação da criança sugere a necessidade de se repensar, *de lege ferenda*, os limites do consentimento parental em matéria de exposição digital de imagem infantil, especialmente diante dos riscos qualitativamente novos introduzidos pela inteligência artificial generativa. Trata-se de discussão que extrapola os limites deste artigo, mas que se impõe como agenda de pesquisa correlata, na medida em que a proteção da personalidade da criança contra *deepfakes* não pode prescindir de uma reflexão sobre a origem lícita, porém potencialmente arriscada, do próprio material fotográfico que alimenta, direta ou indiretamente, os sistemas de inteligência artificial.

4 A (in)segurança da prova e os riscos da inteligência artificial à personalidade infantil

A convergência entre os problemas examinados nas seções anteriores manifesta-se de forma mais aguda no fenômeno do chamado AI-Generated Child Sexual Abuse Material (CSAM sintético), definido como material de abuso sexual infantil produzido, total ou parcialmente, por sistemas de inteligência artificial generativa. Fuziger e Fernandes (2025) analisam esse fenômeno sob a perspectiva jurídico-penal, concluindo que os dispositivos legais atualmente existentes no Brasil são insuficientes para enfrentar o CSAM produzido de forma integralmente sintética, o que evidencia a necessidade de tipificação penal autônoma, de políticas de responsabilização das plataformas digitais e de fortalecimento da cooperação internacional.

Relatórios de organizações internacionais dedicadas à proteção da infância evidenciam a magnitude do problema: a entidade britânica Internet Watch Foundation registrou crescimento expressivo nas denúncias confirmadas de materiais gerados por inteligência artificial, ao passo que, no Brasil, a organização SaferNet identificou, em 2023, o maior volume de denúncias sobre imagens de abuso em dezoito anos de monitoramento, fenômeno atribuído em parte à disseminação de ferramentas de IA generativa de fácil acesso (CONJUR, 2026). O mesmo levantamento aponta a existência de extenso número de grupos em aplicativos de mensagens dedicados à disseminação desse tipo de conteúdo ilícito, o que revela a dimensão organizada e escalável da exploração sexual infantil mediada por tecnologia.

O núcleo do problema jurídico-penal reside no fato de que a legislação brasileira, ao criminalizar a simulação de participação de criança ou adolescente em cena pornográfica mediante adulteração de fotografia ou vídeo, pressupõe a existência de uma vítima real cuja imagem tenha sido manipulada (BRASIL, 1990). Quando o material é gerado de forma integralmente sintética — isto é, sem que exista uma criança real fotografada, mas apenas um "rosto composto" estatisticamente derivado do treinamento do modelo em milhares de imagens —, a subsunção típica torna-se juridicamente controvertida, gerando o que a doutrina identifica como um vazio de tipicidade a exigir intervenção legislativa (FUZIGER; FERNANDES, 2025). Esse vazio não é meramente acadêmico: repercute diretamente sobre a persecução penal e sobre a própria dinâmica probatória, uma vez que a autoridade policial e o Ministério Público precisam, muitas vezes, demonstrar a existência de uma vítima identificável para viabilizar a ação penal, tarefa tecnicamente inviável quando o material é puramente sintético.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, qualifica os dados biométricos como dados pessoais sensíveis, sujeitos a regime de tratamento reforçado, e estabelece, em seus art 14 e seguintes, regras específicas para o tratamento de dados de crianças e adolescentes, exigindo, como regra geral, o consentimento específico e em destaque de ao menos um dos pais ou do responsável legal (BRASIL, 2018). Ocorre que a imagem facial e a voz, elementos centrais para o treinamento de modelos de IA generativa capazes de produzir *deepfakes*, constituem dados pessoais na medida em que identificam seu titular, de modo que a coleta massiva e não consentida de fotografias e vídeos de crianças disponíveis publicamente em redes sociais, para fins de treinamento de modelos, configura, em tese, tratamento irregular de dados sensíveis.

