

UNIVERSIDADE CESUMAR - UNICESUMAR
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

***DEEPPAKES E DIREITOS DA PERSONALIDADE: VIOLAÇÃO À HONRA,
IMAGEM E PRIVACIDADE NA ERA DIGITAL***

FELIPE DE SOUZA ESMERALDO

MARINGÁ – PR

2025

FELIPE DE SOUZA ESMERALDO

***DEEPFAKES E DIREITOS DA PERSONALIDADE: VIOLAÇÃO À HONRA,
IMAGEM E PRIVACIDADE NA ERA DIGITAL***

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em Direito sob a orientação da Prof. Dra. Mayume Caires Moreira.

MARINGÁ – PR

2025

FOLHA DE APROVAÇÃO
FELIPE DE SOUZA ESMERALDO

**DEEPPAKES E DIREITOS DA PERSONALIDADE: VIOLAÇÃO À HONRA,
IMAGEM E PRIVACIDADE NA ERA DIGITAL**

Artigo apresentado ao Curso de Graduação em Direito da Universidade Cesumar –
UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em Direito,
sob a orientação da Prof. Dr. Mayume Caires Moreira.

Aprovado em: ____ de _____ de ____.

BANCA EXAMINADORA

Nome do professor – (Titulação, nome e Instituição)

Nome do professor - (Titulação, nome e Instituição)

Nome do professor - (Titulação, nome e Instituição)

DEEPPAKES E DIREITOS DA PERSONALIDADE: VIOLAÇÃO À HONRA, IMAGEM E PRIVACIDADE NA ERA DIGITAL

Felipe de Souza Esmeraldo

RESUMO

O presente trabalho analisa os impactos da tecnologia *deepfake* sobre os direitos da personalidade, investigando as violações à honra, imagem e privacidade no contexto digital. A metodologia emprega a revisão bibliográfica e documental, com abordagem qualitativa, para examinar a dualidade da tecnologia, que abrange de usos legítimos a ilícitos, como a desinformação e a violência de gênero. A análise revela que, embora o ordenamento jurídico brasileiro possua uma robusta base protetiva fundamentada na dignidade humana, seus mecanismos tradicionais de reparação são desafiados pela escala e permanência do dano online. Discutem-se as respostas regulatórias internacionais e as inovações na legislação nacional, como o agravamento de penas para a violência psicológica praticada com inteligência artificial. Conclui-se que a proteção efetiva demanda uma abordagem jurídica híbrida, que combine a punição individual com a responsabilização preventiva das plataformas digitais para mitigar os riscos dessa nova modalidade de agressão.

Palavras-chave: Inteligência Artificial. Proteção de Dados. Responsabilidade Civil.

DEEPPAKES AND PERSONALITY RIGHTS: VIOLATION OF HONOR, IMAGE AND PRIVACY IN THE DIGITAL AGE

ABSTRACT

This paper analyzes the impacts of *deepfake* technology on personality rights, investigating violations of honor, image, and privacy in the digital context. The methodology employs a bibliographic and documentary review with a qualitative approach to examine the technology's duality, which ranges from legitimate uses to illicit applications, such as disinformation and gender-based violence. The analysis reveals that while the Brazilian legal framework has a robust protective foundation based on human dignity, its traditional reparation mechanisms are challenged by the scale and permanence of online harm. It discusses international regulatory responses and innovations in national legislation, such as increased penalties for psychological violence committed with artificial intelligence. It is concluded that effective protection requires a hybrid legal approach, combining individual punishment with the preventive accountability of digital platforms to mitigate the risks of this new form of aggression.

Keywords: Artificial Intelligence. Civil Liability. Data Protection.

SUMÁRIO

1 INTRODUÇÃO	5
2 DESENVOLVIMENTO	6
2.1 CONCEITOS E FUNDAMENTOS DOS DEEPFAKES	6
2.1.1 Inteligência Artificial, Redes Neurais Generativas (GANs) e a criação de DeepFakes	6
2.1.2 Usos legítimos e ilegítimos dos Deepfakes	8
2.2 O DESAFIO JURÍDICO TRANSNACIONAL DOS DEEPFAKES	12
2.2.1. A anatomia do dano: o impacto jurídico de casos internacionais de repercussão .	12
2.2.2. Estratégias de enfrentamento no direito comparado: da punição à regulação	14
2.3 AS VIOLAÇÕES CAUSADAS AOS DIREITOS DA PERSONALIDADE PELOS DEEPFAKES.....	17
2.3.1. Conceito, características e tutela dos direitos da personalidade no Brasil	17
2.3.2. A violação da honra, imagem, privacidade e proteção de dados pessoais	20
3 CONCLUSÃO	24
REFERÊNCIAS.....	25

1 INTRODUÇÃO

A ascensão da Era Digital, impulsionada pela onipresença da internet e pela capacidade de processamento massivo de dados, reconfigurou as interações sociais e inaugurou uma nova fronteira para o Direito. Nesse cenário, a inteligência artificial (IA) deixou de ser um conceito de ficção científica para se tornar uma força motriz de inovação, cuja capacidade de gerar conteúdo sintético ultrarrealista, conhecido como *deepfake*, representa uma das mais disruptivas tecnologias contemporâneas. A facilidade de criação e a velocidade de disseminação viral desses materiais audiovisuais manipulados colocam em xeque a própria noção de verdade e autenticidade, gerando um profundo tensionamento com os direitos fundamentais da pessoa humana.

O problema central que norteia esta pesquisa reside na vulnerabilidade dos direitos da personalidade, como a honra, a imagem, a privacidade e a autodeterminação informativa, diante da utilização maliciosa dos *deepfakes*. A tecnologia, que pode ser empregada para fins legítimos no entretenimento ou na educação, tornou-se uma arma potente para a prática de atos ilícitos, como a criação de pornografia não consensual, a difusão de desinformação política, a perpetração de fraudes e a prática de violência psicológica. Diante dessa realidade, surge a questão: o arcabouço jurídico brasileiro, concebido em uma era pré-digital, está adequadamente preparado para responder à complexidade, à escala e à permanência dos danos causados por esta nova forma de violação?

A relevância do tema é inquestionável e urgente. Casos de grande repercussão internacional e nacional demonstram que os danos transcendem a esfera individual, ameaçando a estabilidade de processos democráticos, a segurança patrimonial e, de forma mais contundente, a dignidade de grupos vulneráveis, especialmente mulheres. A necessidade de compreender e estruturar respostas jurídicas eficazes é, portanto, um imperativo para a proteção da pessoa e a manutenção da confiança no ambiente digital.

Assim, o objetivo geral deste trabalho é analisar as formas de violação dos direitos da personalidade pela tecnologia *deepfake* e discutir a adequação das respostas do ordenamento jurídico brasileiro para prevenir e reparar tais danos. Para conduzir esta análise, adotou-se como metodologia a revisão bibliográfica e documental, com abordagem qualitativa e baseada no método hipotético-dedutivo. A pesquisa debruça-se sobre uma gama diversificada de fontes, incluindo artigos acadêmicos, legislação nacional e estrangeira, doutrina jurídica e o estudo de casos concretos de grande repercussão, a fim de fundamentar a discussão sobre os impactos da tecnologia nos direitos da personalidade.

Para alcançar os fins propostos, o artigo foi estruturado em três seções principais. Inicialmente, são explorados os conceitos e fundamentos dos *deepfakes*, detalhando a tecnologia de Redes Neurais Generativas Adversariais (GANs) e a dualidade de seus usos legítimos e ilegítimos. Em seguida, examina-se o desafio jurídico transnacional, analisando as estratégias de enfrentamento punitivas e regulatórias adotadas no direito comparado. Por fim, a análise se aprofunda no contexto brasileiro, dissecando a tutela conferida pelos direitos da personalidade e a forma como a honra, a imagem, a privacidade e os dados pessoais são vulnerados, culminando na avaliação das recentes inovações legislativas sobre o tema.

