



**CENTRO UNIVERSITÁRIO DOM PEDRO II
CURSO DE DIREITO**

WALLACE PATRICK LIMA CARDOSO

DEEPPAKES E RESPONSABILIDADE CIVIL: uma análise das
implicações jurídicas sobre os danos decorrentes da manipulação digital
de imagem por inteligência artificial.

BARREIRAS - BA

2026

WALLACE PATRICK LIMA CARDOSO

DEEPPFAKES E RESPONSABILIDADE CIVIL: uma análise das implicações jurídicas sobre os danos decorrentes da manipulação digital de imagem por inteligência artificial.

Trabalho de Conclusão de Curso apresentado ao Colegiado do Curso de Direito do Instituto de Educação do Centro Universitário Dom Pedro II de Barreiras, como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientador(a): Profa. Ma. Suzana Wong dos Santos.

BARREIRAS - BA

2026

WALLACE PATRICK LIMA CARDOSO

DEEPPAKES E RESPONSABILIDADE CIVIL: uma análise das
implicações jurídicas sobre os danos decorrentes da manipulação digital
de imagem por inteligência artificial.

Trabalho de Conclusão de Curso apresentado
ao Centro Universitário Dom Pedro II de
Barreiras - Bahia

Barreiras/Bahia, 18 de junho de 2026.

Documento assinado digitalmente
 **SUZANA WONG DOS SANTOS**
Data: 30/06/2026 09:27:10-0300
Verifique em <https://validar.iti.gov.br>

Ma. Suzana Wong dos Santos

Documento assinado digitalmente
 **FABIO PEREIRA DE SOUZA**
Data: 30/06/2026 09:14:50-0300
Verifique em <https://validar.iti.gov.br>

Me. Fabio Pereira de Souza

Documento assinado digitalmente
 **MATEUS DE CAMPOS BALDIN**
Data: 30/06/2026 09:07:40-0300
Verifique em <https://validar.iti.gov.br>

Dr. Mateus de Campos Baldin

C268d Cardoso, Wallace Patrick Lima

Deepfakes e responsabilidade civil: uma análise das implicações jurídicas sobre os danos decorrentes da manipulação digital de imagem por inteligência artificial. / Wallace Patrick Lima Cardoso -- Barreiras, 2026.

24 p.

Trabalho de Conclusão de Curso (Graduação – Curso de Direito)
AFYA Centro Universitário – Barreiras/BA.
Orientador (a): Prof. Ma. Suzana Wong dos Santos.

1. Responsabilidade civil 2. Deepfakes. 3. inteligência artificial. I. Santos, Suzana Wong dos II. Título.

CDU 347.51
CDD 346.03

RESUMO

O presente trabalho analisa a responsabilidade civil decorrente da utilização e produção de *deepfakes*, com enfoque na proteção dos direitos da personalidade no ordenamento jurídico brasileiro. As *deepfakes* consistem em manipulações digitais de imagem, voz e vídeo realizadas por inteligência artificial, capazes de reproduzir características humanas com elevado grau de realismo e potencial lesivo. A pesquisa teve como objetivo examinar a adequação dos fundamentos da responsabilidade civil diante dos danos causados por essas tecnologias, especialmente quanto à violação da honra, da imagem, da privacidade e da dignidade da pessoa humana. Utilizou-se metodologia qualitativa, de natureza exploratória e descritiva, por meio de pesquisa bibliográfica e documental. Foram analisados conceitos de responsabilidade civil, direitos da personalidade, aspectos jurídicos das *deepfakes* e entendimentos doutrinários e jurisprudenciais sobre o tema. Conclui-se que o ordenamento jurídico brasileiro oferece mecanismos para a responsabilização civil, embora persistam desafios normativos e práticos que demandam aperfeiçoamento legislativo.

Palavras-chave: *Deepfakes*. Responsabilidade civil. Inteligência artificial. Direitos da personalidade.

ABSTRACT

This study analyzes civil liability arising from the use and creation of deepfakes, focusing on the protection of personality rights within the Brazilian legal system. Deepfakes consist of digital manipulations of images, voices, and videos generated through artificial intelligence, capable of reproducing human characteristics with a high degree of realism and significant harmful potential. The research aimed to examine the adequacy of traditional civil liability principles in addressing damages caused by such technologies, particularly regarding violations of honor, image, privacy, and human dignity. A qualitative, exploratory, and descriptive methodology was adopted, based on bibliographic and documentary research. The study examined the fundamental concepts of civil liability, personality rights, the legal implications of deepfakes, and relevant doctrinal and judicial understandings on the subject. It was concluded that the Brazilian legal system provides mechanisms for civil liability in cases involving deepfakes; however, normative and practical challenges remain, requiring legislative improvements to ensure effective protection of personality rights in the digital age.

Keywords: Deepfakes. Civil liability. Artificial intelligence. Personality rights.