A doutrina especializada, contudo, aponta uma limitação estrutural da LGPD diante do fenômeno dos *deepfakes*: a lei foi concebida para regular o tratamento de dados identificáveis de uma pessoa determinada, ao passo que os conteúdos sintéticos frequentemente resultam da combinação estatística de dados de múltiplas pessoas, dificultando a identificação de um titular específico cujos direitos tenham sido diretamente violados. Essa limitação compromete a efetividade dos instrumentos de tutela previstos na LGPD para a hipótese específica de *deepfakes* sexuais envolvendo crianças, que causam danos individuais profundos — como violação da intimidade e da dignidade sexual — além de danos de natureza coletiva, ao normalizar práticas de violência digital contra a infância. A ausência de normas claras sobre a responsabilização civil e criminal nesse contexto dificulta tanto a reparação das vítimas quanto a prevenção de novos casos.

Some-se a isso a circunstância de que a própria arquitetura da LGPD, centrada no consentimento como fundamento legitimador do tratamento de dados, revela-se pouco eficaz diante de crianças, sujeitos incapazes, por definição, de prestar consentimento juridicamente válido, e cuja proteção depende da atuação diligente dos responsáveis legais e das próprias plataformas digitais, muitas vezes localizadas em jurisdições estrangeiras e submetidas a regimes regulatórios distintos. O quadro revela a insuficiência de um modelo regulatório fragmentado — LGPD, Marco Civil da Internet, ECA e legislação penal — que não dialoga organicamente com as especificidades técnicas da inteligência artificial generativa aplicada à infância.

4.1 A prova em juízo nos casos de exploração e abuso infantil mediados por inteligência artificial

No plano estritamente processual, a insegurança da prova produzida por inteligência artificial repercute nos casos envolvendo exploração e abuso infantil de duas formas antagônicas e igualmente preocupantes. De um lado, a facilidade de fabricação de conteúdo sintético abre a possibilidade de que pessoas inocentes sejam falsamente incriminadas mediante a apresentação, por terceiros mal-intencionados, de vídeos ou áudios manipulados que as associem a condutas criminosas contra crianças, hipótese em que a fragilidade da perícia forense disponível pode comprometer o devido processo legal e a presunção de inocência. De outro lado, e de modo simetricamente grave, a mesma fragilidade pericial pode ser explorada pela defesa de agressores

reais, que passam a alegar, de forma genérica e muitas vezes infundada, que a prova audiovisual autêntica de sua conduta seria, na realidade, uma fabricação por inteligência artificial — fenômeno identificado na literatura internacional como "dividendo do mentiroso" (*liar's dividend*), em que a mera possibilidade de manipulação sintética passa a ser instrumentalizada para desacreditar provas genuínas.

Esse duplo risco impõe ao juiz, ao Ministério Público e aos órgãos de perícia oficial redobrada cautela metodológica na análise de provas audiovisuais em processos envolvendo crianças, especialmente naqueles relativos a crimes sexuais, em que a prova é frequentemente a própria imagem ou gravação da vítima. A ausência de padronização técnica para a perícia de detecção de *deepfakes*, aliada à escassez de peritos qualificados fora dos grandes centros urbanos, cria um cenário de desigualdade territorial no acesso à justiça, em que a efetividade da tutela da personalidade infantil passa a depender, em última análise, da disponibilidade local de recursos periciais especializados (ANÁLISE, 2026).

Adicionalmente, cumpre destacar que a exposição repetida da criança à produção de depoimentos, à realização de perícias e à submissão de imagens a exames técnicos, ainda que necessários à instrução processual, deve observar o princípio da intervenção mínima e as técnicas de escuta especializada previstas na Lei nº 13.431/2017 (Sistema de Garantia de Direitos da Criança e do Adolescente Vítima ou Testemunha de Violência), de modo a evitar a revitimização. A incorporação de perícias sobre autenticidade de conteúdo por IA a esse arcabouço protetivo exige, portanto, não apenas competência técnica em forense digital, mas também sensibilidade quanto aos direitos processuais e à integridade psicológica da criança envolvida, sob pena de a busca pela verdade probatória converter-se, ela própria, em fonte adicional de violação de direitos.