2 DESENVOLVIMENTO

2.1 CONCEITOS E FUNDAMENTOS DOS *DEEPPFAKES*

2.1.1 Inteligência Artificial, Redes Neurais Generativas (GANs) e a criação de *DeepFakes*

A Era Digital consolidou-se como um marco civilizatório que transcende a simples introdução de novas tecnologias, alterando fundamentalmente as estruturas sociais, econômicas e políticas. Essa fase histórica caracteriza-se pela convergência entre a comunicação em rede e o processamento massivo de dados, criando um ambiente no qual a informação e a conectividade são elementos estruturantes do cotidiano. Conforme apontam Bonilla e Oliveira (2011), a circulação instantânea de dados, aliada à interatividade das plataformas digitais, rompe fronteiras geográficas e temporais, conferindo ao espaço virtual o status de uma extensão da esfera pública e privada, com efeitos diretos sobre a identidade e a reputação dos indivíduos.

Nesse cenário, as interações humanas passaram a ser majoritariamente mediadas por ambientes digitais que funcionam como novas arenas sociais e econômicas. Plataformas de redes sociais, aplicativos de mensagens e fóruns online instauram dinâmicas de comunicação e sociabilidade que remodelam as interações tradicionais. Essa mediação, contudo, não é neutra. Como adverte Gonçalves (2022), os algoritmos atuam como curadores de conteúdo, selecionando, classificando e priorizando informações, definindo o que se torna visível ou invisível. Esse processo de curadoria algorítmica fomenta ecossistemas informacionais personalizados que não apenas influenciam percepções e moldam opiniões, mas também redimensionam a própria noção de privacidade.

O ambiente hiperconectado é o motor do fenômeno da dataficação, no qual cada clique, busca ou interação social gera rastros informacionais passíveis de coleta, análise e monetização. A transformação de atividades cotidianas em dados quantificáveis alimenta diretamente os sistemas de aprendizado de máquina (*machine learning*), permitindo a identificação de padrões e a previsão de comportamentos com precisão crescente (Bonilla; Oliveira, 2011). Desse modo, os indivíduos tornam-se, simultaneamente, produtores e objetos de informação, integrando um ciclo em que uma maior participação digital implica uma maior geração de dados, retroalimentando os próprios algoritmos que medeiam suas experiências.

É nesse contexto de vasta disponibilidade de dados e poder computacional que as tecnologias de Inteligência Artificial (IA) surgem como consequência e motor da digitalização. A compreensão de fenômenos como os *deepfakes* requer, portanto, a análise da infraestrutura digital que os sustenta (Gonçalves, 2022). A IA, a partir dessa base, não apenas interpreta a realidade, mas passa a recriá-la, gerando conteúdos sintéticos que tornam a fronteira entre o real e o virtual cada vez mais tênue.

Academicamente, a Inteligência Artificial é definida como um campo da ciência da computação dedicado ao desenvolvimento de agentes inteligentes, ou seja, sistemas capazes de raciocinar, aprender com dados, perceber o ambiente e agir para maximizar suas chances de sucesso em um objetivo específico. Conforme detalham Russell e Norvig (2021), o campo se divide conceitualmente entre a IA Forte, que almeja uma consciência análoga à humana, e a IA Fraca ou Restrita, focada em executar tarefas específicas com alta performance. É no âmbito da IA Fraca que os avanços práticos mais notáveis ocorreram, impulsionados pelo subcampo do aprendizado de máquina, que se beneficia diretamente do crescente volume de dados digitais para aprimorar seu desempenho.

O avanço crucial que permitiu a criação de conteúdo sintético ultrarrealista foi o desenvolvimento das Redes Neurais Generativas Adversariais (*Generative Adversarial Networks* - GANs), em um trabalho seminal de Ian Goodfellow e seus colaboradores (2014). A arquitetura de uma GAN é elegantemente concebida como um jogo competitivo entre duas redes neurais que são treinadas simultaneamente: a rede Geradora (G) e a rede Discriminadora (D). A função do Gerador é criar dados sintéticos – como imagens de rostos – que sejam indistinguíveis de exemplos reais. Em contrapartida, o objetivo do Discriminador é se tornar um especialista em diferenciar os dados autênticos dos falsos, criados pelo Gerador. Essa dinâmica adversarial força ambas as redes a se aprimorarem continuamente.

O processo se inicia com a rede Geradora, que atua como uma espécie de "falsificador". Partindo de um vetor de ruído aleatório, ela tenta transformá-lo em uma saída complexa e

estruturada, como uma imagem. A cada tentativa, o Gerador recebe um feedback do Discriminador, que o informa sobre o quão convincente foi sua criação. Com base nessa avaliação, o Gerador ajusta seus parâmetros internos para produzir resultados cada vez mais realistas, aprendendo progressivamente a capturar as características e a distribuição estatística dos dados reais usados no treinamento (Creswell et al., 2018).

Em oposição, a rede Discriminadora funciona como um "perito" ou "detetive". Trata-se de um classificador treinado com um conjunto de dados que inclui tanto exemplos reais quanto as falsificações produzidas pelo Gerador. Sua única tarefa é analisar uma entrada e determinar a probabilidade de ela ser autêntica. A precisão do Discriminador é fundamental, pois um perito eficaz obriga o falsificador a refinar suas técnicas para conseguir enganá-lo, elevando continuamente o padrão de qualidade das criações sintéticas (Salimans et al., 2016).

A genialidade das GANs reside justamente nessa dinâmica de treinamento competitivo. Goodfellow et al. (2014) descrevem essa relação de forma análoga a um jogo entre um falsificador que tenta criar dinheiro falso e a polícia que tenta detectá-lo; o aprimoramento de um força o aprimoramento do outro. O ciclo de treinamento continua até que o Gerador se torne tão proficiente que o Discriminador não consiga mais diferenciar suas criações das amostras reais, atingindo um ponto de equilíbrio teórico. Nesse processo, como resumem Park, Huh e Kim (2020), o gerador adquire técnicas de síntese cada vez mais sofisticadas, enquanto o discriminador se transforma em um avaliador extremamente preciso. A tecnologia resultante desse processo, quando aplicada para alterar ou criar vídeos e áudios com o propósito de que pareçam autênticos, é denominada *deepfake*.

2.1.2 Usos legítimos e ilegítimos dos *Deepfakes*

Toda tecnologia disruptiva nasce como uma ferramenta desprovida de um propósito inerente, seja ele bom ou mau; é o uso humano que lhe confere um caráter e um valor. Essa concepção, ecoada no pensamento de juristas como Danilo Doneda (2021), aplica-se com perfeição aos *deepfakes*. Eles representam uma tela em branco: de um lado, a promessa de inovações que podem enriquecer a cultura, a educação e o bem-estar; do outro, a sombra de uma arma capaz de ferir reputações, desestabilizar a democracia e causar sofrimento profundo. Analisar essa dualidade não é um mero exercício técnico, mas um exame de consciência sobre os caminhos que escolhemos trilhar com as ferramentas que criamos, sendo um passo fundamental para compreender a complexa tarefa de proteger os direitos da personalidade na era digital.

Na indústria do entretenimento, a tecnologia de manipulação sintética de mídia oferece soluções para dilemas profundamente humanos e logísticos. Um dos exemplos mais emblemáticos ocorreu durante a produção de *Velozes e Furiosos 7*, abalada pelo trágico falecimento do ator Paul Walker em meio às filmagens. O desafio de concluir a obra e, ao mesmo tempo, prestar uma homenagem digna ao legado do ator foi superado com o auxílio da computação gráfica, conforme detalha o portal Terra (2015), incluindo a participação dos irmãos Caleb e Cody Walker como dublês e a recriação digital do rosto de Paul Walker pela Weta Digital. O resultado foi uma delicada fusão entre tecnologia e sensibilidade, que não apenas garantiu a finalização do filme, mas transformou a ferramenta digital em um veículo para o luto e a homenagem, permitindo que o público se despedisse do personagem e do ator. Este caso ilustra como a tecnologia de manipulação de mídia pode ser usada para preservar a arte e a memória, oferecendo um fechamento narrativo e emocional que de outra forma seria impossível.