SUMÁRIO

1. INTRODUÇÃO.....	5
2. DEEPFAKES E MANIPULAÇÃO DIGITAL: ASPECTOS CONCEITUAIS E IMPLICAÇÕES JURÍDICAS MULTIDIMENSIONAIS.....	7
2.1. EVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL E DAS TECNOLOGIAS DE MANIPULAÇÃO DIGITAL.....	7
2.2. CONCEITO E FUNCIONAMENTO DA TECNOLOGIA DE <i>DEEPFAKE</i>	7
2.3. TIPOS DE <i>DEEPFAKES</i> E SUAS APLICAÇÕES.....	8
2.4. A VIOLAÇÃO PLURIFACETADA DOS DIREITOS DA PERSONALIDADE.....	9
2.5. A INCIDÊNCIA DE MICROSSISTEMAS JURÍDICOS.....	11
3. RESPONSABILIDADE CIVIL NOS CASOS DE <i>DEEPFAKE</i>: ANÁLISE DOUTRINÁRIA E JURISPRUDENCIAL.....	13
3.1 RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO...	13
3.2 PROTEÇÃO JURÍDICA DA IMAGEM, HONRA E PRIVACIDADE.....	14
3.3 RESPONSABILIDADE CIVIL DECORRENTE DA MANIPULAÇÃO DIGITAL DE IMAGEM.....	15
3.4 RESPONSABILIDADE DE PROVEDORES E PLATAFORMAS DIGITAIS.....	16
3.5 ENTENDIMENTO DOUTRINÁRIO SOBRE <i>DEEPFAKES</i> E DANOS DIGITAIS.	17
3.6 JURISPRUDÊNCIA BRASILEIRA SOBRE MANIPULAÇÃO DIGITAL E VIOLAÇÃO DE IMAGEM.....	17
4. ESTUDO DE CASO: RESPONSABILIDADE CIVIL DECORRENTE DE <i>DEEPFAKE</i>.....	19
4.1 APRESENTAÇÃO DO CASO ANALISADO.....	19
4.2 CONTEXTUALIZAÇÃO JURÍDICA DO CASO.....	19
4.3 ANÁLISE DA CONDUTA E DA UTILIZAÇÃO DE <i>DEEPFAKE</i>	20
4.4 RESPONSABILIDADE CIVIL DAS PARTES ENVOLVIDAS.....	21
4.5 DECISÃO JUDICIAL E FIXAÇÃO DA INDENIZAÇÃO.....	21
4.6 RELEVÂNCIA DO CASO PARA O ESTUDO DA RESPONSABILIDADE CIVIL POR <i>DEEPFAKES</i>	22
5. CONCLUSÃO.....	23
REFERÊNCIAS.....	24

1. INTRODUÇÃO

O avanço das tecnologias de inteligência artificial transformou significativamente a forma como informações, imagens e conteúdos audiovisuais são produzidos e compartilhados na sociedade contemporânea. Nesse cenário, destacam-se as chamadas *deepfakes*, tecnologias capazes de manipular imagens, vídeos e áudios com elevado grau de realismo, reproduzindo artificialmente características físicas e vocais de pessoas reais por meio de algoritmos de aprendizado profundo.

Embora essa inovação possua aplicações legítimas em áreas como entretenimento, publicidade e educação, sua utilização indevida passou a representar uma relevante ameaça aos direitos da personalidade, especialmente à honra, à imagem, à privacidade e à dignidade da pessoa humana. Nesse sentido, como o ordenamento jurídico brasileiro, à luz dos princípios e institutos da responsabilidade civil, pode oferecer respostas adequadas e efetivas aos danos resultantes da manipulação digital de imagens por meio de *deepfakes*?

Partindo da hipótese de que a responsabilidade civil brasileira revela-se parcialmente insuficiente para abranger os danos causados pelas *deepfakes*, demandando releituras doutrinárias e adequações normativas que considerem as novas tecnologias e os riscos associados à manipulação digital de imagens, a fim de assegurar a efetiva proteção dos direitos da personalidade.

O presente trabalho teve como objetivo analisar os impactos jurídicos de tais ferramentas sob a perspectiva da responsabilidade civil, investigando a adequação dos fundamentos tradicionais do ordenamento jurídico brasileiro para responder aos danos decorrentes da falsificação sintética de imagem por inteligência artificial. A pesquisa buscou compreender de que forma os direitos personalíssimos são violados por meio dessas tecnologias, bem como examinar os mecanismos jurídicos de reparação existentes e os desafios enfrentados pela doutrina e pela jurisprudência na responsabilização civil desses atos ilícitos.

Quanto à metodologia, a pesquisa desenvolveu-se por meio de abordagem qualitativa, de natureza exploratória e descritiva, utilizando o método dedutivo para analisar a aplicação dos fundamentos gerais da responsabilidade civil aos casos específicos envolvendo essas mídias sintéticas. O estudo baseou-se em pesquisa bibliográfica e documental, com análise de obras doutrinárias, legislação nacional, artigos científicos e precedentes jurisprudenciais relacionados à violação de atributos essenciais da personalidade no ambiente digital.

Para a construção teórica da pesquisa, destacaram-se as contribuições doutrinárias de Carlos Roberto Gonçalves, no estudo da responsabilidade civil; Maria Helena Diniz, na análise da tutela da personalidade; e Patrícia Peck Pinheiro, nas discussões sobre direito digital, proteção de dados pessoais, privacidade e os desafios jurídicos decorrentes do uso de novas tecnologias e da inteligência artificial.

Para estruturar e desenvolver o trabalho, inicialmente foram apresentados aspectos conceituais e técnicos sobre *deepfakes* e manipulação digital, bem como implicações jurídicas multidimensionais. Em sequência, foram apresentados os conceitos fundamentais da responsabilidade civil e dos direitos da personalidade, abordando seus elementos estruturais, e também, uma análise doutrinária e jurisprudencial acerca da responsabilidade civil em ambientes digitais, destacando a aplicação do Código Civil, do Marco Civil da Internet, da Lei Geral de Proteção de Dados e da jurisprudência do Superior Tribunal de Justiça em casos relacionados à violação de imagem e danos morais. Por fim, a pesquisa abordou um estudo de caso, trazendo uma situação concreta da temática, demonstrando como o avanço tecnológico tem exigido adaptações interpretativas do Direito brasileiro.