Para melhor compreender a dimensão prática dos riscos examinados, é útil considerar duas situações hipotéticas, construídas a partir da sistematização da literatura consultada, que ilustram a ambivalência do problema. Na primeira hipótese, uma criança é vítima de *deepfake* sexual criado a partir de fotografias legitimamente publicadas por seus responsáveis em redes sociais, sem qualquer conotação sexual original. A produção do conteúdo sintético, embora não envolva captura de imagem real em contexto de abuso, gera dano à dignidade e à honra da criança comparável, em muitos aspectos, ao do abuso tradicional, ao mesmo tempo em que desafia a subsunção típica da legislação vigente, por inexistir, a rigor, "adulteração" de fotografia ou vídeo em cena efetivamente pornográfica

preexistente, mas sim criação integralmente nova a partir de dados de treinamento diversos (FUZIGER; FERNANDES, 2025).

Na segunda hipótese, um adulto produz e distribui material genuíno de abuso sexual contra criança, mas, ao ser confrontado judicialmente, alega que o conteúdo seria produto de manipulação por inteligência artificial, buscando instaurar dúvida razoável sobre a autenticidade da prova e, por consequência, obter a absolvição ou o trancamento da ação penal. Nesse cenário, a ausência de perícia forense especializada disponível tempestivamente pode conduzir a decisões judiciais equivocadas, seja pela condenação baseada em prova posteriormente questionável, seja pela absolvição de agressor real amparada em dúvida técnica insuficientemente esclarecida. As duas hipóteses, extremas em sentidos opostos, evidenciam que a "insegurança da prova" mencionada no título deste artigo não é unidirecional: ela ameaça, a um só tempo, a proteção da criança vítima de conteúdo sintético e a correta responsabilização do agressor de abuso real, exigindo do sistema de justiça capacidade técnica para distinguir, com o máximo rigor possível, cada uma dessas situações.

5 Caminhos para a mitigação: propostas normativas, técnicas e institucionais

Tramita no Congresso Nacional o Projeto de Lei nº 2.338/2023, que estabelece normas gerais de caráter nacional para o desenvolvimento, a implementação e o uso responsável de sistemas de inteligência artificial no Brasil, adotando abordagem regulatória baseada em risco, inspirada, em larga medida, no modelo europeu (BRASIL, 2023). O projeto prevê categorias de sistemas de "alto risco", entre os quais se incluem, potencialmente, sistemas empregados em contextos de administração da justiça e de proteção de grupos vulneráveis, sujeitando-os a obrigações reforçadas de transparência, avaliação de impacto algorítmico e supervisão humana. A aprovação de marco regulatório dessa natureza representa passo relevante para a construção de um regime de responsabilização proporcional aos riscos de sistemas de IA aplicados à produção e à análise de prova.

Paralelamente à regulação geral da IA, observa-se movimento legislativo pontual voltado a hipóteses específicas de dano, a exemplo da já mencionada Lei nº 15.123/2025, que agravou a pena do crime de violência psicológica contra a mulher quando praticado mediante uso de inteligência artificial (BRASIL, 2025). Tramitam ainda no Senado Federal projetos de lei destinados a tipificar autonomamente o crime de conteúdo sexual manipulado por inteligência

artificial, inclusive em contextos eleitorais, bem como propostas voltadas à proteção de crianças e adolescentes em ambientes digitais. A multiplicação de iniciativas legislativas pontuais, conquanto positiva do ponto de vista simbólico e reativo, revela a ausência de uma política legislativa coordenada, que articule a regulação geral da IA com a proteção específica da infância no ambiente digital, risco que a doutrina especializada recomenda evitar mediante a criação de tipo penal autônomo para o CSAM sintético, independentemente da identificação de vítima real (FUZIGER; FERNANDES, 2025).

Nesse contexto, defende-se que a regulação da inteligência artificial no Brasil deveria prever, de forma expressa, o dever de responsabilização das plataformas digitais e dos desenvolvedores de modelos generativos pela implementação de mecanismos técnicos de prevenção à produção de conteúdo sexual envolvendo crianças, a exemplo de filtros de conteúdo, sistemas de verificação etária e cooperação ativa com autoridades de persecução penal, em linha com experiências regulatórias estrangeiras que já preveem sanções específicas para conteúdo sexual sintético não consentido, inclusive envolvendo menores (AUSTRALIAN GOVERNMENT, 2024).