Expandindo essa visão positiva, a campanha "Malaria Must Die" ("A Malária Deve Morrer") surge como um exemplo paradigmático de como a tecnologia *deepfake* pode ser canalizada para o bem social em escala global. Conforme aponta a análise da Fecomercio SP (2022), o projeto foi muito além de uma simples peça publicitária, transformando-se em um poderoso instrumento de comunicação humanitária. Na campanha, a imagem do ex-jogador David Beckham foi utilizada para veicular um apelo contra a malária em nove idiomas diferentes. A sofisticação da tecnologia permitiu não apenas a tradução da mensagem, mas a sincronização labial perfeita, criando a impressão convincente de que o próprio Beckham falava aquelas línguas. Essa abordagem inovadora superou barreiras linguísticas e culturais, permitindo que um apelo unificado chegasse de forma pessoal e direta a diferentes nações, demonstrando como uma ferramenta frequentemente associada à desinformação pode ser eticamente reconfigurada para promover a conscientização e salvar vidas.

No campo da educação e da cultura, o potencial da tecnologia para criar pontes entre o passado e o presente é notável, permitindo que o público vivencie a arte de maneiras antes inimagináveis. A iniciativa "Dalí Lives", promovida pelo Museu Dalí na Flórida, é um exemplo vívido dessa inovação. Conforme detalhado no comunicado de imprensa da instituição (The Dalí Museum, 2019), o projeto utilizou inteligência artificial para "ressuscitar" o artista. O processo envolveu o treinamento de um algoritmo de aprendizado de máquina com centenas de entrevistas, cartas e filmagens de arquivo, permitindo que a IA aprendesse e replicasse os trejeitos e a personalidade do pintor surrealista. O resultado é um avatar em escala humana que acolhe os visitantes, interage com eles em tempo real, comenta sobre eventos atuais e até posa

para "selfies", transformando a visita ao museu em um diálogo imersivo e inesquecível com o próprio artista.

Essa fronteira de inovação se estende de forma particularmente intrigante à área da saúde mental, onde a tecnologia *deepfake* começa a ser explorada como uma ferramenta terapêutica. Em um estudo aprofundado sobre o tema, Hoek et al. (2025) analisam o potencial da chamada "*deepfake therapy*". Uma das aplicações mais promissoras, segundo os autores, seria no tratamento do luto, onde *deepfakes* interativos de entes queridos falecidos poderiam ser criados para permitir "conversas póstumas". Essa simulação controlada poderia ajudar os pacientes a processar a perda e a se despedir de uma maneira que antes era impossível. Adicionalmente, a tecnologia poderia ser empregada em terapias de exposição para fobia social, permitindo que os pacientes interajam com avatares realistas em cenários seguros e customizáveis. Trata-se de um uso que, embora eticamente complexo, coloca a sofisticação da IA a serviço direto do bem-estar psicológico.

Em violento contraste, o uso malicioso de *deepfakes* representa uma das mais insidiosas ameaças contemporâneas, sendo a pornografia não consensual sua manifestação mais devastadora. Em sua análise sobre a necessidade de um modelo de criminalização para a prática, Rodrigues (2023) a caracteriza não como um mero ilícito contra a honra, mas como uma modalidade de violência sexual que atenta contra a dignidade e a liberdade sexual da vítima. O autor argumenta que, ao inserir a imagem de uma pessoa em um contexto sexualizado sem seu consentimento, o agressor usurpa sua identidade e a submete a uma violação que é "permanente e replicável" no ambiente digital. O dano transcende a tela, provocando um profundo abalo psicológico, o estigma social e a destruição da reputação. A viralização do conteúdo, segundo o autor, agrava a agressão, tornando a vítima prisioneira de uma "execução pública digital" que se multiplica a cada compartilhamento.

Na arena política, o *deepfake* deixa de ser uma ferramenta de entretenimento para se tornar uma arma de desinformação, com potencial para corroer os alicerces da própria democracia. A ameaça não é hipotética; ela reside na possibilidade real de um vídeo falso, mostrando um candidato em uma situação comprometedora, viralizar às vésperas de uma eleição e influenciar o voto do cidadão com base em uma mentira. Reconhecendo esse risco, o Tribunal Superior Eleitoral (TSE) agiu de forma preemptiva ao editar a Resolução nº 23.732/2024. A norma estabeleceu, primeiramente, um dever de transparência para o uso de qualquer conteúdo sintético, buscando alertar o eleitor sobre a natureza do material. Conforme o Art. 9º-B da referida resolução:

Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons impõe ao responsável pela propaganda o dever de informar, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada. (BRASIL, 2024)

Indo além da obrigação de rotular, a Justiça Eleitoral impôs uma vedação expressa ao uso de conteúdo manipulado para a disseminação de inverdades, visando proteger a integridade do processo eleitoral, como prevê o Art. 9º-C. De forma ainda mais específica e contundente, a norma proibiu categoricamente o uso de *deepfakes* com o intuito de manipular a imagem ou a voz de pessoas, mesmo que ficcionais, para fins de propaganda. O parágrafo primeiro deste artigo é o cerne da proteção contra a usurpação de identidade para fins eleitorais, estabelecendo uma proibição inequívoca de seu uso malicioso:

Art. 9º-C. É vedada a utilização, na propaganda eleitoral, qualquer que seja sua forma ou modalidade, de conteúdo fabricado ou manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral.

§ 1º É proibido o uso, para prejudicar ou para favorecer candidatura, de conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia (*deep fake*). (BRASIL, 2024)

Na esfera patrimonial, os criminosos têm explorado as tecnologias emergentes para criar golpes de engenharia social cada vez mais sofisticados. Um exemplo alarmante é a chamada "fraude de CEO", que atingiu um novo patamar de complexidade em um incidente envolvendo uma empresa multinacional em Hong Kong. Conforme detalhado em reportagem da Forbes Brasil (2024), golpistas utilizaram *deepfakes* para recriar digitalmente o diretor financeiro da empresa, induzindo um funcionário do setor financeiro a transferir mais de US\$ 25 milhões. O diferencial desse golpe não foi apenas o uso de um *deepfake* de áudio, mas a simulação de uma videoconferência inteira, na qual o golpista se passava pelo diretor financeiro e contava com a "presença" de avatares digitais de outros funcionários, também criados por inteligência artificial. Essa tática de criar uma reunião de grupo falsa foi crucial para dissipar as suspeitas iniciais da vítima, que, ao ver rostos familiares, acreditou na legitimidade da ordem. O caso expõe a evolução do crime, que agora explora a dinâmica da confiança coletiva para criar uma ilusão perfeita, resultando em prejuízos financeiros massivos.

Finalmente, para além dos grandes esquemas, os *deepfakes* tornaram-se uma ferramenta cotidiana para o assédio e a vingança social, manifestando-se como uma nova faceta da violência digital. Na análise de Vieira (2025), essa tecnologia representa "o novo rosto da opressão contra mulheres", sendo utilizada não apenas para ataques aleatórios, mas como um instrumento de silenciamento e controle. A autora argumenta que a criação de conteúdos falsos e vexatórios, que minam a credibilidade e a reputação, é uma forma de perpetuar a violência de gênero no ambiente digital, visando afastar as mulheres do debate público e de posições de destaque. Este ataque sistemático à honra e à imagem configura uma agressão que, segundo a autora, busca a aniquilação moral da vítima, representando uma grave violação aos direitos da personalidade e infligindo uma violência psicológica cujas cicatrizes são profundas e, por vezes, permanentes.

2.2 O DESAFIO JURÍDICO TRANSNACIONAL DOS *DEEPFAKES*

2.2.1. A anatomia do dano: o impacto jurídico de casos internacionais de repercussão

Partindo da dualidade de usos dos *deepfakes*, que transitam entre o entretenimento e a manipulação maliciosa, a análise de seu impacto jurídico torna-se imperativa. Os casos de repercussão internacional, nesse contexto, funcionam como verdadeiros laboratórios para a dissecação da natureza e da escala do dano jurídico provocado por essa tecnologia. Eles não apenas ilustram o potencial destrutivo das criações sintéticas, mas expõem, de forma contundente, a insuficiência dos arcabouços legais tradicionais para lidar com a velocidade, o alcance e, sobretudo, a permanência da violência digital. Os *deepfakes* constituem uma ameaça emergente de escala global, com potencial de desestabilizar a política e a vida privada de indivíduos, conforme discutido por Schick (2020).