2. DEEPPAKES E MANIPULAÇÃO DIGITAL: ASPECTOS CONCEITUAIS E IMPLICAÇÕES JURÍDICAS MULTIDIMENSIONAIS

2.1. EVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL E DAS TECNOLOGIAS DE MANIPULAÇÃO DIGITAL

Provocada pelo desenvolvimento da Inteligência Artificial (IA) nas últimas décadas, uma profunda transformação na forma como conteúdos digitais são produzidos e disseminados tem causado diversos desafios para o ordenamento jurídico, em especial, no que se refere à proteção dos direitos da personalidade e à responsabilização civil por danos.

A evolução da inteligência artificial ocorreu gradualmente, passando de sistemas baseados em regras previamente programadas para modelos capazes de aprender padrões a partir de grandes volumes de dados. Esse avanço permitiu o desenvolvimento de aplicações cada vez mais sofisticadas, incluindo sistemas de reconhecimento facial, processamento de linguagem natural e geração de conteúdos sintéticos (RUSSELL; NORVIG, 2021, p. 26).

Conforme Russell e Norvig (2021, p. 4), a IA pode ser compreendida como o estudo e desenvolvimento de agentes capazes de perceber o ambiente e agir racionalmente para atingir determinados objetivos. Nesse sentido, as *deepfakes* representam uma das maneiras mais complexas e disruptivas de manipulação digital, confundindo o real com o virtual.

2.2. CONCEITO E FUNCIONAMENTO DA TECNOLOGIA DE DEEPPAKE

O termo *deepfake* é uma junção das expressões em inglês *deep learning* (aprendizado profundo) e *fake* (falso). Conforme Russell e Norvig (2021, p. 25), refere-se a mídias sintéticas, como áudios, vídeos e imagens, geradas através de técnicas avançadas de IA, evoluindo do *deep learning* e de modelos como as Redes Generativas Adversariais (GANs – *Generative Adversarial Networks*), que permite a

criação de conteúdos audiovisuais sintéticos com um grau de realismo capaz de iludir o observador médio, tornando a distinção entre o real e o artificial uma tarefa árdua. Todavia, a complexidade de tal tecnologia não está presente apenas na qualidade visual ou sonora do que foi produzido, mas também na exploração da confiança social atribuída historicamente a registros audiovisuais (CHESNEY; CITRON, 2019, p. 1760).

O funcionamento desse mecanismo de IA geralmente está associado ao uso de GANs, compostas por dois sistemas que atuam simultaneamente. “Enquanto uma rede produz imagens ou vídeos sintéticos, a outra avalia a autenticidade do conteúdo gerado, promovendo um processo contínuo de aperfeiçoamento até que a falsificação se torne visualmente convincente” (RUSSELL; NORVIG, 2021, p. 29).

Do ponto de vista técnico, “um *deepfake* consiste em uma mídia sintética que simula a realidade de forma convincente, permitindo a substituição de rostos, a clonagem de vozes e a alteração de expressões de maneira quase imperceptível” (CHESNEY; CITRON, 2019). Essa capacidade de manipulação se manifesta em diversas modalidades, estando entre elas as de vídeo, áudio, imagem e em tempo real.

2.3. TIPOS DE *DEEPPAKES* E SUAS APLICAÇÕES

Conforme observam Chesney e Citron (2019, p. 1765), os *deepfakes* podem assumir diferentes formas, incluindo manipulações de vídeo, áudio e imagem, com distintos potenciais lesivos.

As *deepfakes* de vídeo são utilizadas amplamente na indústria do entretenimento, inserindo o rosto de uma pessoa no corpo de outra ou na manipulação de expressões faciais em gravações existentes, sendo a forma mais conhecida e frequentemente associada à criação de conteúdo pornográfico ou à difusão de desinformação política.

Temos também os *deepfakes* de áudio, permitindo a criação de falas completamente fictícias com a voz autêntica de uma pessoa, reproduzindo

perfeitamente entonações, sotaques e padrões linguísticos, podendo ser considerada uma clonagem de voz. Tal modalidade tem sido utilizada com mais frequência em fraudes bancárias e golpes digitais, uma vez que a voz é socialmente atribuída como forma de validação da identidade.

Outra modalidade relevante é a dos *deepfakes* de imagem, que consistem na manipulação de fotografias para inserir indivíduos em contextos inexistentes, possuindo um potencial lesivo elevado, principalmente quando utilizados para associar a vítima a situações vexatórias ou socialmente reprováveis.

Além disso, existem as *deepfakes* em tempo real, tecnologia que permite a alteração instantânea de imagem ou voz durante transmissões ao vivo, ou seja, um observador externo pode acreditar estar em uma chamada de vídeo com uma pessoa, mas ela ser outra que está usando ferramentas de IA para fraudar a identidade de outra. Portanto, os riscos de manipulação em debates, depoimentos ou eventos públicos, são ampliados exponencialmente.

Apesar de existirem aplicações legítimas e práticas para essa tecnologia, como na educação, na publicidade e no entretenimento, o uso indevido e malicioso representa uma ameaça à confiança pública, à integridade informacional e à proteção dos direitos fundamentais.