Ao lado da regulação de comando e controle, mostra-se recomendável que o marco legal da inteligência artificial incorpore instrumentos de regulação responsiva, como códigos de conduta setoriais, selos de conformidade e mecanismos de autorregulação regulada, que permitam ajuste mais célere às constantes transformações técnicas do setor, sem prejuízo da fiscalização estatal. A experiência regulatória em proteção de dados pessoais, consolidada a partir da LGPD e da atuação da Autoridade Nacional de Proteção de Dados, oferece parâmetro institucional relevante para a estruturação de autoridade ou núcleo técnico especializado em supervisão de sistemas de inteligência artificial de alto risco, com competência específica para a fiscalização de sistemas que envolvam, direta ou indiretamente, dados e imagens de crianças e adolescentes.

5.2 Governança, compliance e cooperação internacional na proteção da infância

A efetividade da tutela dos direitos da personalidade da criança na era da inteligência artificial depende, por fim, da articulação entre instrumentos normativos, técnicos e institucionais em escala nacional e internacional. No plano institucional, recomenda-se o fortalecimento de protocolos de governança de dados voltados à proteção de crianças, com a

incorporação da avaliação de impacto algorítmico centrada na infância às políticas de compliance de empresas de tecnologia que operam plataformas com potencial exposição de menores, na linha do que já vem sendo adotado por parte do setor privado em resposta a pressões regulatórias internacionais.

No plano da cooperação internacional, a natureza transnacional da disseminação de CSAM sintético exige o aprimoramento dos mecanismos de assistência jurídica mútua, de modo a reduzir o tempo de resposta das autoridades brasileiras diante de conteúdo hospedado em servidores estrangeiros. Organismos como a Europol e a Interpol já classificam a ciberpedofilia potencializada por tecnologia de *deepfake* como ameaça criminal emergente, de combate prioritário, o que reforça a necessidade de o Brasil intensificar sua participação em redes internacionais de cooperação policial e judicial dedicadas ao enfrentamento da exploração sexual infantil digital (FUZIGER; FERNANDES, 2025).

Por fim, a dimensão educativa não pode ser negligenciada: a capacitação de magistrados, membros do Ministério Público, defensores públicos e delegados de polícia para a compreensão técnica mínima dos riscos e das limitações da inteligência artificial aplicada à prova constitui pressuposto para que as garantias processuais e materiais examinadas ao longo deste artigo sejam efetivamente observadas na prática judiciária cotidiana. Sem essa alfabetização técnico-jurídica, corre-se o risco de que operadores do direito, por desconhecimento, atribuam confiabilidade excessiva a provas sintéticas ou, em sentido oposto, descartem provas autênticas sob suspeita infundada de manipulação, comprometendo, em ambos os casos, a justa composição do litígio e a proteção efetiva da criança.

A articulação entre esses três planos — regulação normativa, capacidade técnica pericial e cooperação institucional — não deve ser compreendida como sequência cronológica de reformas isoladas, mas como sistema integrado e retroalimentado, em que o aprimoramento de um dos eixos potencializa a efetividade dos demais. A tipificação penal autônoma do CSAM sintético, por exemplo, somente produzirá efeitos práticos consistentes se acompanhada de perícia forense capaz de identificar, com segurança técnica suficiente, a natureza sintética do material apreendido; do mesmo modo, a notariação digital de provas de nada valerá se o arcabouço legal não reconhecer expressamente sua força probatória. É nessa perspectiva sistêmica, e não fragmentada, que devem ser lidas as propostas apresentadas nesta seção, como contribuição para um debate legislativo, técnico e institucional ainda em construção no Brasil.

CONCLUSÃO

O presente artigo teve como propósito investigar em que medida a inteligência artificial fragiliza a veracidade da prova no processo judicial brasileiro e quais os reflexos dessa fragilização sobre a tutela dos direitos da personalidade da criança. A análise desenvolvida ao longo das seções permite confirmar a hipótese inicialmente formulada: a legislação processual e a legislação de proteção à infância, concebidas em contexto tecnológico anterior à consolidação da inteligência artificial generativa, mostram-se estruturalmente insuficientes para assegurar, de modo pleno, tanto a autenticidade da prova quanto a proteção da personalidade infantil.

