ReGeo
ISSN: 2177-3246

DEEPFAKES E DIREITOS DA PERSONALIDADE: PROTEÇÃO JURÍDICA DA VOZ NA ERA DA INTELIGÊNCIA ARTIFICIAL GENERATIVA

DEEPFAKES AND PERSONALITY RIGHTS: LEGAL PROTECTION OF VOICE IN THE ERA OF GENERATIVE ARTIFICIAL INTELLIGENCE

DEEPFAKES Y DERECHOS DE LA PERSONALIDAD: PROTECCIÓN JURÍDICA DE LA VOZ EN LA ERA DE LA INTELIGENCIA ARTIFICIAL GENERATIVA

https://doi.org/10.56238/revgeov17n8-107

Data de submissão: 09/07/2026 **Data de publicação:** 09/08/2026

Antonio Felipe Pereira de Souza
Doutorando em Direito Constitucional
Instituição: Universidade de Fortaleza (Unifor)
E-mail: afelipeps@gmail.com
Orcid: https://orcid.org/0009-0002-4147-2744
Lattes: http://lattes.cnpq.br/7968186761509083

Danelle Tamborini Lopes
Doutoranda em Direito Constitucional
Instituição: Universidade de Fortaleza (Unifor)
E-mail: d_tamborini@hotmail.com
Orcid: https://orcid.org/0000-0003-0626-2506
Lattes: http://lattes.cnpq.br/5250924725186161

Paulo Andre Nobre Palmeira
Doutorando em Direito Constitucional
Instituição: Universidade de Fortaleza (Unifor)
E-mail: paulo.nobre.palmeira20@gmail.com
Orcid: https://orcid.org/0009-0007-4298-5943
Lattes: http://lattes.cnpq.br/0399848442653894

RESUMO
O artigo analisa os limites jurídicos do uso não consentido da imagem e da voz em deepfakes, à luz dos direitos da personalidade, da proteção de dados pessoais e da responsabilidade civil. Parte-se da premissa de que a inteligência artificial generativa ampliou a capacidade de reprodução sintética da identidade humana, potencializando riscos de desinformação, exploração econômica indevida, danos morais e violação da autodeterminação informativa. O problema de pesquisa consiste em verificar se os instrumentos jurídicos atualmente disponíveis no ordenamento brasileiro são suficientes para proteger a vítima diante desse tipo de lesão. A pesquisa adota abordagem qualitativa, de natureza bibliográfica e dogmático-jurídica, com método dedutivo. Conclui-se que os mecanismos tradicionais de tutela permanecem aplicáveis, mas se mostram insuficientes de forma isolada, exigindo interpretação sistemática e atualização da proteção jurídica da personalidade no contexto digital.

Palavras-chave: Deepfakes. Direitos da Personalidade. Imagem. Voz. Responsabilidade Civil.

ABSTRACT
This article examines the legal limits of the non-consensual use of image and voice in deepfakes, in light of personality rights, personal data protection, and civil liability. It starts from the premise that generative artificial intelligence has expanded the capacity for the synthetic reproduction of human identity, increasing the risks of disinformation, improper economic exploitation, moral damages, and violations of informational self-determination. The research problem is to determine whether the legal instruments currently available in the Brazilian legal system are sufficient to protect victims against this type of harm. The study adopts a qualitative approach, based on bibliographic and legal-dogmatic research, using the deductive method. It concludes that traditional protective mechanisms remain applicable, but are insufficient when considered in isolation, thus requiring a systematic interpretation and an updated legal protection of personality rights in the digital context.

Keywords: Deepfakes. Personality Rights. Image. Voice. Civil Liability.

RESUMEN
El artículo analiza los límites jurídicos del uso no consentido de la imagen y de la voz en deepfakes, a la luz de los derechos de la personalidad, de la protección de datos personales y de la responsabilidad civil. Se parte de la premisa de que la inteligencia artificial generativa amplió la capacidad de reproducción sintética de la identidad humana, potencializando riesgos de desinformación, explotación económica indebida, daños morales y violación de la autodeterminación informativa. El problema de investigación consiste en verificar si los instrumentos jurídicos actualmente disponibles en el ordenamiento brasileño son suficientes para proteger a la víctima ante este tipo de lesión. La investigación adopta enfoque cualitativo, de naturaleza bibliográfica y dogmático-jurídica, con método deductivo. Se concluye que los mecanismos tradicionales de tutela permanecen aplicables, pero se muestran insuficientes de forma aislada, exigiendo interpretación sistemática y actualización de la protección jurídica de la personalidad en el contexto digital.

Palabras clave: Deepfakes. Derechos de la Personalidad. Imagen. Voz. Responsabilidad Civil.

1 INTRODUÇÃO

O avanço da inteligência artificial generativa transformou profundamente a produção e circulação de conteúdos digitais, permitindo a criação de imagens, vídeos e áudios sintéticos com alto grau de realismo. Nesse cenário, os chamados *deepfakes* passaram a representar uma das manifestações mais sensíveis da tecnologia, pois tornam possível reproduzir, alterar ou simular traços da identidade de uma pessoa como seu rosto, sua voz e sua performance expressiva sem que haja participação ou autorização do titular.

Embora tais ferramentas possam ser empregadas para fins criativos, educacionais e até humorísticos, sua utilização também potencializa formas graves de lesão à esfera jurídica individual, sobretudo quando a manipulação é realizada de maneira enganosa, ofensiva, comercial ou difamatória.A imagem e a voz, nesse contexto, deixam de ser apenas elementos de identificação e passam a constituir matéria-prima para a fabricação de representações sintéticas capazes de circular com aparência de autenticidade.

Esse fenômeno intensifica os riscos de apropriação indevida da identidade, exploração econômica sem autorização, exposição vexatória, desinformação e danos morais de difícil reversão. Em outras palavras, a inteligência artificial não apenas reproduz conteúdos, mas pode reconstruir a presença digital de alguém de modo artificial, deslocando o debate jurídico da simples falsidade documental para a tutela da própria personalidade no espaço informacional.

Sob a perspectiva do Direito, o problema torna-se mais complexo porque os instrumentos tradicionais de proteção foram concebidos em um contexto tecnológico distinto, no qual a captação, a reprodução e a difusão da imagem ou da voz exigiam maior intervenção humana, maior custo de produção e menor capacidade de desenvolvimento. Com os *deepfakes*, a manipulação pode ser realizada com relativa facilidade, em larga escala, com rapidez de disseminação e com alto potencial de permanência nas redes.

Além disso, o conteúdo sintético pode ser produzido a partir de dados publicamente disponíveis como fragmentos de fala, fotografias ou de vídeos legítimos, o que gera conflitos entre consentimento, proteção de dados, uso informacional da imagem e responsabilidade pelos danos causados. Assim, emerge a seguinte pergunta de pesquisa: os instrumentos jurídicos atualmente disponíveis no ordenamento são suficientes para proteger a imagem e a voz contra o uso não consentido em *deepfakes*, ou a especificidade dessa tecnologia exige uma releitura dos direitos da personalidade e dos mecanismos de responsabilização civil?