O recente ataque coordenado contra a artista Taylor Swift, por meio da disseminação massiva de imagens pornográficas sintéticas, evidencia os desafios da proteção da dignidade na era viral. Conforme relatado por Saner (2024), o episódio transcende o ataque a uma figura pública e exemplifica o impacto negativo da pornografia não consensual sobre mulheres em posições de destaque, mostrando como a viralização rápida dificulta a remoção efetiva do conteúdo pelas plataformas digitais. Nesta análise, entende-se que tais ataques configuram uma forma de violência de gênero digital e de objetificação sexual em escala industrial, interpretando os efeitos sociais e psicológicos que a autora do artigo não detalha explicitamente. Além disso, Sturges (2024) destaca que as lacunas legais existentes nos Estados Unidos contribuem para a

perpetuação dos danos à imagem, à honra e à privacidade das vítimas, reforçando a necessidade de respostas jurídicas que superem a simples reparação, garantindo a proteção efetiva dos bens jurídicos vulnerados.

A análise aprofundada do caso evidencia a inadequação de tipos penais tradicionais, como difamação e injúria, concebidos para um paradigma de dano interpessoal e de escala limitada. Jacobsen (2024) observa que a natureza do ilícito gerado por um *deepfake* pornográfico não consensual é distinta e mais complexa, configurando uma usurpação da identidade da vítima. Nesta análise, entende-se que tais ataques representam uma forma de violência simulada, que ataca a autodeterminação da vítima sobre seu corpo e sua representação pública, interpretando os efeitos sociais e psicológicos que o artigo não detalha explicitamente. Além disso, Van der Sloot e Wagenveld (2022) destacam que os mecanismos jurídicos tradicionais são insuficientes para lidar com os danos causados, justificando a necessidade de respostas preventivas que superem a simples compensação financeira.

Em um espectro distinto de dano, o *deepfake* que simulou a rendição do presidente ucraniano Volodymyr Zelenskyy no início do conflito com a Rússia expôs a vulnerabilidade da fé pública e da segurança nacional. Neste caso, o bem jurídico tutelado transcende a esfera individual e atinge o coração da ordem democrática e da confiança nas instituições. Conforme reportado por Pearson e Zinets (2022), o vídeo, embora rudimentar e rapidamente desmentido, gerou preocupação sobre possíveis desinformações de maior alcance. Nesta análise, entende-se que o episódio funcionou como um ato hostil de guerra informacional, com potencial de semear o caos, desmoralizar tropas e manipular a opinião pública global. Busch (2023) reforça que a utilização de *deepfakes* nesse contexto representa uma forma de ataque à soberania estatal, mostrando como a desinformação pode ser instrumentalizada como arma para minar a estabilidade política.

A análise comparada desses emblemáticos casos permite, portanto, sintetizar os danos provocados por *deepfakes* em, pelo menos, duas categorias macro: a permanência da violação individual, que ataca a dignidade e a identidade de forma quase indelével, e a ameaça sistêmica à confiança coletiva, que corrói os alicerces da fé pública e da estabilidade democrática (Helmus et al., 2022). Ambos os cenários demonstram que as ferramentas jurídicas existentes, focadas em reparar danos passados e de alcance limitado, são insuficientes para conter uma tecnologia que opera na velocidade da luz e cujo dano se perpetua. Diante deste diagnóstico, que demonstra a insuficiência das ferramentas jurídicas preexistentes para lidar com um dano tão profundo e multifacetado, como os ordenamentos jurídicos ao redor do mundo começaram a se estruturar para responder a este desafio? As estratégias adotadas serão o objeto de análise a seguir.

2.2.2. Estratégias de enfrentamento no direito comparado: da punição à regulação

A rápida proliferação de casos de *deepfakes* e a constatação da insuficiência dos aparatos jurídicos tradicionais provocaram uma demanda global por inovação legislativa. A resposta internacional, porém, não tem sido uniforme. Segundo relatório da GLOBSEC (2024), é possível identificar duas correntes predominantes: uma vertente punitiva, que busca criminalizar de forma específica os atos de criação e disseminação de *deepfakes* maliciosos, e uma vertente regulatória, voltada à mitigação de riscos sistêmicos e à proteção da confiança coletiva. A partir dessa base, compreende-se que tais estratégias refletem diferentes filosofias de intervenção jurídica, oscilando entre a repressão do dano consumado e a prevenção de sua ocorrência em massa.

A abordagem punitiva ancora-se na premissa de que a criação e disseminação não consensual de *deepfakes*, sobretudo os de natureza pornográfica ou difamatória, configuram uma violação severa da dignidade, da identidade, da privacidade e da liberdade sexual. Kira (2024) evidencia como tais conteúdos perpetuam o trauma das vítimas no ambiente digital, reforçando a noção da “permanência da violação individual”. A partir dessa perspectiva, entende-se que a intervenção do Direito Penal se justifica como *ultima ratio*, recurso extremo para a proteção dos bens jurídicos mais sensíveis. Nesse mesmo sentido, McGlynn (2024) argumenta que a criminalização exerce não apenas função retributiva, punindo o ofensor, mas também dissuasória, ao sinalizar socialmente a intolerância estatal frente a esse tipo de conduta e desestimular futuros agressores.

Na prática, a vertente punitiva concretiza-se em legislações que tipificam criminalmente a conduta. O Reino Unido, por meio de seu *Online Safety Act* de 2023, estabelece um crime específico para o compartilhamento de imagens íntimas *deepfake* sem consentimento, inserindo-o em um marco regulatório mais amplo voltado à segurança online (UNITED KINGDOM, 2023). Nos Estados Unidos, a resposta é mais fragmentada, ocorrendo predominantemente em nível estadual. Conforme relata a *National Conference of State Legislatures* (2024), estados como Califórnia, Virgínia e Nova York criminalizaram a criação ou distribuição de pornografia *deepfake* não consensual, tomando o consentimento da pessoa retratada como critério central para a licitude do ato. Além da esfera penal, muitas dessas leis estaduais preveem mecanismos civis que permitem às vítimas buscar reparações financeiras, incluindo *punitive damages* (danos punitivos), com o objetivo de punir exemplarmente os ofensores e desestimular condutas semelhantes. Nesse sentido, observa-se que a abordagem

punitiva combina tanto a função retributiva quanto a dissuasória do Direito Penal, tentando abarcar os múltiplos impactos da violação individual causada pelos *deepfakes*.

Em contrapartida, a vertente regulatória parte de um diagnóstico distinto. Embora não negue a gravidade do dano individual, ela concentra-se na “ameaça sistêmica à confiança coletiva” que a proliferação de *deepfakes* representa para a democracia, o discurso público e a própria noção de verdade. Marushchak et al. (2025) destacam que essa corrente não busca punir primariamente o criador individual, mas criar um ecossistema digital mais seguro e transparente, promovendo uma espécie de “higiene informacional”. O enfoque desloca-se do agente para a estrutura, mirando plataformas de disseminação e desenvolvedores de tecnologia. Sob essa perspectiva, entende-se que a prevenção em escala deve impor obrigações que dificultem a viralização de conteúdo sintético malicioso e empoderem os usuários a distinguir o real do fabricado, antes mesmo que a violação individual se consolide, como previsto no *Artificial Intelligence Act* da União Europeia (EUROPEAN UNION, 2021).

O exemplo mais avançado e abrangente da vertente regulatória encontra-se na União Europeia, que adotou uma estratégia legislativa dupla e complementar. Por um lado, o *AI Act* (Lei de Inteligência Artificial) estabelece uma abordagem baseada em risco, impondo obrigações de transparência para sistemas de IA que geram ou manipulam conteúdo sintético, incluindo *deepfakes*, exigindo que estes sejam claramente identificados como artificialmente produzidos, a fim de não induzir o público ao erro (EUROPEAN PARLIAMENT, 2025). Por outro lado, o *Digital Services Act* (DSA) amplia a responsabilidade das grandes plataformas online, as chamadas VLOPs (*Very Large Online Platforms*), que deixam de ser vistas apenas como intermediárias e passam a atuar como agentes responsáveis pela avaliação e mitigação de riscos sistêmicos, como a disseminação de desinformação e conteúdos ilícitos, incluindo *deepfakes* (EUR-LEX, 2022). Observa-se, portanto, que a União Europeia busca combinar transparência, prevenção e responsabilidade corporativa, movendo-se do enfoque punitivo sobre indivíduos para um controle estrutural que previna danos em escala sistêmica.