Verificou-se, na primeira e na segunda seções, que a presunção relativa de veracidade historicamente atribuída à prova digital foi construída sobre pressupostos técnicos hoje superados pela sofisticação dos *deepfakes*, o que impõe a reconstrução dos parâmetros de distribuição do ônus probatório e o fortalecimento da perícia forense especializada em mídia sintética, ainda incipiente no Brasil. Na terceira seção, evidenciou-se que a Doutrina da Proteção Integral confere à criança um regime jurídico de proteção reforçada da personalidade, cuja efetividade prática, contudo, depende da confiabilidade dos instrumentos probatórios disponíveis ao sistema de justiça.

A quarta seção demonstrou que a convergência entre a insegurança probatória e a vulnerabilidade da infância atinge seu ponto mais crítico no fenômeno do CSAM sintético, em que a legislação penal brasileira, ao pressupor a existência de vítima real fotografada ou filmada, revela lacuna de tipicidade diante de conteúdos integralmente gerados por inteligência artificial, e em que a arquitetura da LGPD, centrada no consentimento, mostra-se estruturalmente inadequada para proteger sujeitos incapazes de consentir. Constatou-se, ainda, o risco simetricamente perigoso do chamado "dividendo do mentiroso", pelo qual a mera possibilidade técnica de fabricação sintética pode ser instrumentalizada para desacreditar provas autênticas de abuso infantil.

Por fim, a quinta seção indicou caminhos possíveis de mitigação, que perpassam a aprovação de um marco regulatório geral para a inteligência artificial atento aos riscos específicos à infância, a tipificação penal autônoma do CSAM sintético, o investimento em notariação digital e em forense de mídia sintética, e o fortalecimento da cooperação internacional e da capacitação técnica dos operadores do direito. Nenhuma dessas medidas,

isoladamente, é suficiente; sua efetividade depende de articulação sistêmica entre regulação, tecnologia e instituições de justiça.

Conclui-se, portanto, que a tutela dos direitos da personalidade da criança na era da inteligência artificial não pode prescindir de um redesenho da própria epistemologia da prova judicial, capaz de reconhecer que a veracidade processual, antes assentada em presunções relativamente estáveis, tornou-se um bem jurídico ele próprio ameaçado, e que, como tal, demanda proteção jurídica específica. Recomenda-se, como agenda de pesquisa futura, o aprofundamento empírico sobre a efetividade da perícia forense de mídia sintética nos tribunais brasileiros, bem como o exame comparado de experiências estrangeiras de regulação penal do CSAM sintético, de modo a subsidiar o aperfeiçoamento contínuo do arcabouço normativo nacional de proteção à infância diante dos desafios impostos pela inteligência artificial.

Cumprе reconhecer, por fim, as limitações inerentes a um estudo de natureza eminentemente bibliográfica e dogmática, que não se propôs a examinar empiricamente decisões judiciais brasileiras envolvendo *deepfakes* ou CSAM sintético, tampouco a mensurar quantitativamente a incidência do fenômeno nos tribunais pátrios, tarefa que demandaria pesquisa jurimétrica específica, atualmente dificultada pela ausência de padronização classificatória desses casos nos sistemas de gestão processual. Não obstante essa limitação metodológica, entende-se que a sistematização doutrinária e normativa aqui empreendida oferece base conceitual sólida para investigações empíricas futuras, bem como subsídio imediato para a atuação de operadores do direito diante de casos concretos que, com crescente frequência, colocarão à prova a capacidade do sistema de justiça brasileiro de conciliar inovação tecnológica e proteção efetiva da infância.

REFERÊNCIAS

AMERINI, I. et al. Deepfake media forensics: status and future challenges. PMC, v. 11, n. 3, p. 73, 28 fev. 2025. Disponível em: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11943306/>. Acesso em: 22 maio 2026.

ANÁLISE. Quando a IA vira prova: deepfakes e o colapso da autenticidade documental. 2026. Disponível em: <https://analise.com/noticias/quando-a-ia-vira-prova-deepfakes-e-o-colapso-da-autenticidade-documental>. Acesso em: 14 ago. 2026.

AUSTRALIAN GOVERNMENT. Criminal Code Amendment (Deepfake Sexual Material) Act 2024. Canberra: Australian Government, 2024.

BODIN DE MORAES, Maria Celina. Danos à pessoa humana: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 16 jul. 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015.

BRASIL. Lei nº 13.431, de 4 de abril de 2017. Estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência. Diário Oficial da União, Brasília, DF, 5 abr. 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal (Pacote Anticrime). Diário Oficial da União, Brasília, DF, 24 dez. 2019.