2.4. A VIOLAÇÃO PLURIFACETADA DOS DIREITOS DA PERSONALIDADE

No atual cenário de tensão jurídica, marcado pelo potencial de violação massiva dos direitos personalíssimos, garantias fundamentais previstas no art. 5º, incisos V e X, da Constituição Federal e regulamentadas pelos arts. 11 a 21 do Código Civil, são inerentes à dignidade humana, caracterizando-se por serem irrenunciáveis e intransmissíveis. Sob essa perspectiva, a manipulação digital proporcionada por IA não apenas tangencia, mas atinge diretamente esse núcleo essencial de proteção jurídica, configurando uma violação que desafia a visão tradicional do direito civil.

No que diz respeito ao direito à imagem, esse recurso tecnológico causa danos que vão muito além do uso não autorizado do rosto de alguém. A doutrina atual divide esse direito em três partes: a imagem-retrato (aparência física), a imagem-atributo (reputação e como a pessoa é vista pela sociedade) e a imagem-voz (som da fala) (DINIZ, 2023, p. 137). Ao manipular áudio e vídeo de forma avançada, essas mídias sintéticas violam as três áreas ao mesmo tempo.

Conforme leciona Diniz (2023), os direitos da personalidade constituem projeções jurídicas da própria dignidade humana, portanto, a utilização de *deepfakes* não representa mera apropriação indevida da imagem, pois a tecnologia não apenas copia a aparência da vítima, mas a coloca em situações falsas e muitas vezes vergonhosas, o que atinge sua credibilidade e inventa condutas que ela nunca praticou. Além disso, a clonagem de voz representa um ataque específico à identidade sonora, aumentando o potencial de dano.

Essas manipulações também geram impactos graves sobre a honra. Sob a ótica de Gonçalves (2023), a divulgação de vídeos falsos com intenção de humilhar prejudica tanto a honra objetiva (a fama da pessoa perante os outros) quanto a honra subjetiva (sua autoestima e dignidade). No Direito Civil, essas violações geram o dever de indenizar por danos morais. Já no Direito Penal, dependendo do conteúdo, quem cria ou divulga pode responder por crimes como difamação, injúria ou calúnia.

Conforme observa Doneda (2020, p. 25-26), os dados pessoais representam aspectos da própria personalidade do indivíduo, razão pela qual sua utilização indevida pode comprometer a autonomia, a liberdade e a identidade da pessoa. Nesse contexto, essas ferramentas não configuram mera manipulação tecnológica de imagens, mas verdadeira interferência na esfera existencial do sujeito, uma vez que utilizam dados biométricos, voz e imagem para construir representações falsas capazes de afetar sua reputação, autodeterminação e livre desenvolvimento da personalidade.

Por fim, esses sistemas de geração artificial ameaçam o direito à identidade pessoal, que garante que cada um seja reconhecido pela sua história e características reais (DINIZ, 2023). Criar versões artificiais de alguém para simular

falas e comportamentos é uma forma de roubo de identidade. Esse fenômeno desliga a imagem pública da pessoa de sua vida real, causando confusão na sociedade e sofrimento psicológico para a vítima. Em última análise, essa tecnologia não fere apenas direitos isolados, mas atinge a própria integridade do ser humano, o que exige leis modernas e preparadas para os desafios da era digital.

2.5. A INCIDÊNCIA DE MICROSSISTEMAS JURÍDICOS

A complexidade desse fenômeno exige que a análise jurídica vá além do Código Civil, integrando diferentes microssistemas que oferecem respostas específicas para cada faceta do dano. No campo da Lei Geral de Proteção de Dados (LGPD), lei nº 13.709/2018, por exemplo, a criação de um *deepfake* pressupõe o tratamento e uso de dados pessoais, em muitos casos, de dados biométricos utilizados para identificação do titular (BRASIL, 2018).

Como o uso desses dados exige uma autorização clara e específica do titular, o que raramente ocorre em casos ilícitos, a simples utilização de imagens e áudios para treinar sistemas de IA já atrai a incidência da LGPD e se configura como uma violação que permite a responsabilização civil de quem a pratica. Para Doneda (2020, p. 35), a proteção de dados pessoais deve ser compreendida como instrumento de proteção da personalidade humana e da autodeterminação informativa.

Somando-se a isso, o Marco Civil da Internet (Lei nº 12.965/2014) desempenha um papel fundamental ao lidar com a velocidade com que esses conteúdos se espalham no ambiente digital. Embora a regra geral determine que as plataformas só são responsáveis por remover conteúdos após uma ordem judicial, a lei abre uma exceção rigorosa para casos de nudez ou atos sexuais não autorizados. Nessas situações, que abrangem os *deepfakes* pornográficos, o provedor é obrigado a remover o material logo após uma simples notificação da vítima, sob pena de ser responsabilizado junto com o agressor pelo prejuízo causado (BRASIL, 2014).

Essa proteção alcança também o Direito do Consumidor, uma vez que o uso de mídias sintéticas em fraudes financeiras ou comerciais pode ser caracterizado como uma falha na prestação de serviços. Nesses casos, as instituições envolvidas respondem de forma objetiva pelos danos causados, conforme o Código de Defesa do Consumidor, independentemente de terem agido com culpa. No campo político, o Tribunal Superior Eleitoral tem estabelecido regras rígidas para proteger a honestidade das eleições. O uso de tecnologias para manipular a imagem ou a voz de candidatos com o intuito de enganar o eleitor é expressamente proibido, podendo resultar em multas pesadas e até na perda do mandato.

Diante desse cenário, essas ferramentas não apenas criam novas formas de violar os direitos da personalidade, mas também tornam os danos muito mais graves e difíceis de reparar por causa do efeito multiplicador do dano no ambiente digital. Conforme Pinheiro (2021, p. 306), os danos ocorridos no ambiente digital apresentam características próprias, como a rápida propagação das informações e a dificuldade de eliminação definitiva dos conteúdos ilícitos, dificultando a efetiva reparação dos prejuízos causados. Dessa forma, a união entre o extremo realismo tecnológico e a disseminação maliciosa acaba gerando um conjunto de infrações simultâneas em diversas esferas do Direito.