Interessantemente, observa-se que as fronteiras entre as abordagens punitiva e regulatória tendem a se tornar mais fluidas, revelando uma convergência centrada na corresponsabilização das plataformas digitais. A solução jurídica mais moderna identifica um *duty of care* (dever de cuidado), segundo o qual as empresas de tecnologia devem adotar medidas razoáveis para proteger seus usuários de danos previsíveis. Essa lógica transcende a dicotomia entre punir o indivíduo e regular a tecnologia, ao responsabilizar intermediários que lucram com a disseminação de conteúdo prejudicial. O *Online Safety Act* do Reino Unido exemplifica essa fusão: além de criminalizar determinadas condutas individuais, impõe

rigorosos deveres às plataformas para que removam conteúdo ilegal de maneira diligente (UNITED KINGDOM, 2023). De forma similar, a Austrália sinalizou sua intenção de adotar modelos legislativos análogos, reforçando a tendência internacional de atribuir um papel central às intermediárias na prevenção de danos online (AP NEWS, 2024).

Apesar dos avanços, ambas as estratégias enfrentam limites e desafios significativos. A via criminal, embora essencial para a reparação simbólica e individual, depara-se com obstáculos práticos consideráveis: a natureza transfronteiriça da internet dificulta a aplicação da lei e a determinação da jurisdição, enquanto o anonimato e o uso de tecnologias de ofuscação tornam a prova de autoria uma tarefa complexa para a persecução penal. Por sua vez, a via regulatória, especialmente no modelo europeu, não está isenta de críticas. Conforme reportado pela Reuters (2025), autoridades norte-americanas, como o presidente da FCC, expressaram preocupação de que a imposição de deveres de moderação de conteúdo pelas plataformas possa levar à censura privada e ao cerceamento de discursos legítimos. Adicionalmente, Federspiel et al. (2023) destacam que a regulamentação da inteligência artificial e das plataformas digitais deve equilibrar cuidadosamente a proteção contra danos previsíveis com a preservação de direitos fundamentais, como a liberdade de expressão. Nessa perspectiva, observa-se que o equilíbrio entre segurança e liberdade continua sendo o desafio central para legisladores em âmbito global.

Em síntese, o cenário internacional funciona como um verdadeiro “laboratório” de modelos jurídicos, onde diferentes jurisdições experimentam abordagens que vão do estritamente punitivo ao preventivo-regulatório, com soluções híbridas surgindo como a tendência mais promissora. Cada modelo, com suas virtudes e limitações, oferece lições valiosas sobre como equilibrar a proteção de direitos fundamentais, a inovação tecnológica e a manutenção de um espaço cívico saudável. No contexto brasileiro, observa-se um esforço inicial de regulamentação: conforme noticiado pelo Senado Federal (2024), tramita no país projetos de lei que buscam restringir a manipulação de imagens por meio de inteligência artificial. Esse panorama evidencia a necessidade de avaliar criticamente as capacidades e lacunas da legislação nacional, tema que será aprofundado no capítulo seguinte, com o objetivo de compreender como o ordenamento jurídico brasileiro pode se posicionar frente aos desafios globais já identificados.

2.3 AS VIOLAÇÕES CAUSADAS AOS DIREITOS DA PERSONALIDADE PELOS DEEPPFAKES

2.3.1. Conceito, características e tutela dos direitos da personalidade no Brasil

Diante do “laboratório de respostas” regulatórias que se observa no cenário internacional para enfrentar os desafios impostos por tecnologias como os deepfakes, o ordenamento jurídico brasileiro recorre a um alicerce já consolidado para a proteção da pessoa: os direitos da personalidade. Esta categoria jurídica representa a cláusula geral de tutela do ser humano em suas múltiplas dimensões existenciais, encontrando seu fundamento primordial diretamente no texto constitucional. A dignidade da pessoa humana e a inviolabilidade dos direitos existenciais formam o núcleo de proteção da pessoa, conforme positivado nos seguintes dispositivos da Constituição Federal:

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:

[...]

III – a dignidade da pessoa humana;

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X – **são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas**, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988, grifo meu).

Esses mandamentos constitucionais elevam a dignidade a princípio-matriz e especificam a proteção à honra e à imagem, conferindo aos direitos da personalidade o status de direitos fundamentais. Nesse sentido, Andrade (2013) destaca que o enquadramento constitucional garante aplicabilidade imediata e máxima eficácia a esses direitos, tornando-os o principal escudo jurídico do indivíduo contra violações.

Sob a ótica do Direito Civil Constitucional, os direitos da personalidade são conceituados como os direitos subjetivos inerentes ao ser humano, que tutelam os atributos essenciais de sua pessoa, compreendendo as dimensões física, psíquica e moral. Nesse sentido, Moraes (1993) defende que a legislação civil deve ser reinterpretada sob o filtro axiológico da

Constituição, de modo a recentrar a pessoa humana no núcleo do sistema jurídico privado. Na mesma linha, Tepedino (2021) aprofunda a ideia de que os direitos da personalidade não podem ser reduzidos a meras projeções patrimoniais, devendo ser compreendidos como instrumentos de tutela da dignidade humana. Assim, a dimensão moral desses direitos, que abrange honra, imagem, identidade, privacidade e nome, revela-se a mais vulnerável frente à disseminação de *deepfakes*, os quais manipulam precisamente tais atributos para produzir representações falsas, degradantes e potencialmente devastadoras.

A eficácia protetiva desses direitos é reforçada por um conjunto de características jurídicas essenciais, cuja relevância se intensifica no ambiente digital. Conforme o Art. 11 do Código Civil, “os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo seu exercício sofrer limitação voluntária” (BRASIL, 2002). Essa barreira legal é crucial no combate aos *deepfakes*, pois mitiga a validade de consentimentos genéricos ou abusivos para o uso da imagem, impedindo que uma autorização inicial seja desvirtuada para fins ilícitos não contemplados pela manifestação de vontade do titular. São, ademais, imprescritíveis, o que significa que a pretensão de fazer cessar a lesão não se extingue pelo decurso do tempo (ZANINI; QUEIROZ, 2024). Tal característica é vital na internet, onde um conteúdo danoso pode ser repostado e viralizado anos após sua criação, garantindo à vítima o direito perpétuo de buscar a sua remoção. Por fim, são direitos absolutos, ou seja, oponíveis erga omnes (contra todos), o que fundamenta juridicamente a responsabilização não apenas do criador do conteúdo falso, mas também das plataformas digitais que o hospedam e disseminam, solidificando o dever geral de respeito e abstenção de violação aos direitos da personalidade (ANDRADE, 2013).

A proteção conferida pelo ordenamento não se esgota na lista de direitos previstos nos Arts. 11 a 21 do Código Civil. A doutrina e a jurisprudência são pacíficas em afirmar que este é um rol exemplificativo (*numerus apertus*), e não taxativo. Isso significa que, para além da proteção ao corpo, ao nome e à imagem, o sistema jurídico está aberto a tutelar novas manifestações da personalidade que venham a ser ameaçadas pelo avanço tecnológico e social (ANDRADE, 2013). O argumento central reside na existência de uma cláusula geral de tutela da pessoa humana, decorrente diretamente do princípio da dignidade (CASTRO; MASCARENHAS, 2015). Essa cláusula geral confere ao Poder Judiciário a prerrogativa de proteger a vítima de uma violação por *deepfake*, ainda que não exista uma lei específica que tipifique tal conduta, com base na aplicação direta dos princípios constitucionais e das normas abertas do Código Civil, garantindo uma proteção dinâmica e adaptável.

Em face de uma lesão iminente ou já em curso, o Direito brasileiro prioriza a tutela preventiva, buscando evitar o dano ou fazê-lo cessar. O principal instrumento para tal é a tutela inibitória, prevista de forma geral no Código Civil, que dispõe:

Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei

Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau. (BRASIL, 2002).