A hipótese que orienta o presente estudo traz mecanismos tradicionais de tutela da imagem, da voz, da privacidade, dos dados pessoais e da responsabilidade civil que permanecem juridicamente

aplicáveis aos *deepfakes*, mas se mostram, isoladamente, insuficientes para enfrentar de modo satisfatório os danos produzidos por essa tecnologia.

Isso ocorre devido a facilidade de criação, multiplicação de agentes envolvidos, circulação transnacional do conteúdo e dificuldade de identificação imediata do ilícito, que enfraquecem a eficácia dos modelos tradicionais de prevenção e reparação. Diante disso, o objetivo geral do artigo é analisar os limites jurídicos para o uso não consentido da imagem e da voz em *deepfakes*, verificando se os direitos da personalidade e a responsabilidade civil oferecem tutela adequada à vítima no contexto da inteligência artificial generativa.

Para alcançar esse propósito, o estudo se desenvolve a partir de três objetivos específicos: primeiro, examinar o conceito de *deepfake* e seus impactos sobre a imagem, a voz e a identidade pessoal; segundo, identificar de que forma os direitos da personalidade, a proteção de dados e a responsabilidade civil podem ser mobilizados para a proteção da vítima; terceiro, avaliar as insuficiências do regime jurídico atual e indicar parâmetros interpretativos capazes de fortalecer a tutela diante do uso ilícito de conteúdos sintéticos.

No plano metodológico, a pesquisa adota abordagem qualitativa, de natureza bibliográfica e dogmático-jurídica, com emprego do método dedutivo. Parte-se do exame de fontes recente sobre *deepfakes*, direitos da personalidade, privacidade, proteção de dados e responsabilidade civil, bem como de estudos que discutem o papel do consentimento e da identidade digital no contexto da inteligência artificial generativa.

Ao final, pretende-se demonstrar que a resposta jurídica aos *deepfakes* não depende necessariamente da criação imediata de uma categoria totalmente inédita, mas exige, ao menos, uma releitura sistemática dos direitos da personalidade à luz da inteligência artificial generativa e de seus efeitos sobre a autonomia, a identidade e a dignidade da pessoa humana.

2 DEEPFAKES E A VIOLAÇÃO DA IDENTIDADE PESSOAL

Os deepefakes, apesar de ser um termo muito usado na era atual, possui significado e contexto histórico abrangente, porém sua utilização para fins ilícitos trouxe um grande debate jurídico quanto a proteção dos indivíduos pelo ordenamento jurídico e a responsabilidação dos agente causadores.

2.1 CONCEITO E CARACTERÍSTICAS DOS DEEPFAKES

O surgimento da Inteligência Artificial não foi acompanhado, de forma imediata, por sua regulamentação, seja no plano internacional, no âmbito nacional. Essa defasagem entre inovação tecnológica e produção normativa não é exclusiva da IA, mas característica recorrente do

desenvolvimento tecnológico, tendo em vista que a elaboração de marcos regulatórios exige tempo de maturação institucional e jurídica. Além disso, tais normas devem ser construídas em conformidade com os princípios e objetivos fundamentais da República, previstos na Constituição Federal. (Barrea et. al. 2023)

Nesse contexto, os deepfakes apresentam relação direta com a Inteligência Artificial, uma vez que sua criação depende de modelos computacionais capazes de simular, manipular ou reproduzir imagens, vozes e vídeos com elevado grau de verossimilhança. A compreensão desse fenômeno exige, portanto, retomar o próprio desenvolvimento histórico da IA.

E pensar que a IA surgiu de uma simples pergunta que o Alan Turing fez em 1950 na qual o autor propôs substituir a pergunta "as máquinas podem pensar"? (Turing, 1950, p.

433) por uma análise operacional sobre a capacidade de uma máquina imitar respostas humanas, conhecida como "jogo da imitação" ou Teste Turing.

Apesar da ideia de Turing marcar o início da busca do homem em criar "máquinas pensantes", foi em 1955 com John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon apresentaram a expressão *artificial intelligence* na proposta do *Dartmouth Summer Research Project on Artificial Intelligence*, marcando o surgimento da IA. Nas Décadas de 60 e 70 a IA passou por um novo avanço significativo que marcando o chamado *machine learning* (ML) (Tavares 2024).

Na década de 80 o investimento em IA passou por um forte declínio chamado de "inverno IA", só então, a partir da década de 90 os investimentos em IA aumentaram significativamente em razão dos grandes avanços tecnológicos marcando o início da Primavera da IA (Castro, et. al. 2021). Os *deepfakes* surgiram no ano de 2017 unindo os conceitos de aprendizado profundo de inteligência artificial – IA (*deep learning)* e falsificação (*fake*) para a propagação de conteúdo pornográfico (Tavares 2024).

Makraki (2024) define *deepfakes* como a criação de conteúdo sintético ou manipulado, produzido com o auxílio de sistemas de inteligência artificial e técnicas de aprendizado profundo, apto a fazer parecer autêntica uma imagem, um vídeo ou um áudio em que determinada pessoa aparece dizendo ou fazendo algo que, na realidade, não disse nem fez.

Benabou (2026) destaca a definição dada pelo AI Act promulgado pela União Europeia que conceitua *deepfakes* como conteúdos de imagem, áudio ou vídeo gerados ou manipulados por inteligência artificial, que se assemelham a pessoas, objetos, lugares, entidades ou eventos existentes e que, para um observador, podem parecer autênticos ou verídicos, no entanto apesar da conceituação a União Europeia não considerou os *deepfakes* como ilícitos em si mesmos.

Apesar da falta de harmonização na definição do que seriam os *deepfakes*, pode-se entender como uso da inteligência artificial para criar conteúdos digitais "falsos" utilizando imagens ou vozes verdadeiras retratando eventos que não aconteceram com intuito de convencer um terceiro sobre a veracidade de determinado evento.

Como se observa, os *deepfakes* criam a ilusão de espontaneidade, naturalidade e coerência expressiva, diferentemente das manipulações tradicionais, que em regra exigiam maior intervenção humana visível e frequentemente deixavam rastros perceptíveis, o resultado do *deepfake* não é apenas uma "imagem falsa", mas uma performance sintética da pessoa, construída a partir de fragmentos reais reorganizados por sistemas automatizados.

Apesar do uso indiscriminado dos *deepfakes* para propagação de atos ilegais e/ou imorais, Bosher (2026) elenca algumas formas em que os *deepfakes* foram utilizadas de forma benigna como:

> "For example, artist Randy Travis was able to release new music for the first time since suffering a stroke using deepfake technology that cloned his own voice, and a Malaria No More campaign used deepfake videos of celebrity David Beckham appealing to the public in nine different languages, enabling the charity to increase accessibility of their message to a wider audience" (Bosher (2026, p.2).

Makraki, (2024) aponta ao menos, quatro modalidades principais de *deepfakes* que podem recair sobre a imagem, vídeo, áudio ou de texto. Para os fins deste artigo, interessam, sobretudo os três primeiros, pois são eles que incidem diretamente sobre a imagem e a voz, objetos centrais da tutela da personalidade.