Assim, torna-se indispensável que o sistema jurídico ofereça uma resposta coordenada, unindo os conceitos tradicionais de responsabilidade civil às novas ferramentas digitais para garantir uma proteção real à dignidade humana na era da IA.

3. RESPONSABILIDADE CIVIL NOS CASOS DE *DEEPPFAKE*: ANÁLISE DOUTRINÁRIA E JURISPRUDENCIAL

3.1 RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

Com a finalidade de reparação de danos, a responsabilidade civil constitui um dos principais instrumentos do ordenamento jurídico brasileiro, e assume um papel central diante dos danos provocados pelas novas tecnologias digitais. Embora tradicionalmente voltado para uma concepção patrimonial, foi evoluindo historicamente e passou a abranger, também, direitos existenciais, morais e personalíssimos.

Na legislação brasileira, a responsabilidade civil é regulamentada pelo art. 186 do Código Civil, “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”, e complementarmente pelo art. 927, em que “aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo”.

Sob essa perspectiva, a configuração da responsabilidade civil subjetiva depende, tradicionalmente, da presença de quatro elementos essenciais: conduta, culpa, dano e nexos causal. Segundo Cavalieri Filho (2023, p. 18), “A responsabilidade civil é o dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário.”

A conduta é o comportamento humano voluntário capaz de gerar consequências jurídicas, podendo ocorrer tanto por ação quanto por omissão. A culpa, refere-se à violação do dever de cuidado, podendo se manifestar por negligência, imprudência ou imperícia. O dano representa elemento indispensável para a configuração da responsabilidade civil, sendo compreendido como a lesão efetiva a um interesse juridicamente protegido.

Além da responsabilidade subjetiva, o ordenamento jurídico brasileiro, fundamentada na teoria do risco, admite hipóteses de responsabilidade civil objetiva.

Segundo Gonçalves (2023, p. 9):

Na teoria do risco se subsume a ideia do exercício de atividade perigosa como fundamento da responsabilidade civil. O exercício de atividade que

possa oferecer algum perigo representa um risco, que o agente assume, de ser obrigado a ressarcir os danos que venham resultar a terceiros dessa atividade.

O parágrafo único do artigo 927 do Código Civil prevê que haverá obrigação de reparar o dano independentemente de culpa quando a atividade normalmente desenvolvida pelo autor implicar, por sua natureza, risco para os direitos de terceiros. Dito isso, Pinheiro (2023, p. 303), afirma:

Para o Direito Digital, a teoria do risco tem maior aplicabilidade, uma vez que, nascida na era da industrialização, vem resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações, em virtude do princípio de equilíbrio de interesses e genérica equidade. Considerando apenas a Internet, que é mídia e veículo de comunicação, seu potencial de danos indiretos é muito maior que de danos diretos, e a possibilidade de causar prejuízo a outrem, mesmo que sem culpa, é real. Por isso, a teoria do risco atende às questões virtuais e a soluciona de modo mais adequado, devendo estar muito bem associada à determinação legal de quem é o ônus da prova em cada caso.

3.2 PROTEÇÃO JURÍDICA DA IMAGEM, HONRA E PRIVACIDADE

Os direitos da personalidade enfrentam diariamente problemas relacionados a danos decorrentes de *deepfakes*. A Constituição Federal de 1988 assegura, em seu artigo 5º, inciso X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo o direito à indenização pelos danos materiais ou morais decorrentes de sua violação.

O Código Civil, em seu art. 20, dispõe que:

Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação da imagem de uma pessoa poderá ser proibida, a seu requerimento, se lhe atingir a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

A proteção de direitos personalíssimos constitui importante expressão dos atributos da personalidade no ordenamento jurídico brasileiro, estando diretamente relacionada à tutela da dignidade da pessoa humana. Conforme afirma Diniz (2023, p. 120), “Os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis e inexpropriáveis”

O direito à imagem garante ao indivíduo o controle sobre a utilização de sua representação física, voz e características pessoais. A honra relaciona-se à reputação e à dignidade da pessoa perante a sociedade, abrangendo tanto a honra objetiva, ligada à percepção social, quanto a honra subjetiva, vinculada à autoestima e ao sentimento pessoal de dignidade. Ademais, a privacidade protege a vida íntima do indivíduo contra interferências externas indevidas, garantindo ao sujeito o direito de manter reservadas informações pessoais, hábitos, relações e aspectos de sua vida privada.

3.3 RESPONSABILIDADE CIVIL DECORRENTE DA MANIPULAÇÃO DIGITAL DE IMAGEM

Fundamentando-se na violação dos bens jurídicos da personalidade, uma vez que a falsificação sintética da imagem ultrapassa a simples reprodução não autorizada, pois atribui à vítima comportamentos e situações inexistentes, configurando verdadeiro ato ilícito. Além disso, a IA possibilita a criação artificial de conteúdos falsos altamente realistas, capazes de atribuir ao indivíduo comportamentos, falas ou situações inexistentes. Tal tecnologia permite a manipulação integral da identidade da vítima, somada ao elevado potencial de disseminação em massa, circunstância que dificulta significativamente a identificação do autor da conduta ilícita.