Com base nesse dispositivo, a vítima de *deepfake* pode se valer de medidas judiciais de urgência para "exigir que cesse a ameaça, ou a lesão", o que se traduz, na prática, na obtenção de uma ordem para que plataformas digitais removam o conteúdo danoso imediatamente. Esse mecanismo processual, frequentemente acompanhado da fixação de multas diárias (*astreintes*) em caso de descumprimento, age diretamente na fonte da disseminação para estancar o prejuízo (ANDRADE, 2013).

Quando a prevenção falha e o dano se consuma, entra em cena a tutela reparatória. Alicerçada no dever geral de indenizar, previsto no Art. 927 do Código Civil, essa tutela impõe àquele que, por ato ilícito, causar dano a outrem, a obrigação de repará-lo (BRASIL, 2002). O amparo à reparação do dano extrapatrimonial, por sua vez, possui status constitucional. A Carta Magna é inequívoca ao garantir a compensação financeira como resposta à violação dos bens mais caros à pessoa, conforme seus incisos V e X do art. 5º, que asseguram o "direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem" e o "direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988)

A compensação pecuniária por danos morais não se destina a “precificar” a dor, mas sim a proporcionar à vítima uma satisfação que atenuie seu sofrimento, ao mesmo tempo em que impõe ao ofensor uma sanção de caráter pedagógico (ANDRADE, 2013), no entanto, no contexto digital, essa medida se revela insuficiente. Uma vez que um *deepfake* é divulgado na internet, sua circulação se torna praticamente irreversível, espalhando-se por múltiplas plataformas e servidores em escala global. Nesses casos, a indenização financeira pode atenuar parcialmente os efeitos do dano, mas não consegue restaurar integralmente a imagem e a honra pulverizadas, evidenciando a necessidade de mecanismos complementares, como a remoção imediata do conteúdo e a adoção de medidas preventivas que impeçam novas violações (CASTRO; MASCARENHAS, 2015).

Em síntese, o ordenamento jurídico brasileiro, alicerçado na Constituição Federal e no Código Civil, oferece um arsenal jurídico teoricamente robusto e multifacetado para a defesa da pessoa humana, combinando ferramentas preventivas, como a tutela inibitória, e reparatórias, como a indenização por danos morais, que formam um sistema abrangente de proteção aos direitos da personalidade. A estrutura legal, dotada de cláusulas gerais e princípios sólidos, permite adaptação às novas formas de violação que surgem com a evolução tecnológica. Contudo, permanece a questão crítica: será que este arsenal, concebido para uma realidade analógica, possui a agilidade e a força necessárias para combater um inimigo assimétrico como os *deepfakes*? A análise específica da vulnerabilidade dos direitos à honra, à imagem e à privacidade diante dessa nova tecnologia será abordada a seguir.

2.3.2. A violação da honra, imagem, privacidade e proteção de dados pessoais

A análise das violações causadas pelos *deepfakes* aos direitos da personalidade exige uma abordagem que parta da estrutura de proteção existente no ordenamento jurídico brasileiro para, então, demonstrar como a tecnologia a desafia. A tutela jurídica da pessoa, consolidada na Constituição Federal e no Código Civil, prevê a reparação por danos morais como um de seus pilares, conforme o art. 5º, incisos V e X, da Constituição (BRASIL, 1988), e os artigos 12 e 186 do Código Civil (BRASIL, 2002). Contudo, em seu estudo sobre o tema, Schreiber, Ribas e Mansur (2020) apontam que a responsabilidade civil tradicional encontra severos limites quando confrontada com a disseminação em massa e a permanência do dano no ambiente digital, questionando a suficiência da tutela meramente reparatória para coibir e compensar as violações perpetradas por *deepfakes*.

O fundamento último de toda a proteção à pessoa no Brasil reside no princípio da dignidade da pessoa humana, consagrado como pilar da República no art. 1º, III, da Constituição Federal (BRASIL, 1988). A partir deste núcleo axiológico, irradiam-se todos os direitos da personalidade. A doutrina contemporânea, como a de Doneda (2021), demonstra que a proteção de dados pessoais deixou de ser compreendida sob uma ótica meramente patrimonial para afirmar-se como extensão da tutela da pessoa. Nesse mesmo sentido, obras como o *Tratado de Proteção de Dados Pessoais* (BIONI et al., 2020) reforçam que a gestão sobre as próprias informações constitui elemento essencial da dignidade na sociedade tecnológica. A partir dessas premissas, pode-se compreender que a manipulação não consentida da imagem e da voz por meio de *deepfakes* representa ofensa direta a este fundamento do Estado de Direito.

Dentre os direitos da personalidade, o direito à imagem é um dos mais diretamente atingidos, pois envolve a projeção pública da identidade de um indivíduo e sua proteção legal. A utilização da imagem de uma pessoa depende de sua autorização, salvo exceções de interesse público, conforme estabelece o Código Civil, em seu Art. 20:

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. (BRASIL, 2002).

No contexto das *deepfakes*, a violação da imagem assume contornos ainda mais graves: a tecnologia permite a criação de representações artificiais verossímeis que atribuem à vítima atos e falas inexistentes, extrapolando o mero uso indevido e afetando a própria percepção pública da pessoa. Affonso (2021) aborda esse fenômeno como uma forma de “reconstrução digital da imagem”, evidenciando os desafios jurídicos de responsabilização das plataformas e a necessidade de estratégias normativas que considerem a natureza persistente e viral do dano no ambiente digital. Assim, a proteção do direito à imagem no contexto das *deepfakes* não se limita à autorização prévia, mas exige uma abordagem mais ampla, capaz de abarcar prevenção, responsabilização e reparação diante de usos tecnológicos que reproduzem a identidade sem consentimento.

A violação da imagem está intrinsecamente ligada à privacidade e à proteção de dados. A Lei Geral de Proteção de Dados Pessoais - LGPD (BRASIL, 2018) estabelece um marco regulatório robusto ao definir que a imagem facial, por ser um dado biométrico, é um "dado pessoal sensível", cujo tratamento exige um regime jurídico mais rigoroso. Nesse contexto, a criação de *deepfakes* sem consentimento representa um uso indevido de dados sensíveis, afetando a autonomia do titular sobre sua própria identidade digital. Doneda (2021) reforça que o cerne da LGPD é assegurar ao titular o poder de controle sobre suas informações, princípio conhecido como autodeterminação informativa, garantindo que a manipulação de seus dados não ocorra sem autorização. Essa perspectiva é ainda respaldada por Bioni et al. (2020), que destacam a necessidade de estratégias jurídicas que combinem prevenção, responsabilização e reparação frente ao uso não consentido de informações pessoais no ambiente digital, como ocorre com *deepfakes*.

A tecnologia *deepfake*, baseada em redes generativas antagônicas (GANs), evoluiu rapidamente, tornando cada vez mais complexa a distinção entre conteúdo real e sintético

(TOLOSANA et al., 2020). As GANs funcionam por meio de duas redes neurais em competição: uma cria conteúdos falsos e outra avalia sua autenticidade, gerando resultados cada vez mais realistas. Pesquisas recentes demonstram uma corrida constante entre os métodos de criação e as ferramentas de detecção dessas mídias (MIRSKY; LEE, 2021). Esse desafio tecnológico global manifesta-se de forma concreta no Brasil: um relatório do Netlab (2024) sobre o período pré-eleitoral de 2024 identificou o uso de *deepfakes* e outras mídias sintéticas para fins de propaganda eleitoral, evidenciando que a tecnologia já se tornou uma ferramenta ativa no cenário informacional do país, com potencial para manipulação e disseminação de desinformação. Esses dados reforçam a necessidade de políticas públicas, regulamentação e mecanismos de responsabilização adaptados ao contexto digital, em especial quando direitos fundamentais, como imagem e privacidade, estão em jogo.