2.2 O USO DA IMAGEM E DA VOZ COMO ELEMENTOS DA PERSONALIDADE E OS RISCOS JURÍDICOS

No direito brasileiro, a Constituição Federal de 1988 confere tutela expressa a bens jurídicos imateriais ao estabelecer, no artigo 5º, inciso X que são invioláveis a imagem, a honra, a intimidade e a vida privada das pessoas assegurando reparação pelo dano material ou moral decorrente de sua violação.

Além disso, o artigo 5º, inciso XXVIII, alínea "a", também protege a reprodução da imagem e da voz humana, o que assume especial relevância diante do uso de ferramentas de inteligência artificial generativa capazes de simular, manipular ou reproduzir artificialmente a aparência e a fala de indivíduos sem o devido consentimento.

No plano infraconstitucional, o Código Civil, reforça essa proteção ao disciplinar em seu artigo 20, direitos da personalidade e ao vedar, em determinadas hipóteses, a exposição, utilização ou

publicação não autorizada da imagem da pessoa, especialmente quando houver atingimento de sua honra, boa fama ou exploração econômica indevida.

Ainda que a voz nem sempre apareça autonomamente destacada no texto legal, a doutrina recente sobre *deepfakes* a trata como atributo identificador diretamente ligado à identidade pessoal e à autodeterminação sobre a própria representação (Bosher, 2026; Olasiyan; Olasiyan, 2026). Assim, a relevância da imagem e da voz, nesse contexto, não decorre apenas de seu valor econômico eventual, mas sobretudo de seu papel como sinais de reconhecimento social.

Quando um sistema de inteligência artificial reproduz artificialmente o rosto, a entonação, o timbre ou os modos expressivos de alguém, não está apenas manipulando dados dispersos. Todavia, está recriando uma forma de manifestação pessoal irreal suscetível de ser confundida com a manifestação autêntica do sujeito. Essa manipulação ilegal de dados podem trazer resultados de engano público e a disputa pelo controle e pela exploração das novas "características sintéticas" derivadas da imagem e da voz humanas (Benabou, 2026).

Bosher (2026), ao discutir *deepfakes*, réplicas digitais e gêmeos digitais humanos, sustenta que a imagem e a voz passaram a ser replicadas em um ambiente técnico que favorece usos não autorizados, reaproveitamento constante e circulação ampliada. Pois, diferente de uma fotografia isolada ou de uma gravação específica, os *deepfakes* permitem a criação de novos conteúdos a partir de sinais pretéritos da pessoa, reconfigurando-os em situações jamais vividas. A ofensa, nesse caso, não está apenas no uso indevido de um registro preexistente, mas na fabricação de uma nova manifestação atribuída artificialmente ao indivíduo.

Esse ponto ajuda a compreender por que o consentimento assume posição central no tema, pois ele não possui função apenas de autorização patrimonial para uso de imagem ou voz, mas como expressão da autonomia pessoal sobre os modos de apresentação de si no espaço público e digital. A ausência de consentimento não é, por si só, suficiente para tornar toda criação sintética ilícita.

Todavia, quando a representação sintética se apresenta como autêntica, quando não há contextualização adequada ou quando o conteúdo causa dano à esfera pessoal da vítima, a falta de autorização torna-se elemento jurídico especialmente relevante para a caracterização da ilicitude (Benabou, 2026; Makraki, 2024).

Makhambetsaliyev (2025) propõe compreender o fenômeno a partir da relação entre pessoa e performance, destacando que a tecnologia é capaz de projetar um "eu sintético" com efeitos reais no mundo social. Nessa linha, a imagem e a voz deixam de ser vistas apenas como objetos isolados de proteção e passam a ser compreendidas como componentes de uma unidade identitária vulnerável à manipulação algorítmica.

O dano potencial, portanto, não se esgota na exposição indevida da imagem e voz, mas pode atingir a reputação, credibilidade, autodeterminação e integridade narrativa da pessoa. Em razão disso, pode-se afirmar que o uso da imagem e da voz em *deepfakes* possui densidade jurídica própria, não se tratando de simples dado técnico disponível no ambiente digital, sobretudo de elemento de personalidade cuja manipulação pode afetar diretamente a dignidade do titular.

O problema jurídico dos *deepfakes* emerge quando a simulação sintética passa a produzir dano, engano relevante, exploração indevida da personalidade ou violação de direitos fundamentais, para Makraki (2024) a tecnologia comporta usos benignos e usos nocivos, sendo os riscos decorrentes dos *deepfakes* múltiplos e exigem tratamento diferenciado. Todavia, existem alguns riscos que merecem se destacados.

A apropriação não consentida da identidade pessoal apresenta-se como um risco, visto que a criação de um vídeo, imagem ou áudio em que alguém aparece praticando atos que nunca praticou ou proferindo falas que nunca pronunciou representa uma forma de imputação artificial de conduta, capaz de gerar danos à imagem da pessoa.

As *deepfakes*, também podem ser empregadas para difundir conteúdo ofensivo, sexualizado, humilhante, difamatório ou politicamente sensível, com grave potencial de atingir honra, boa fama e credibilidade da vítima. Shirish e Komal (2023) destacam que a circulação desses conteúdos amplia a vulnerabilidade dos indivíduos justamente porque a sofisticação técnica da fraude pode dificultar a pronta desconfiança do público em razão da rapidez de propagação no ambiente digital, que pode se consolidar antes mesmo de eventual contestação.

Outro grande risco destaca-se a desinformação e uso para fins financeiros, d*eepfakes* de voz têm sido discutidos em associação a golpes de engenharia social, em que a simulação vocal de pessoa conhecida serve para induzir pagamentos, transferências ou entrega de informações sensíveis (Olasiyan; Olasiyan, 2026), ou ainda, para utilização em publicidade, entretenimento, promoção comercial ou monetização de conteúdo sem autorização.

Outro risco importante é a dificuldade de reação jurídica eficaz, a criação de *deepfakes* pode ser barata, rápida, tecnicamente acessível e transnacional. Uma vez divulgado, o conteúdo tende a ser replicado em múltiplas plataformas, perfis e grupos, o que dificulta sua remoção integral e amplia a persistência do dano. Além disso, a identificação do autor nem sempre é simples, seja pelo anonimato digital, seja pela fragmentação da cadeia de criação, edição e circulação do conteúdo.

Por fim, os *deepfakes* desafiam o Direito, pois combinam três fatores: capacidade elevada de simulação, incidência direta sobre atributos personalíssimos e circulação massiva em ambiente digital. A violação, nesses casos, não se reduz à manipulação de um arquivo, mas alcança a identidade

socialmente projetada da pessoa. É precisamente por isso que, na sequência deste trabalho, será necessário examinar em que medida os direitos da personalidade, a privacidade, a proteção de dados e a responsabilidade civil oferecem instrumentos adequados para enfrentar esse tipo de lesão.

3 DIREITOS DA PERSONALIDADE, PRIVACIDADE E PROTEÇÃO DE DADOS DIANTE DOS DEEPFAKES

Os direitos da personalidade não garantidos constitucionalmente, e possuem um arcabouço de legislações que intitulam a proteção da pessoa, com o viés da Dignidade da Pessoa Humana como corolário dos direitos humanos, além da previsão da proteção de dados e privacidade que estão ligados à intimidade.