Tais elementos ampliam significativamente o potencial lesivo da conduta. De acordo com a doutrina, o uso indevido da imagem em ambiente digital gera responsabilidade civil independentemente da prova do prejuízo concreto, configurando dano moral presumido. Nessa linha, a utilização indevida da imagem de uma pessoa, especialmente quando a expõe a situações constrangedoras ou vexatórias, configura hipótese de reparação por dano moral, sendo dispensável a demonstração concreta do prejuízo sofrido pela vítima (GONÇALVES, 2023, p. 487). Assim, o reconhecimento do dano moral decorre automaticamente da própria violação.

Em complemento, também podem surgir danos materiais, pois, em determinadas situações, a falsificação digital da imagem pode gerar prejuízos permanentes à reputação do indivíduo, dada a velocidade e a amplitude da disseminação de conteúdos na internet, principalmente quando a manipulação compromete atividades profissionais, contratos publicitários, relações comerciais ou a credibilidade pública da vítima.

3.4 RESPONSABILIDADE DE PROVEDORES E PLATAFORMAS DIGITAIS

A responsabilidade das plataformas digitais nos casos de *deepfake* é regulada principalmente pelo Marco Civil da Internet (Lei nº 12.965/2014). Em seu art. 19, ela estabelece que o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para tornar indisponível o conteúdo apontado como ilícito. Portanto, os provedores só teriam uma responsabilidade objetiva em caso de descumprimento.

Esse modelo busca equilibrar a liberdade de expressão, a proteção de direitos fundamentais, e a neutralidade das plataformas. Nesse sentido, o Marco Civil da Internet busca evitar a censura privada, valorizando a liberdade de expressão, condicionando a responsabilização dos provedores ao descumprimento de ordem judicial (MIRAGEM, 2021).

Entretanto, ainda é alvo de críticas, especialmente diante da velocidade e capacidade de disseminação de conteúdos ilícitos na internet, e a sua dificuldade de remoção imediata. Conforme aponta Pinheiro (2021, p. 305), as barreiras legais afetam diretamente os envolvidos:

Agora, após a nova lei, a remoção do conteúdo só irá ocorrer após ordem judicial específica e fundamentada, o que traz, além de um ônus financeiro para a vítima (custo judicial), também o efeito do tempo sobre a disseminação do conteúdo (quanto maior a demora na remoção, maior o impacto do conteúdo para a vítima).

Apesar da remoção por decisão judicial, existe uma alta probabilidade de continuar circulando em diferentes plataformas, aplicativos de mensagens e redes

sociais, dificultando a identificação do responsável e ampliando os danos sofridos pela vítima.

3.5 ENTENDIMENTO DOUTRINÁRIO SOBRE *DEEPPFAKES* E DANOS DIGITAIS

Como se trata de uma nova problemática, a doutrina ainda está em processo de consolidação, mas há consenso de que essa tecnologia representa um novo desafio para o Direito, pois se trata de uma tecnologia que amplia o alcance das violações aos direitos inerentes à pessoa humana, exigindo releitura dos institutos tradicionais da responsabilidade civil.

Conforme adverte Pinheiro (2021, p. 112), “A manipulação de dados e imagens por inteligência artificial exige uma atualização da interpretação jurídica, pois o dano digital pode ser instantâneo, massivo e de difícil reversão”, destacando, também, que o ambiente digital potencializa o chamado efeito multiplicador do dano, tornando a reparação mais complexa.

Dessa perspectiva, diversos autores entendem que os danos digitais ultrapassam a concepção tradicional de lesão patrimonial, atingindo diretamente direitos existenciais e a própria dignidade da pessoa humana. Segundo Pinheiro (2021, p. 113), a dificuldade de reversão dos danos digitais decorre da replicabilidade dos conteúdos, da permanência das informações nos ambientes virtuais e da multiplicação exponencial dos meios de compartilhamento. Diferentemente das ofensas convencionais, os danos digitais apresentam caráter amplificado e permanente, uma vez que os conteúdos podem ser replicados indefinidamente em redes sociais, plataformas digitais e aplicativos de mensagens.

3.6 JURISPRUDÊNCIA BRASILEIRA SOBRE MANIPULAÇÃO DIGITAL E VIOLAÇÃO DE IMAGEM

A jurisprudência brasileira, embora ainda precária quanto aos *deepfakes*, apresenta entendimento consolidado sobre a responsabilização por uso indevido de imagem e conteúdos ofensivos na internet. Os tribunais têm reconhecido que a divulgação de conteúdo ofensivo gera dano moral presumido; a liberdade de expressão não autoriza ofensas à honra; a responsabilidade do provedor depende do descumprimento de ordem judicial.

Além disso, o Superior Tribunal de Justiça consolidou o entendimento de que o dano moral, especialmente nas hipóteses capazes de gerar constrangimento, exposição vexatória ou abalo à reputação da vítima, prescinde de comprovação específica do prejuízo, por ser considerado presumido (*in re ipsa*). Nesse sentido, a Súmula 403 do STJ estabelece que “independe de prova do prejuízo a indenização pela publicação não autorizada da imagem de pessoa com fins econômicos ou comerciais” (BRASIL, 2009). Tal entendimento mostra-se particularmente relevante nos casos envolvendo *deepfakes*, pois a manipulação artificial da imagem frequentemente produz danos à reputação da vítima independentemente da demonstração de prejuízo econômico concreto.

Em relação às plataformas digitais, o STJ tem reconhecido a importância da remoção rápida de conteúdos ofensivos, especialmente em demandas que envolvem a violação da esfera existencial da pessoa humana, admitindo a concessão de tutela de urgência para impedir a continuidade ou ampliação do dano. Nesse contexto, aplica-se de forma reiterada o art. 19 do Marco Civil da Internet, segundo o qual os provedores somente poderão ser responsabilizados civilmente caso deixem de cumprir ordem judicial específica destinada à retirada do conteúdo ilícito.