O risco eleitoral representa uma das mais graves ameaças sociais geradas pelos *deepfakes*. As eleições municipais de 2024 no Brasil serviram como um verdadeiro campo de testes para avaliar o impacto dessa tecnologia no debate democrático. Relatórios especializados, como os do DFRLab (2024) e do Netlab (2024), documentaram o uso de conteúdos gerados por inteligência artificial para atacar candidatos e disseminar desinformação em redes sociais e aplicativos de mensagens. Embora a legislação eleitoral tenha sido atualizada para coibir tais práticas, a velocidade de propagação e a dificuldade de moderação desses conteúdos nas plataformas digitais continuam a representar um desafio contínuo à integridade do processo eleitoral, evidenciando a necessidade de mecanismos de prevenção, responsabilização e educação digital.

Além da manipulação política, um dos usos mais nefastos da tecnologia *deepfake* ocorre no âmbito da violência de gênero. A criação de pornografia não consensual e outras formas de manipulação da imagem se tornaram armas de humilhação e violência psicológica, atingindo diretamente a dignidade e a integridade das vítimas. O legislador brasileiro reagiu a este problema por meio do PL 370/2024, transformado na Lei nº 15.123, de 24 de abril de 2025, que alterou o art. 147-B do Código Penal para agravar a pena do crime de violência psicológica contra a mulher quando praticado com o uso de inteligência artificial ou recurso tecnológico que altere imagem ou som da vítima. Como relata Hérica Christian (2025) no site do Senado, a senadora Daniella Ribeiro (PSD-PB) foi relatora da proposta e justificou sua iniciativa afirmando que foi alvo de divulgação de fotos falsas de nudez durante a campanha de 2018, o que motivou a inclusão do agravante tecnológico. Na mesma sessão, a senadora Damares Alves (Republicanos-DF) alertou para os impactos devastadores dessa prática, mencionando

demissão, danos psicológicos e até ideação suicida entre vítimas de *deepfakes*. A nova redação legal estabelece:

Art. 147-B. Causar dano emocional à mulher que a prejudique e perturbe seu pleno desenvolvimento ou que vise a degradar ou a controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, chantagem, ridicularização, limitação do direito de ir e vir ou qualquer outro meio que cause prejuízo à sua saúde psicológica e autodeterminação:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Parágrafo único. A pena é aumentada de metade se o crime é **cometido mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima**. (BRASIL, 2025, grifo meu)

Essa alteração representa um marco no ordenamento jurídico brasileiro, reconhecendo formalmente a IA como vetor de violência de gênero e demonstrando a preocupação legislativa com as formas mais cruéis de utilização tecnológica para fins de abuso. A repercussão internacional também reforça sua relevância: a International Association of Privacy Professionals (IAPP, 2025) destacou a lei como exemplo de inovação legal para coibir violência digital e proteger a integridade psicológica das mulheres. Dessa forma, a legislação não apenas prevê responsabilização, mas também sinaliza a necessidade de políticas preventivas, educação digital e mecanismos de monitoramento para lidar com *deepfakes* e outras tecnologias emergentes.

A perspectiva futura aponta para desafios contínuos na atribuição de responsabilidade. Pinto e Oliveira (2023) analisam as lacunas do ordenamento jurídico brasileiro quanto à responsabilidade civil por conteúdos sintéticos, destacando que a velocidade de propagação e a dificuldade de identificação dos agentes envolvidos tornam a reparação um desafio (PINTO; OLIVEIRA, 2023, p. 430, 439). Nesse contexto, o relatório *Radar Tecnológico: Biometria e Reconhecimento Facial*, elaborado por Cebrian et al. (2024), sinaliza os riscos associados ao uso de tecnologias de manipulação de imagem e som, evidenciando que a proteção de dados e da identidade digital integra o núcleo da tutela dos direitos da personalidade. Assim, mesmo com a implementação de medidas regulatórias e mecanismos de controle tecnológico, a construção de um ecossistema de responsabilização eficaz, capaz de harmonizar a proteção da pessoa humana, a inovação tecnológica e a liberdade de expressão, permanece como um desafio em aberto para o Direito na era digital.

3 CONCLUSÃO

O percurso analítico deste trabalho demonstrou que a tecnologia *deepfake*, nascida dos avanços em inteligência artificial e Redes Neurais Generativas Adversariais, representa uma força de dupla face: ao mesmo tempo que oferece possibilidades inovadoras para o entretenimento, a cultura e a saúde, emerge como uma das mais potentes ferramentas de violação aos direitos da personalidade na Era Digital. A capacidade de criar e disseminar conteúdos audiovisuais sintéticos ultrarrealistas desafia a estabilidade do ordenamento jurídico, cuja estrutura, embora sólida em seus fundamentos, revela-se lenta e, por vezes, insuficiente para conter um dano que opera na velocidade da viralização e se perpetua no ambiente online.

Foi constatado que as violações perpetradas por *deepfakes* não são meras ofensas pontuais, mas agressões multifacetadas que atingem o núcleo da dignidade humana. A pornografia não consensual, a desinformação política, as fraudes financeiras e a violência psicológica são manifestações de um fenômeno que usurpa a identidade, degrada a honra, aniquila a privacidade e trata a imagem como um dado manipulável sem consentimento. O dano, como visto, é profundo, sistêmico e de difícil reparação integral, tornando a tradicional tutela reparatória por danos morais uma medida paliativa, incapaz de restaurar o *status quo ante*.

A análise do direito comparado revelou que as nações buscam responder a este desafio por meio de duas vertentes principais, a punitiva e a regulatória, com uma tendência crescente para modelos híbridos que corresponsabilizam as plataformas digitais. Essa visão internacional oferece um aprendizado crucial: a solução não reside apenas na criminalização da conduta individual, mas na criação de um ecossistema de prevenção que imponha um dever de cuidado aos intermediários que lucram com a circulação de informações.

No Brasil, o arcabouço de proteção aos direitos da personalidade, ancorado na Constituição Federal e no Código Civil, oferece uma base teórica robusta para a defesa da pessoa. A legislação, por meio de cláusulas gerais e da tutela da dignidade, permite uma adaptação a novas formas de agressão. A recente alteração no Código Penal, que agrava a pena para a violência psicológica contra a mulher cometida com uso de IA, representa um avanço legislativo importante e simbólico, ao reconhecer a gravidade do uso da tecnologia como vetor de violência de gênero.

Contudo, apesar desses alicerces, a resposta brasileira ainda é reativa e fragmentada. A proteção efetiva contra os danos causados por *deepfakes* demanda uma evolução para além da punição e da reparação. É imperativo o desenvolvimento de uma regulação abrangente para a

inteligência artificial, que harmonize a proteção de direitos fundamentais com a inovação, e que estabeleça de forma clara a responsabilidade civil das plataformas digitais na moderação e remoção de conteúdos ilícitos. O desafio, portanto, permanece em aberto: construir um sistema jurídico ágil, preventivo e multifacetado, capaz de garantir que, na inevitável tensão entre tecnologia e humanidade, a dignidade da pessoa humana prevaleça.

REFERÊNCIAS

AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 27, n. 1, p. 251-277, jan./mar. 2021. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438>. Acesso em: 24 set. 2025.

ALERTA DEEPFAKE: entenda como empresa de Hong Kong caiu em golpe milionário. **Forbes Brasil**, 5 fev. 2024. Disponível em: <https://forbes.com.br/forbes-tech/2024/02/alerta-deepfake-entenda-como-empresa-de-hong-kong-caiu-em-golpe-milionario/>. Acesso em: 16 set. 2025.

ANDRADE, Fábio S. de. A tutela dos direitos da personalidade no direito brasileiro. **Revista Derecho del Estado**, Bogotá, n. 30, p. 93-124, jan./jun. 2013. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4352267.pdf>. Acesso em: 21 set. 2025.

AP NEWS. Australia will require social media platforms to act to prevent online harm. **AP News**, 18 dez. 2024. Disponível em: <https://apnews.com/article/australia-digital-duty-of-care-bcc626eb7b465738dff3dd06650e8b23>. Acesso em: 18 set. 2025.

ARTIFICIAL INTELLIGENCE ACT. **The AI Act**. [s.d.]. Disponível em: <https://artificialintelligenceact.eu/>. Acesso em: 18 set. 2025.

BIONI, Bruno Ricardo; *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

BONILLA, Maria Helena Silveira; OLIVEIRA, Paulo Cezar Souza de. Inclusão digital: ambiguidades em curso. In: BONILLA, M. H. S.; PRETTO, N. de L. (org.). **Inclusão digital: polêmica contemporânea**. Salvador: EDUFBA, 2011. p. 23-48.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 set. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 21 set. 2025.