BRASIL. Congresso Nacional. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da inteligência artificial. Brasília, DF, 2023.

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). Diário Oficial da União, Brasília, DF, 25 abr. 2025.

BRASIL. Superior Tribunal de Justiça. Súmula nº 403. Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais. Brasília, DF: STJ, 2009.

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. Teoria geral do processo. 31. ed. São Paulo: Malheiros, 2015.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Resolução nº 332, de 21 de agosto de 2020. Dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2020.

CONSULTOR JURÍDICO (CONJUR). Brasil tem vazão legal para punir pornografia infantil sintética. 2026. Disponível em: <https://www.conjur.com.br/2026-jul-18/brasil-tem-vazio-legal-para-punir-pornografia-infantil-produzida-por-ia/>. Acesso em: 14 ago. 2026.

DEBATE JURÍDICO. Deepfakes e o Direito brasileiro. 2026. Disponível em: <https://debatejuridico.com.br/deepfakes-e-o-direito-brasileiro/>. Acesso em: 14 ago. 2026.

DECISOR BRASIL. Deepfakes na Justiça do Trabalho: como a IA desafia a autenticidade das provas digitais. 2026. Disponível em: <https://www.decisorbrasil.com.br/deepfakes-provas-digitais-e-inteligencia-artificial-novos-desafios-na-producao-da-prova-trabalhista/>. Acesso em: 14 ago. 2026.

DIDIER JR., Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael. Curso de direito processual civil: teoria da prova, direito probatório, decisão, precedente, coisa julgada e tutela provisória. v. 2. 15. ed. Salvador: Juspodivm, 2020.

FUZIGER, Rodrigo; FERNANDES, Lis Vitória de Almeida. Ciberpedofilia e inteligência artificial: perspectivas jurídico-penais da pornografia infantil sintética. Revista CNJ, Brasília, 2025. Disponível em: <https://www.cnj.jus.br/ojs/revista-cnj/article/view/979>. Acesso em: 22 maio 2026.

GALÍCIA EDUCAÇÃO. Provas digitais e deepfakes: desafios da autenticidade jurídica. 2025. Disponível em: <https://www.galiciaeducacao.com.br/blog/provas-digitais-e-deepfakes-desafios-da-autenticidade-juridica/>. Acesso em: 14 ago. 2026.

INSTITUTO ALANA. Proteção integral. 2022. Disponível em: <https://alana.org.br/glossario/protecao-integral/>. Acesso em: 14 ago. 2026. 24

LEGALE EDUCACIONAL. Deepfakes no Direito: responsabilidade e prova digital. 2025. Disponível em: <https://legale.com.br/blog/deepfakes-no-direito-responsabilidade-e-prova-digital/>. Acesso em: 14 ago. 2026.

LEXLEGAL. Deepfakes em provas judiciais: estamos prontos para a manipulação de evidências digitais? 2026. Disponível em: <https://lexlegal.com.br/deepfakes-em-provas-judiciais-estamos-preparados-para-a-manipulacao-de-evidencias-digitais/>. Acesso em: 14 ago. 2026.

NIEVA-FENOLL, Jordi. Inteligencia artificial y proceso judicial. Madrid: Marcial Pons, 2018.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: entre a promoção do acesso à justiça e os riscos à igualdade e à segurança jurídica. Revista Eletrônica de Direito Processual, Rio de Janeiro, 2018.

REVISTA POLÍTICAS PÚBLICAS & CIDADES. Provas no processo judicial e a ameaça de conteúdos gerados por IA. 2024. Disponível em: <https://journalppc.com/RPPC/article/view/2178>. Acesso em: 14 ago. 2026.

SCHREIBER, Anderson. Direitos da personalidade. 3. ed. São Paulo: Atlas, 2014.

SOARES, Igor. Ameaça invisível: detectando deepfakes de áudio em processos trabalhistas. ISP Forense, 15 maio 2025.

TARUFFO, Michele. Uma simples verdade: o juiz e a construção dos fatos. Trad. Vitor de Paula Ramos. São Paulo: Marcial Pons, 2016.

TEPEDINO, Gustavo. Temas de direito civil. 5. ed. Rio de Janeiro: Renovar, 2021.