A tendência jurisprudencial também pode ser observada no Processo nº 0000868-06.2024.8.17.3520, julgado pelo Tribunal de Justiça de Pernambuco, no qual foi reconhecida a ocorrência de dano moral decorrente da utilização de tecnologia *deepfake* para manipulação vexatória da imagem do autor.

4. ESTUDO DE CASO: RESPONSABILIDADE CIVIL DECORRENTE DE DEEPPFAKE

4.1 APRESENTAÇÃO DO CASO ANALISADO

O presente estudo de caso analisa o processo nº 0000868-06.2024.8.17.3520, julgado pelo Poder Judiciário do Estado de Pernambuco, na Vara Única da Comarca de Triunfo/PE. A demanda foi proposta por L. F. D. S., então prefeito do município de Triunfo/PE, em face de G. F. A. e da empresa B. B. T. L., responsável pela plataforma digital TikTok.

A ação consistiu em Ação de Obrigação de Fazer cumulada com pedido de indenização por danos morais, em razão da divulgação de um vídeo produzido com tecnologia de geração artificial, no qual a imagem do autor teria sido manipulada de forma considerada ofensiva ou difamatória.

Segundo os autos, o vídeo foi publicado na rede social TikTok pela primeira ré e apresentava uma montagem digital em que o autor aparecia dançando de forma ridicularizada, acompanhada de trilha sonora com conteúdo de conotação sexual e ofensiva. A publicação também continha legenda crítica à atuação administrativa do autor como prefeito.

Diante disso, o autor alegou violação aos seus direitos da personalidade, especialmente à honra e à imagem, requerendo a remoção do conteúdo e indenização por danos morais no valor de R\$10.000,00.

4.2 CONTEXTUALIZAÇÃO JURÍDICA DO CASO

O litígio do caso envolve o conflito entre liberdade de expressão e direitos da personalidade, especialmente quando há utilização de tecnologias digitais que manipulam a imagem de terceiros.

A Constituição Federal de 1988 garante a proteção à honra, à imagem e à dignidade da pessoa humana, conforme previsto no art. 5º, incisos V e X, assegurando o direito à indenização por danos decorrentes de sua violação.

Entretanto, também é assegurada a liberdade de manifestação do pensamento e de expressão, conforme disposto no art. 5º, inciso IV, da Constituição. Todavia, esse direito não é absoluto, devendo ser exercido de maneira razoável dentro dos limites estabelecidos pelo ordenamento jurídico.

No caso analisado, a discussão judicial apresenta três pontos principais: a utilização indevida da imagem do autor por meio de tecnologia *deepfake*; os limites da liberdade de expressão em críticas dirigidas a agentes públicos; a responsabilidade civil da plataforma digital pelo conteúdo publicado por usuários.

4.3 ANÁLISE DA CONDUTA E DA UTILIZAÇÃO DE *DEEPPFAKE*

O magistrado reconheceu durante a análise do mérito que o vídeo publicado pela primeira ré foi produzido mediante utilização de tecnologia *deepfake*, na qual permitiu a manipulação da imagem do autor para criar uma situação fictícia.

No vídeo, o autor foi retratado dançando de forma considerada vexatória, com a legenda criticando a gestão pública do autor. Embora críticas a agentes públicos sejam consideradas legítimas em uma sociedade democrática, o magistrado entendeu que houve extrapolação dos limites da liberdade de expressão. Assim, segundo a fundamentação da sentença, a manipulação da imagem do autor, associada a conteúdo ofensivo e sexualizado, configura uso indevido da imagem, caracterizando violação aos direitos da personalidade, reforçando a concepção de Diniz (2023) acerca da tutela ampla dos atributos da personalidade, especialmente da imagem e da honra.

Além disso, outro aspecto considerado pela juíza foi o alcance da publicação, na qual atingiu aproximadamente 27 mil visualizações, evidenciando o efeito multiplicador e ampliando a repercussão do conteúdo e os danos à imagem do autor.

4.4 RESPONSABILIDADE CIVIL DAS PARTES ENVOLVIDAS

No julgamento do caso, o magistrado diferenciou a responsabilidade entre as duas rés. A requerida **G. F. A.**, responsável pela publicação do vídeo, foi considerada civilmente responsável pelos danos causados ao autor, pois o magistrado entendeu que a utilização de *deepfake* para criar uma representação vexatória da imagem do autor ultrapassou os limites do exercício regular da liberdade de expressão, configurando ato ilícito.

Assim, foi reconhecida a responsabilidade civil da ré, com base nos dispositivos constitucionais e nas normas do Código Civil que protegem os direitos da personalidade. Além disso, foi reconhecido o dano moral presumido (*in re ipsa*), uma vez que a utilização indevida da imagem em contexto vexatório dispensa prova do prejuízo concreto.

Quanto à empresa **B. B. T. L.**, responsável pela plataforma TikTok, o magistrado aplicou as disposições do Marco Civil da Internet (Lei nº 12.965/2014), especialmente o art. 19. De acordo com essa norma, provedores de aplicações de internet somente podem ser responsabilizados civilmente por conteúdo gerado por terceiros caso não cumpram ordem judicial determinando a remoção do conteúdo ilícito.