3.1 DIREITOS DA PERSONALIDADE E TUTELA DA IMAGEM E DA VOZ

A análise jurídica dos *deepfakes* exige, antes de tudo, o reconhecimento de que a imagem e a voz não constituem meros dados técnicos disponíveis no ambiente digital, mas projeções juridicamente protegidas da pessoa humana. No ordenamento brasileiro, a tutela da personalidade encontra fundamento constitucional na proteção à intimidade, à vida privada, à honra e à imagem, com expressa previsão de indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988).

Em nível infraconstitucional, o Código Civil reforça essa proteção ao disciplinar os direitos da personalidade e ao limitar a divulgação, a exposição e a utilização da imagem da pessoa quando ausente autorização ou quando presentes circunstâncias lesivas à honra, à respeitabilidade ou ao aproveitamento econômico indevido (Brasil, 2002).

Essa base normativa é especialmente relevante diante dos *deepfakes* porque a tecnologia atua precisamente sobre os elementos mais visíveis da individualidade. Ao reproduzir artificialmente um rosto, uma fala ou uma performance expressiva, o conteúdo sintético não apenas manipula informação, mas interfere na forma como a pessoa é socialmente representada.

Pois pode configurar violação a direitos da personalidade, na medida em que retira do indivíduo o controle sobre a circulação de sua própria exteriorização. Nesse ponto, Bosher (2026), ao discutir *deepfakes*, sustenta que a propagação não autorizada da imagem e da voz coloca em evidência a insuficiência de tratamentos fragmentados entre privacidade, proteção de dados e confidencialidade, sugerindo a necessidade de uma leitura mais robusta da proteção da personalidade.

A incidência dos direitos da personalidade sobre os *deepfakes* torna-se ainda mais evidente quando se observa que o conteúdo sintético pode atribuir à pessoa comportamentos, falas e situações

jamais vividos por ela. Nessa hipótese, a representação não autorizada deixa de ser mero uso indevido de um registro preexistente e passa a operar como fabricação artificial de presença**.**

No Brasil, já se reconhece que os direitos da personalidade possuem natureza existencial e estão diretamente vinculados à dignidade da pessoa humana, não podendo ser reduzida a uma lógica exclusivamente patrimonial. Benabou (2026), analisando o cenário europeu, sustenta que a proteção da pessoa por meio dos direitos da personalidade se mostra alternativa mais adequada do que a simples expansão de modelos proprietários ou de propriedade intelectual para resolver os casos de *deepfakes* individuais.

Dessa forma, a tutela da personalidade oferece uma das primeiras e mais importantes chaves de leitura para o problema dos *deepfakes*, ela permite compreender que o uso não consentido da imagem e da voz não é apenas tecnicamente problemático, mas juridicamente ofensivo à condição da pessoa como sujeito de direitos.

Singh (2024) observa, em estudo voltado ao desenvolvimento dos direitos da personalidade e da regulação da privacidade de dados em *deepfakes*, que o uso da semelhança ou da voz de uma pessoa levanta questões profundas sobre consentimento e sobre o direito de controlar a própria imagem. Em igual sentido, Usman (2025) destaca que a criação de *deepfakes* a partir de imagens, vozes e dados pessoais sem autorização compromete o equilíbrio entre inovação tecnológica e respeito aos direitos individuais.

O fato de alguém ter publicado uma fotografia ou participado de uma entrevista não autoriza, por si só, a reutilização desse material para a fabricação de conteúdo sintético que o faça aparentar dizer ou fazer algo diverso do originalmente registrado. A lógica jurídica do consentimento exige especificidade, finalidade legítima e compatibilidade entre o uso autorizado e o uso efetivamente realizado.

3.2 PROTEÇÃO DE DADOS PESSOAIS E LIMITES DO USO DE CONTEÚDOS SINTÉTICOS

A disciplina da proteção de dados pessoais oferece importante complemento à tutela da personalidade e da privacidade no enfrentamento dos *deepfakes*. Nesse sentindo Medon Affonso (2026, p. 7) “proteger a imagem de uma pessoa é, em última análise, proteger a sua personalidade”. No Brasil, a Lei Geral de Proteção de Dados Pessoais – LGPD, Lei 13.709 de 14 de agosto de 2018, define dado pessoal como informação relacionada a pessoa natural identificada ou identificável, conferindo especial proteção ao tratamento dessas informações (Brasil, 2018).

Makraki (2024), ao examinar os *deepfakes* sob o prisma do GDPR e do AI Act, parte justamente da constatação de que essa tecnologia envolve tratamento de dados pessoais. A autora sustenta que a

criação e a circulação de *deepfakes* se vinculam ao uso de informações relativas à pessoa, inserindo o fenômeno no universo das normas de proteção de dados.

Tal raciocínio é compatível com a realidade brasileira, vez que quando fotografias, vídeos, gravações de voz ou padrões biométricos são coletados, combinados e processados para produzir conteúdo sintético associado a uma pessoa determinada, há forte argumento para reconhecer a incidência da LGPD.

Essa percepção é relevante porque a proteção de dados desloca a análise para o ciclo completo do tratamento informacional. Não se examina apenas o momento da divulgação do *deepfake*, mas também as etapas anteriores de coleta, armazenamento, organização, combinação e reaproveitamento de materiais pessoais. Isso permite compreender que a ilicitude pode se instalar antes mesmo da publicação do conteúdo final.

Bosher (2026) observa que os *deepfakes* colocam em evidência a replicação não autorizada da imagem e da voz e a dificuldade de enquadrar adequadamente essa realidade apenas com ferramentas tradicionais. Singh (2024), por sua vez, aproxima explicitamente os direitos da personalidade da regulação da privacidade de dados, indicando que a semelhança e a voz da pessoa exigem leitura articulada entre consentimento e governança informacional.

Todavia Usman (2025) enfatiza que a criação de *deepfakes* frequentemente depende do uso de dados pessoais e, por isso, não pode ser dissociada do debate sobre controle informacional e limites éticos do reaproveitamento desses materiais. Assim, os dados coletados para ferramenta de *deepfakes* nem sempre ultrapassam os limites éticos.

O fato de uma foto ou gravação estar na internet não autoriza, de maneira automática, sua utilização em sistemas de IA para fins de clonagem, manipulação ou simulação da identidade alheia. A questão jurídica continua sendo a compatibilidade da finalidade, a existência de base legal e a preservação dos direitos do titular.

Por outro lado, é preciso reconhecer que a proteção de dados, sozinha, não resolve integralmente o problema dos *deepfakes*. Como observa Benabou (2026), o fenômeno também envolve dimensões de identidade, personalidade e engano público que escapam de uma abordagem puramente informacional.

A proteção de dados ajuda a estruturar a análise do tratamento dos insumos e dos fluxos informacionais, mas não substitui a necessidade de discutir dano moral, ofensa à reputação, apropriação da voz e da imagem, ou violação à dignidade da pessoa. Pode-se concluir, assim, que a tutela dos *deepfakes* exige leitura integrada de pelo menos três planos normativos.