Como a plataforma cumpriu prontamente a decisão judicial que determinou a remoção do vídeo, não houve resistência ou descumprimento da ordem judicial. Dessa forma, o magistrado concluiu que não houve responsabilidade civil da plataforma digital, afastando o pedido de indenização em relação à empresa.

4.5 DECISÃO JUDICIAL E FIXAÇÃO DA INDENIZAÇÃO

Ao final do julgamento, o magistrado decidiu pela procedência parcial da ação, determinando a manutenção da remoção do vídeo da plataforma TikTok; a condenação da autora da publicação ao pagamento de indenização por danos morais no valor de R\$ 3.000,00; a improcedência do pedido de indenização em

relação à plataforma digital. A decisão mostra consonância com a doutrina de Gonçalves (2023), ao reconhecer que a utilização indevida da imagem em situação vexatória gera dano moral presumido.

Na fixação do valor da indenização, o magistrado considerou diversos critérios, entre eles: a gravidade da ofensa; a ampla repercussão do conteúdo; a condição de agente público do autor; a situação econômica da ré, assistida pela Defensoria Pública; e o caráter pedagógico da indenização.

Dessa forma, o valor inicialmente pleiteado pelo autor (R\$10.000,00) foi reduzido para R\$3.000,00, em atenção aos princípios da razoabilidade e proporcionalidade.

4.6 RELEVÂNCIA DO CASO PARA O ESTUDO DA RESPONSABILIDADE CIVIL POR *DEEPPFAKES*

O caso analisado possui valor elevado para o debate jurídico sobre o uso de tecnologias de IA na manipulação de imagens. A decisão demonstra que, mesmo diante de novas tecnologias como os *deepfakes*, o ordenamento jurídico brasileiro possui instrumentos capazes de proteger os direitos da personalidade.

Sob a perspectiva doutrinária, o caso evidencia a atualidade das reflexões de Diniz (2023) acerca da proteção dos atributos da personalidade e confirma a preocupação de Pinheiro (2021) quanto ao efeito multiplicador dos danos digitais decorrentes da ampla circulação de conteúdos ilícitos na internet.

Além disso, o caso evidencia a necessidade de equilíbrio entre liberdade de expressão e proteção à honra e à imagem, especialmente quando se trata de conteúdos manipulados digitalmente. Por fim, o julgamento também reforça o papel do Marco Civil da Internet na delimitação da responsabilidade das plataformas digitais, estabelecendo critérios específicos para a responsabilização de provedores por conteúdos produzidos por terceiros.

5. CONCLUSÃO

O desenvolvimento das ferramentas de manipulação digital de imagem trouxe benefícios significativos para diversos setores da sociedade, como nas áreas da comunicação, entretenimento e inovação tecnológica. Entretanto, ao longo deste trabalho, verificou-se que o uso indevido de tecnologias de IA representa uma nova forma de agressão à honra, à privacidade, à dignidade e à reputação das vítimas. Diferentemente das formas tradicionais de exposição indevida, os *deepfakes* possuem elevado potencial ofensivo em razão de sua aparente autenticidade, dificultando a identificação da falsidade e ampliando os danos sociais, psicológicos e patrimoniais suportados pela vítima.

No ordenamento jurídico brasileiro, embora ainda não exista legislação específica voltada exclusivamente à regulamentação dos sistemas de geração artificial, observou-se, por meio do estudo de caso, que a Constituição Federal, o Código Civil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados oferecem instrumentos jurídicos parcialmente capazes de fundamentar a responsabilização civil decorrente dessas práticas, permitindo a reparação dos danos causados pela representação digital ilícita e fraudulenta da imagem e da identidade.

Além disso, a jurisprudência brasileira tem demonstrado preocupação com a proteção da imagem e da honra no ambiente digital, reconhecendo a necessidade de rápida remoção de conteúdos ofensivos e a possibilidade de responsabilização dos envolvidos. O entendimento consolidado pelo STJ acerca do dano moral presumido em casos de uso indevido da imagem reforça a importância da proteção jurídica da personalidade diante das novas tecnologias.

Também se constatou a exigência de uma atuação conjunta do Estado, das plataformas digitais, da sociedade e da comunidade científica. A velocidade da disseminação de conteúdos manipulados evidencia a necessidade de mecanismos mais eficientes de prevenção, identificação e remoção dessas mídias, bem como o fortalecimento de políticas de educação digital e conscientização social sobre os riscos da desinformação tecnológica.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Brasília, DF: Presidência da República, 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil**. Brasília, DF: Presidência da República, 2002.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília, DF: Presidência da República, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 16. ed. São Paulo: Atlas, 2023.

CHESNEY, Robert; CITRON, Danielle Keats. Deep fakes: a looming challenge for privacy, democracy, and national security. **California Law Review**, Berkeley, v. 107, n. 6, p. 1753-1819, 2019.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro: teoria geral do direito civil**. 40. ed. São Paulo: SaraivaJur, 2023. v. 1.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

GONÇALVES, Carlos Roberto. **Responsabilidade civil**. 18. ed. São Paulo: SaraivaJur, 2023. v. 4.

MIRAGEM, Bruno. **Responsabilidade civil digital e proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2021.

PERNAMBUCO. Tribunal de Justiça de Pernambuco. Vara Única da Comarca de Triunfo. **Processo n. 0000868-06.2024.8.17.3520**. Triunfo, PE, 2024. Disponível em: <<https://www.jusbrasil.com.br/processos/730849797/processo-n-000XXXX-0620248173520-do-tjpe>>. Acesso em: 19 fev. 2026.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: SaraivaJur, 2021.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: a modern approach**. 4. ed. Hoboken: Pearson, 2021.