Os direitos da personalidade, que protege a pessoa em sua dimensão existencial. Os direitos da privacidade e do consentimento, que asseguram autonomia sobre a projeção da identidade e sobre os usos da representação pessoal. Por fim, os direitos da proteção de dados, que disciplina os fluxos informacionais e os limites jurídicos do tratamento de conteúdos capazes de identificar o sujeito. Desse normativo mínimo que se extrai uma resposta juridicamente mais robusta ao uso não consentido da imagem e da voz em conteúdos sintéticos, capaz de trazer ao debate a responsabilidade civil.

4 RESPONSABILIDADE CIVIL PELO USO NÃO CONSENTIDO DE DEEPFAKES

A responsabilidade civil dos danos causados pela utilização ilícita de *deepfakes* pressupõe análise profunda quanto a caracterização do dano e sua ilicitude, a identificação e responsabilidade do sujeito criador, propagador e a concorrência dos fatos que os fazem figurar como responsáveis.

4.1 CONFIGURAÇÃO DO DANO E DA ILICITUDE

A análise da responsabilidade civil pelos *deepfakes* deve partir da constatação de que o uso não consentido da imagem e da voz alheia, quando apto a criar aparência de autenticidade e a produzir repercussões negativas concretas, pode configurar ato ilícito no âmbito do Direito Civil.

No ordenamento brasileiro, a regra geral da responsabilidade civil encontra fundamento nos arts. 186 e 927 do Código Civil, segundo os quais aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem comete ato ilícito e fica obrigado a repará-lo (Brasil, 2002).

O primeiro aspecto a ser destacado é que o dano decorrente de *deepfakes* não se reduz a uma única categoria, pois a lesão pode assumir dimensões morais, reputacionais, existenciais, informacionais e, em certos casos, patrimoniais, quando se trata de utilização indevida para fins comerciais, com a finalidade de obter vantagens sejam econômicas, ou com vieses econômicos.

Singh (2024) observa que uma das consequências mais sensíveis dos *deepfakes* está no abalo de reputações, relações pessoais e controle sobre a própria semelhança ou voz. Sharma e Daschaudhuri (2025), ao tratarem dos danos à imagem em contextos de *deepfake*, também salientam que o uso não consentido da identidade visual ou sonora pode comprometer seriamente a reputação do indivíduo, sobretudo quando o conteúdo o associa a comportamentos vexatórios, humilhantes ou enganosos.

A responsabilidade civil por *deepfakes*, de maneira geral, se insere no regime subjetivo, ou seja, é necessária a prova da culpa do agente (Freitas Filho, Santana Melo, 2025). Neste ínterim, tem-se como regra que a exposição, utilização ou divulgação da imagem ou voz de uma pessoa, requer como

regra de licitude o consentimento do titular, sob pena de violar a proteção dos direitos de personalidade, uma vez que subtrai do indivíduo a liberdade para dispor de sua própria imagem.

No entanto, há a discussão da possibilidade de se aplicar a responsabilidade objetiva em certos casos, principalmente em atividades que apresentam riscos intrínsecos:

> "Desse modo, a busca constante deve ser pela obtenção do consentimento inequívoco do titular da imagem violada, dado o potencial lesivo que sua divulgação pode ter, sobretudo com a mola propulsora da internet, que, em poucos minutos, consegue tornar mundialmente conhecida uma imagem obtida com o recurso da câmera de um smartphone" (Medon Affonso, Filipe, 2021, p. 6).

Sob a perspectiva civil, a ilicitude não depende apenas da falsidade técnica do conteúdo, mas do fato de que a pessoa é artificialmente inserida em uma narrativa não autorizada, com potencial de afetar sua dignidade, honra, respeitabilidade ou autodeterminação. Na esfera judicial, a responsabilidade pode ser evidenciada quando o sujeito não comprova de forma inequívoca a existência de consentimento da parte que seja apto a afastar a irregularidade na exposição da imagem ou voz, nos moldes do artigo 373, inciso II, do Código de Processo Civil.

Makhambetsaliyev (2025) sustenta, nesse sentido, que o dano causado por *deepfakes* não pode ser reduzido a uma visão simplificada de manipulação de imagem, pois a tecnologia afeta diretamente as concepções jurídicas de identidade, consentimento e personalidade. A lesão, portanto, é qualitativamente distinta daquela produzida por montagens tradicionais, já que a simulação sintética pode atribuir presença, ação e fala à pessoa sem qualquer correspondência com sua vontade.

Goodyear (2025), ao refletir sobre dignidade e *deepfakes*, indica que determinadas categorias de *deepfakes*, sobretudo as sexualizadas, produzem formas agravadas de dano, justamente porque reúnem exposição indevida, violação da autonomia sexual e intensa repercussão social, o que traz graves danos irreparáveis à vítima.

No plano da estrutura da responsabilidade civil, o dano pode ser compreendido como resultado da violação do direito da pessoa de controlar a utilização de sua imagem e de sua voz em contextos socialmente relevantes. Esse dano não exige, necessariamente, prejuízo econômico mensurável. A própria lógica constitucional da proteção da imagem e da honra, bem como a natureza existencial dos direitos da personalidade, autoriza reconhecer que a lesão pode estar presente na ofensa à dignidade e à projeção social do indivíduo.

Além disso, a ilicitude pode ser reforçada quando o *deepfake* é produzido ou divulgado em descumprimento de deveres de informação, transparência ou de observância da finalidade para a qual os dados foram originalmente coletados. Dessa forma, é possível afirmar que, em matéria de *deepfakes*,

a configuração do dano e da ilicitude exige olhar ampliado sobre a personalidade humana no ambiente digital. O ato ilícito não se limita à fabricação de conteúdo falso, mas se consuma quando essa fabricação compromete, sem justificativa legítima, o controle do indivíduo sobre sua representação, sua reputação e sua identidade narrativa.

A responsabilidade civil, por conseguinte, apresenta-se como mecanismo central para restaurar, ainda que imperfeitamente, o equilíbrio rompido pela manipulação sintética, o desafio passa a ser a identificação do sujeito criador da *deepfake* que causou o dano à vítima.

4.2 QUEM PODE SER RESPONSABILIZADO

Uma das maiores dificuldades práticas no campo dos *deepfakes*, e que constitui uma das questões mais sensíveis da responsabilidade civil, reside na identificação dos sujeitos potencialmente responsáveis pelos danos causados, precisamente porque a lesão, em muitos casos, não decorre de uma atuação isolada, mas de uma cadeia de produção e circulação do conteúdo sintético composta por múltiplos agentes.

Como se pode observar, em vez de um único autor claramente identificável, o dano pode resultar de atuação distribuída em ambiente digital com pluralidade de condutas e agentes. Ainda assim, isso não impede a construção de critérios jurídicos de imputação e responsabilidade civil.

A responsabilidade não deve ser analisada apenas sob a ótica formal da autoria imediata, mas a partir da contribuição causal e juridicamente relevante de cada sujeito para a produção ou a ampliação do dano. A complexidade tecnológica, portanto, não elimina a responsabilização, ao contrário, impõe ao intérprete o dever de reconstruir a cadeia de intervenção para verificar quem criou, quem divulgou, quem se beneficiou e quem, podendo agir, deixou de adotar providências adequadas para impedir a continuidade da lesão.

4.2.1 A Responsabilidade Civil dos Agentes Responsáveis

Nessa perspectiva, o primeiro responsável, em tese, é o criador do *deepfake*, isto é, aquele que manipula ou gera o conteúdo sintético usando a imagem, a voz ou outros traços identificadores de terceiro sem autorização. Em regra, é ele quem pratica a conduta diretamente ofensiva à personalidade da vítima, especialmente quando o conteúdo é deliberadamente forjado para causar engano, humilhação, exploração econômica ou dano.

Rezvorovych (2025), ao tratar dos aspectos civis do uso de *deepfakes*, ressalta que a produção e a disseminação não autorizadas de conteúdos que reproduzem imagem, voz ou traços comportamentais

de uma pessoa podem atingir direitos pessoais não patrimoniais, inclusive quando o conteúdo não está adequadamente identificado como artificial.

Além disso, a responsabilidade do criador pode surgir mesmo quando o conteúdo não é imediatamente disseminado em larga escala. Isso porque o simples ato de fabricar uma representação sintética não autorizada já pode configurar agressão à esfera jurídica da vítima, especialmente se o material for apto a atingir sua honra, sua reputação ou sua autodeterminação informativa.

O segundo possível responsável é o divulgador ou disseminador do conteúdo, que possui função fundamental na configuração do dano, pois nos *deepfakes*, frequentemente se intensifica na etapa de circulação. O conteúdo pode ser produzido em ambiente restrito, mas adquire gravidade jurídica maior quando é compartilhado de forma ampla, replicado em plataformas, ou inserido em contextos enganosos.

No ambiente digital, o dano causado por *deepfakes* frequentemente se agrava na etapa da circulação, pois a lesão se multiplica na medida em que o material é replicado em redes sociais, aplicativos de mensagens, fóruns, páginas de conteúdo ou plataformas de vídeo. Ainda que o criador original tenha acesso restrito ao material, a ampliação do dano ocorre quando terceiros reexpõem a vítima, perpetuam a aparência de autenticidade ou inserem o conteúdo em contextos ainda mais lesivos.

A responsabilidade do disseminador é especialmente relevante porque, em matéria de *deepfakes*, a repercussão social muitas vezes é mais danosa do que a criação inicial. O conteúdo pode ganhar ampla visibilidade em curto espaço de tempo, tornando praticamente irreversível a sua difusão. Assim, quem conscientemente compartilha, republica ou impulsiona o material ofensivo não atua como mero espectador passivo, mas como verdadeiro vetor de agravamento do dano.

Benabou (2026) chama atenção para o fato de que algumas respostas regulatórias recentes na Europa passaram a se preocupar não apenas com a criação, mas também com a publicação e a disseminação de imagens, vídeos ou vozes falsificadas sem consentimento e com capacidade de enganar sobre sua autenticidade. Embora essa discussão esteja vinculada a sistemas estrangeiros, ela reforça uma intuição dogmática relevante: quem conscientemente amplia a difusão do dano também pode participar juridicamente da ofensa.

Além disso, pode haver responsabilidade de quem obtém vantagem econômica com o conteúdo sintético. Isso ocorre, por exemplo, quando a imagem ou a voz alheia é utilizada em publicidade, monetização de conteúdo, promoção de serviços, captação de audiência ou exploração comercial da identidade da vítima.

A responsabilidade do beneficiário econômico é importante porque impede que a cadeia de exploração da personalidade se torne invisível sob o pretexto de ausência de autoria direta. Quem aufere vantagem com a lesão, especialmente quando participa conscientemente da sua estrutura de circulação, não pode ser tratado como terceiro neutro. Ao contrário, sua posição jurídica deve ser examinada à luz da contribuição concreta para o resultado danoso.

Outro ponto de destaque é a responsabilidade dos agentes que participam da cadeia de produção e edição, em ambientes tecnológicos complexos de diversos agentes em etapas sucessivas de seleção do material, utilização da ferramenta de inteligência artificial, ajustes de edição, por fim, publicação e distribuição do resultado.

Cada etapa pode ser realizada por uma mesma pessoa ou distribuída entre agentes, porém, essa fragmentação não exclui a responsabilidade, mas justifica-se a responsabilização concorrente de todos os que tenham contribuído de forma consciente, relevante e causal para a produção do dano.

A lógica da cadeia de produção é particularmente importante porque a lesão causada por *deepfake* frequentemente não se explica por uma única ação, mas por um encadeamento de intervenções técnicas. Cada etapa pode representar um momento de reforço da ofensa, de modo que a responsabilidade civil deve ser pensada de forma distributiva e funcional. Não interessa apenas quem acionou o comando final da geração do conteúdo, mas também quem forneceu os insumos, quem ajustou a representação, quem validou sua aparência e quem a colocou em circulação.

Essa compreensão é essencial para evitar que a dispersão tecnológica produza impunidade prática. Se o Direito insistisse em localizar apenas um autor originário, ignorando a cooperação dos demais agentes, a tutela da vítima se tornaria insuficiente. Por isso, em matéria de *deepfakes*, a pluralidade de intervenções deve conduzir a um modelo de imputação capaz de abranger tanto a autoria direta quanto as formas indiretas de participação no ilícito.

Bosher (2026) menciona a importância de mecanismos de retirada de conteúdo e chama atenção para a relevância da atuação das plataformas diante de *deepfakes* danosos. Olasiyan e Olasiyan (2026) também apontam que a alocação de responsabilidade entre criadores, distribuidores e plataformas é um dos temas centrais para o futuro da regulação da identidade sintética.

No direito brasileiro, a responsabilidade por conteúdo de terceiros em ambiente digital não se confunde automaticamente com a do autor material do ilícito. A análise depende do regime jurídico aplicável, do grau de conhecimento da plataforma sobre o conteúdo, da eventual inércia diante de notificações ou ordens específicas, da natureza da atividade desenvolvida e do modo como o serviço se relaciona com o dano.

Por isso, não se pode afirmar de maneira abstrata que toda plataforma que hospeda *deepfakes* responde civilmente pelo simples fato da circulação do conteúdo. O mais adequado é reconhecer que a responsabilidade das plataformas deve ser examinada caso a caso, especialmente quando houver omissão relevante, manutenção indevida de conteúdo sabidamente lesivo ou participação estrutural na sua propagação.

4.3 LIMITES DO REGIME ATUAL E PARÂMETROS PARA UMA TUTELA MAIS EFICAZ

Embora os direitos da personalidade, a privacidade, a proteção de dados e a responsabilidade civil já ofereçam instrumentos importantes para enfrentar os *deepfakes*, esses mecanismos, isoladamente, nem sempre são suficientes para garantir tutela efetiva. O problema não reside apenas na ausência de normas, mas na dificuldade de fazer com que categorias jurídicas tradicionais respondam, com velocidade e densidade adequadas.

Um primeiro limite do regime atual está na celeridade do dano, pois os *deepfakes* podem ser criados e disseminados em questão de minutos, enquanto a resposta jurídica tende a ser mais lenta, fragmentada e dependente de iniciativa da vítima. Muitas vezes, quando o reconhecimento formal do ilícito ocorre, o conteúdo já foi replicado amplamente, arquivado por terceiros ou reutilizado em novos contextos.

Bosher (2026) enfatiza justamente a necessidade de instrumentos mais eficazes de remoção e contenção de danos, destacando que a proteção da personalidade, para ser efetiva, precisa dialogar com mecanismos práticos de retirada do conteúdo lesivo.

A prova da autoria e da cadeia causal, também figura como um dos principais desafios. Em se tratando de ambiente digital, nem sempre é simples identificar quem gerou o conteúdo, quem o modificou, quem iniciou sua circulação e quem efetivamente o amplificou. O anonimato, o uso de ferramentas automatizadas e a circulação transnacional tornam a imputação mais complexa.

Outro desafio está na fragmentação das categorias jurídicas disponíveis e suas proteções. Como observam Bosher (2026) e Benabou (2026), o tratamento dos *deepfakes* costuma oscilar entre personalidade, privacidade, proteção de dados, propriedade intelectual, liberdade de expressão e regulação de plataformas.

Cada uma dessas áreas oferece parte da solução, mas nenhuma resolve sozinha o problema. Se o enfoque recair apenas sobre proteção de dados, corre-se o risco de ignorar a dimensão existencial da ofensa. Se o olhar for exclusivamente patrimonial, perde-se de vista a dignidade e a autonomia da vítima. Se a resposta se limitar à transparência, pode-se reduzir o engano público sem impedir o uso não consentido da identidade. A tutela eficaz, portanto, depende de uma interpretação sistemática.

Em matéria de *deepfakes* individuais, o consentimento deve ser tratado como critério jurídico forte para diferenciar usos legítimos e ilícitos da imagem e da voz. Sua ausência, sobretudo quando há aparência de autenticidade e potencial lesivo, deve pesar decisivamente na caracterização da ofensa civil. O segundo parâmetro é a proteção reforçada da personalidade, compreendendo imagem e voz como atributos existenciais e não apenas como objetos de uso econômico. O terceiro é a necessidade de respostas céleres de cessação do dano, com ênfase em mecanismos de remoção e desindexação sempre que juridicamente cabíveis.

Outro parâmetro relevante é a responsabilização proporcional dos agentes da cadeia digital**.** Não se trata de impor responsabilidade automática e indiferenciada, mas de evitar que a dispersão tecnológica produza impunidade prática. Olasiyan e Olasiyan (2026) defendem que a regulação da identidade sintética exigirá justamente modelos mais claros de distribuição de responsabilidade entre criadores, distribuidores e plataformas. A utilidade dessa proposta, para o contexto brasileiro, está em reforçar que a vítima não pode ficar desprotegida apenas porque o dano foi produzido em ambiente tecnicamente complexo.

Por fim, os *deepfakes* exigem releitura do próprio conceito de dano em matéria de personalidade. Makhambetsaliyev (2025) propõe compreender o fenômeno como um problema de construção jurídica da identidade, entre pessoa e performance. Essa formulação é particularmente útil porque evidencia que o dano não se limita à ofensa já consumada à reputação.

Em conclusão, o regime atual oferece fundamentos relevantes para responsabilizar civilmente o uso não consentido de *deepfakes*, mas enfrenta limites evidentes quanto à velocidade da resposta, à prova da autoria, à fragmentação normativa e à eficácia prática da tutela. Ainda assim, esses obstáculos não conduzem à inutilidade da responsabilidade civil.

Ao contrário, reforçam a necessidade de interpretação sistemática dos direitos da personalidade, da privacidade, da proteção de dados e dos deveres de remoção e prevenção. Em um cenário em que a identidade pode ser artificialmente reproduzida e desviada, a responsabilidade civil continua sendo instrumento central de proteção da pessoa, desde que aplicada com sensibilidade à nova realidade tecnológica.

5 CONCLUSÃO

O presente artigo teve por objetivo analisar os limites jurídicos do uso não consentido da imagem e da voz em *deepfakes*, tomando como eixo central a tutela dos direitos da personalidade e a incidência da responsabilidade civil diante das novas formas de manipulação sintética produzidas pela inteligência artificial generativa.

Ao longo do trabalho, buscou-se demonstrar que os *deepfakes* não representam apenas uma inovação técnica no campo da produção audiovisual, mas um desafio jurídico relevante, na medida em que permitem a recriação artificial da presença humana com alto potencial de verossimilhança, afetando diretamente a identidade, a reputação, a autonomia e o controle que o indivíduo deve exercer sobre sua própria representação no ambiente digital.

Na primeira parte do estudo, verificou-se que os *deepfakes* podem ser compreendidos como conteúdos sintéticos ou manipulados, produzidos com o auxílio de inteligência artificial, capazes de fazer parecer autênticas imagens, vídeos ou áudios em que determinada pessoa figura dizendo ou fazendo algo que, na realidade, não disse nem fez.

Não se trata apenas de falsidade tecnológica, mas de simulação convincente da identidade alheia, o que amplia os riscos de fraude, desinformação, exposição indevida e apropriação não autorizada da imagem e da voz. Dessa forma o *deepfake*, , não opera somente sobre arquivos ou dados, mas sobre a própria projeção social da pessoa.

Em seguida, a análise concentrou-se na incidência dos direitos da personalidade, da privacidade e da proteção de dados pessoais sobre o fenômeno. Constatou-se que a imagem e a voz não podem ser tratadas como meros elementos técnicos disponíveis à livre reutilização digital. Ao contrário, constituem atributos diretamente vinculados à personalidade e à autodeterminação do indivíduo, motivo pelo qual sua reprodução, manipulação ou exploração sem autorização pode configurar ofensa juridicamente relevante.

A ausência de consentimento mostrou-se elemento central na delimitação da ilicitude, sobretudo quando o conteúdo sintético é apresentado como autêntico, quando o titular não possui qualquer poder de controle sobre sua circulação ou quando a utilização afeta sua reputação, sua dignidade ou sua esfera informacional.

Também se evidenciou que a proteção de dados pessoais contribui para o enfrentamento do problema, uma vez que os *deepfakes* frequentemente dependem da coleta, do processamento e da recombinação de conteúdos identificadores da pessoa, ainda que tais instrumentos não sejam, por si sós, suficientes para esgotar a dimensão existencial da lesão.

Na terceira seção, o artigo examinou a responsabilidade civil pelo uso não consentido de *deepfakes* e demonstrou que os instrumentos legais do Direito brasileiro permanecem aplicáveis ao fenômeno, embora enfrentem limitações próprias do ambiente digital.

Observou-se que o dano decorrente dos *deepfakes* podem se dar de diversas formas, a depender do contexto de circulação do conteúdo e da intensidade da lesão causada. A ilicitude, por sua vez,

decorre não apenas da falsidade do material, mas da utilização indevida da imagem e da voz para imputar à vítima comportamentos, falas ou situações que ela jamais praticou ou autorizou.

Também verificou-se que a responsabilidade pode recair sobre diferentes agentes da cadeia de produção e difusão do conteúdo sintético, cuja omissão seja juridicamente relevante. Essa multiplicidade de sujeitos revela que os *deepfakes* desafiam os modelos tradicionais de imputação, sem, contudo, inviabilizar a aplicação da responsabilidade civil.

Diante desse percurso, é possível afirmar que a hipótese formulada na introdução foi confirmada. Os direitos da personalidade, a privacidade, a proteção de dados e a responsabilidade civil fornecem bases normativas importantes para enfrentar o uso ilícito de *deepfakes*, mas tais instrumentos, considerados isoladamente, não se mostram inteiramente suficientes para oferecer resposta plena e eficaz à complexidade da tecnologia.

Não se conclui, com isso, que a solução deva necessariamente consistir na criação imediata de um regime jurídico totalmente novo e autônomo para os *deepfakes*. O estudo indica, antes, que o ordenamento já contém fundamentos relevantes para a proteção da vítima, desde que interpretados de maneira coerente com os riscos próprios da inteligência artificial generativa.

Em conclusão, os *deepfakes* revelam uma transformação profunda nas formas de lesão à personalidade na sociedade digital. Se, no passado, a tutela da imagem e da voz já se colocava como exigência de respeito à dignidade da pessoa humana tutelados sobre direitos autorais, hoje essa tutela se torna ainda mais necessária diante da possibilidade de reprodução sintética da identidade em escala massiva e com aparência de verdade.

O Direito, nesse contexto, é chamado não apenas a reparar danos já consumados, mas a reafirmar que a pessoa humana não pode ser convertida, sem consentimento, em matéria-prima de simulações alheias. A proteção jurídica da imagem e da voz, portanto, permanece essencial, mas precisa ser reinterpretada à luz da inteligência artificial generativa, de modo a assegurar que o avanço tecnológico não se dê às custas da integridade, da liberdade e da dignidade do sujeito.

REFERÊNCIAS

BARREA, Adriana; SALMORIA, Camila Henning; RODRIGUES, Francisco Luciano Lima. Inteligência artificial – IA: reflexões sobre sua utilização pelo Poder Judiciário. ReJuB – Revista Judicial Brasileira, Brasília, Edição Especial Direito Digital, p. 329-361, jul./dez. 2023. DOI: 10.54795/RejuBEsp.DirDig.229. Disponível em: https://revistadaenfam.emnuvens.com.br/renfam/article/view/229. Acesso em: 4 maio 2026.

BENABOU, Valérie-Laure. Deepfakes and private rights in the perspective of EU law: is it necessary to intervene? Columbia Journal of Law & the Arts, 2026. Disponível em: https://journals.library.columbia.edu/index.php/lawandarts/article/download/14765/8066. Acesso em: 4 maio 2026.

BOSHER, Hayleigh. Do deepfakes, digital replicas and human digital twins justify personality rights? The Journal of World Intellectual Property, 2026. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/jwip.70020. Acesso em: 4 maio 2026.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 maio 2026.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 4 maio 2026.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 maio 2026.

CASTRO, Danilo et al. Inteligência artificial aplicada à bioinformática. BIOINFO – Revista Brasileira de Bioinformática e Biologia Computacional, ed. 1, jul. 2021. DOI: 10.51780/978-6-599-275326-14. Disponível em: https://bioinfo.com.br/inteligencia-artificial-aplicada-a-bioinformatica/. Acesso em: 6 maio 2026.

FREITAS FILHO, Hudson Ramos; SANTANA NETO, Hamilton Gomes de. RESPONSABILIDADE CIVIL PELO USO DE DEEPFAKES NA MANIPULAÇÃO DA IMAGEM E VOZ DE PESSOAS PÚBLICAS: PROTEÇÃO DA HONRA E DIGNIDADE NO ÂMBITO DO DIREITO CIVIL BRASILEIRO. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 11, n. 12, p. 3000–3016, 2025. DOI: 10.51891/rease.v11i12.22918. Disponível em: https://periodicorease.pro.br/rease/article/view/22918. Acesso em: 4 maio. 2026.

GOODYEAR, Michael P. Dignity and deepfakes. SSRN, 2025. Disponível em: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5199514. Acesso em: 4 maio 2026.

MAKRAKI, Ilektra. Deepfakes: legal challenges and protection under the scope of the General Data Protection Regulation and the Artificial Intelligence Act. 2024. Dissertação (Mestrado) – University of Macedonia, Thessaloniki, 2024. Disponível em: https://dspace.lib.uom.gr/handle/2159/30910. Acesso em: 4 maio 2026.

MEDON AFFONSO, Filipe José. O direito à imagem na era das deep fakes. Revista Brasileira de Direito Civil, [S. l.], v. 27, n. 01, p. 251, 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438. Acesso em: 6 maio. 2026.

OLASIYAN, T.; OLASIYAN, A. Regulating synthetic identity: deepfakes, voice-cloning and the future of AI law. SSRN, 2026. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6660880. Acesso em: 4 maio 2026.

REZVOROVYCH, K. Civil-law aspects of using deepfake content in the context of copyright and personal data protection. 2025. Disponível em: https://er.dduvs.edu.ua/handle/123456789/16855. Acesso em: 4 maio 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. Apelação Cível n. 1007875-45.2016.8.26.0292. Relator: Francisco Loureiro. 1ª Câmara de Direito Privado. Foro de Jacareí, 1ª Vara Cível. Julgado em: 1 dez. 2017. Registrado em: 1 dez. 2017.

SHARMA, P.; DASCHAUDHURI, P. Synthetic faces, real disrepute: deepfake and the quest to safeguard celebrity rights and reputation. Journal of Legal Research and Polity, 2025. Disponível em: https://jlrp.in/index.php/jlrp/article/view/45. Acesso em: 4 maio 2026.

SHIRISH, A.; KOMAL, S. A socio-legal inquiry on deepfakes. California Western International Law Journal, 2023. Disponível em: https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=2066&context=cwilj.
Acesso em: 4 maio 2026.

SINGH, A. Development of personality rights and data privacy regulation of deepfakes. SSRN, 2024. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5348028. Acesso em: 4 maio 2026.

TAVARES, Cláudio de Mello. Inteligência artificial e deepfakes: desafios jurídicos e tecnológicos para a integridade do processo democrático e as implicações para as eleições municipais de 2024. Revista Justiça Eleitoral em Debate, Rio de Janeiro, v. 14, n. 1, p. 49-58, 2024. DOI: 10.71381/awm10y94.

TOMASI, A. Construction and deconstruction of the image in the digital world: protection of personal identity and deepfake. 2025. Disponível em: https://iris.unisalento.it/handle/11587/568148. Acesso em: 4 maio 2026.

TURING, Alan Mathison. Computing machinery and intelligence. Mind, Oxford, v. 59, n. 236, p. 433-460, 1950. Disponível em: https://academic.oup.com/mind/article/LIX/236/433/986238. Acesso em: 4 de maio 2026.

USMAN, S. O. Consent, ownership, and the ethics of using personal data in deepfake creation. 2025. Disponível em: https://www.researchgate.net/profile/Salawudeen-Usman/publication/395019225_Consent_Ownership_and_the_Ethics_of_Using_Personal_Data_in_Deepfake_Creation/links/68b0673ad9261f6f51afbe23/Consent-Ownership-and-the-Ethics-of-Using-Personal-Data-in-Deepfake-Creation.pdf. Acesso em: 4 maio 2026.