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

https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 set. 2025.

BRASIL. **Lei nº 15.123, de 24 de abril de 2025**. Altera o art. 147-B do Código Penal, para agravar a pena do crime de violência psicológica contra a mulher quando praticado com uso de inteligência artificial ou outro recurso tecnológico que altere imagem ou som da vítima. Brasília, DF: Presidência da República. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2025/lei-15123-24-abril-2025-797342-norma-pl.html>. Acesso em: 24 set. 2025.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024**. Dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral nas eleições de 2024. Brasília, DF: TSE, 2024. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em: 16 set. 2025.

BUSCH, E. **The Weaponisation of Deepfakes**. The Hague: International Centre for Counter-Terrorism (ICCT), 2023. Disponível em: <https://icct.nl/publication/the-weaponisation-of-deepfakes/>. Acesso em: 17 set. 2025.

CASTRO, Fabiana M. M. G.; MASCARENHAS, Ana Cristina de S. S. Direitos da personalidade ou direitos da humanidade: fundamentos e implicações. **Revista Eletrônica de Estudos Jurídicos e da Sociedade - UNIFEG**, Artigos Docentes, v. 4, n. 4, 2015. Disponível em: https://www.unifeg.edu.br/revista/artigos-docentes/2015/Fabiana_M._M._Gomes_de_Castro_e_Ana_Cristina_de_S._S.Mascarenhas-Direitos_da_personalidade_ou_Direitos_da_humanidade_fundamentos.pdf. Acesso em: 21 set. 2025.

CEBRIAN, Fabiana S. P. Faraco; *et al.* **Radar Tecnológico: Biometria e reconhecimento facial**. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2024. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf>. Acesso em: 24 set. 2025.

CHIARELLO DE SOUZA PINTO, Felipe; FRANKLIN DE OLIVEIRA, Gabriela. Não acredite em tudo que vê: Deepfake Pornography e responsabilidade civil no ordenamento jurídico brasileiro. **Revista Eletrônica Direito & Política**, Itajaí, v. 18, n. 2, p. 427-451, 2023. Disponível em: <https://periodicos.univali.br/index.php/rdp/article/view/19869>. Acesso em: 24 set. 2025.

CHRISTIAN, Hérica. Senado aprova pena maior por “deepfake” de mulheres para violência psicológica. **Senado Federal**, 19 mar. 2025. Disponível em: <https://www12.senado.leg.br/noticias/audios/2025/03/senado-aprova-pena-maior-por-deepfake-de-mulheres-para-violencia-psicologica>. Acesso em: 24 set. 2025.

CRESWELL, Antonia *et al.* Generative Adversarial Networks: An overview. **IEEE Signal Processing Magazine**, v. 35, n. 1, p. 53-65, jan. 2018. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8253683>. Acesso em: 11 set. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

EUR-LEX. **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)**. Official Journal of the European Union, 2022.

Disponível em: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>. Acesso em: 18 set. 2025.

EUROPEAN PARLIAMENT. **EU AI Act: first regulation on artificial intelligence**. 2025.

Disponível em: <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>. Acesso em: 19 set. 2025.

EUROPEAN UNION. **Artificial Intelligence Act**. Proposal COM(2021) 206 final, 2021.

Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>. Acesso em: 19 set. 2025.

FARRUGIA, Beatriz. Brazil's electoral deepfake law tested as AI-generated content targeted local elections. **DFRLab**, 26 nov. 2024. Disponível em: <https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes/>. Acesso em: 24 set. 2025.

FEDERSPIEL, F.; *et al.* Threats by artificial intelligence to human health and human rights, and the necessity for regulation. **The Lancet Digital Health**, v. 5, n. 6, p. e385-e393, 2023.

Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10186390/>. Acesso em: 19 set. 2025.

GLOBSEC. **Regulating Deepfakes — Global Approaches to Combatting AI-Driven Manipulation**. Policy Paper, 11 dez. 2024. Disponível em: <https://www.globsec.org/what-we-do/publications/regulating-deepfakes-global-approaches-combatting-ai-driven-manipulation>. Acesso em: 19 set. 2025.

GONÇALVES, L. B. B. Tecnologias digitais de informação e comunicação no ensino superior: interatividade e comunicação. **Revista Eletrônica**, 2022.

GONZÁLEZ, Jaime. Como o ator Paul Walker foi 'ressuscitado' para 'Velozes e Furiosos 7'. **Terra**, 3 abr. 2015. Disponível em: <https://www.terra.com.br/diversao/arte-e-cultura/como-o-ator-paul-walker-foi-ressuscitado-para-velozes-e-furiosos-7,dea063009667c410VgnCLD200000b1bf46d0RCRD.html>. Acesso em: 13 set. 2025.

GOODFELLOW, Ian J. *et al.* Generative adversarial nets. In: **Advances in Neural Information Processing Systems**, v. 27, p. 2672-2680, 2014.

HELMUS, Todd C. *et al.* **Artificial Intelligence, Deepfakes, and Disinformation: A Primer**. Santa Monica: RAND Corporation, 2022. Disponível em: <https://www.rand.org/pubs/perspectives/PEA1043-1.html>. Acesso em: 17 set. 2025.

HOEK, S.; METSELAAR, S.; PLOEM, C. *et al.* Promising for patients or deeply disturbing? The ethical and legal aspects of deepfake therapy. **Journal of Medical Ethics**, v. 51, n. 7, p. 481-486, 2025. Disponível em: <https://jme.bmj.com/content/51/7/481>. Acesso em: 16 set. 2025.

IAPP - INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. Brazil enacts AI-focused law to combat psychological violence against women. **IAPP News**, 7 maio

2025. Disponível em: <https://iapp.org/news/a/brazil-enacts-ai-focused-law-to-combat-psychological-violence-against-women>. Acesso em: 24 set. 2025.

JACOBSEN, B. N. The tensions of deepfakes. **New Media & Society**, 2024. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2023.2234980>. Acesso em: 16 set. 2025.

KIRA, B. When non-consensual intimate deepfakes go viral. **Technology in Society**, v. 78, 102717, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364924000906>. Acesso em: 19 set. 2025.

MARUSHCHAK, Anatolii; PETROV, Stanislav; KHOPERIYA, Anayit. Countering AI-powered disinformation through national regulation: learning from the case of Ukraine. **Heliyon**, v. 11, n. 2, e33763, 2025. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11747593/>. Acesso em: 19 set. 2025.

MCGLYNN, C. Pornography, the Online Safety Act 2023 and the need for stronger legal protections. **Feminist Legal Studies**, 2024. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/17577632.2024.2357421>. Acesso em: 20 set. 2025.

MIRSKY, Yisroel; LEE, Wenke. The creation and detection of deepfakes: a survey. **ACM Computing Surveys**, [S. l.], v. 54, n. 1, p. 1-41, 2021. Disponível em: <https://arxiv.org/abs/2004.11138>. Acesso em: 24 set. 2025.

MORAES, Maria Celina Bodin de. A caminho de um Direito Civil Constitucional. **Revista de Direito Civil**, São Paulo, n. 65, p. 21-45, 1993.

NATIONAL CONFERENCE OF STATE LEGISLATURES (NCSL). **Deceptive Audio or Visual Media (“Deepfakes”) — State Legislation**. 2024. Disponível em: <https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation>. Acesso em: 20 set. 2025.

NETLAB (UFRJ). **Lessons from the pre-campaign: the challenge of combating deepfakes in the 2024 elections in Brazil**. Rio de Janeiro: UFRJ, 2024. Disponível em: <https://netlab.eco.ufrj.br/en/post/lessons-from-the-pre-campaign-the-challenge-of-combating-deepfakes-in-the-2024-elections-in-brazil>. Acesso em: 24 set. 2025.

PARK, Sung-Wook; HUH, Jun-Ho; KIM, Jong-Chan. BEGAN v3: avoiding mode collapse in GANs using variational inference. **Electronics**, v. 9, n. 4, p. 688, 2020. Disponível em: <https://www.mdpi.com/2079-9292/9/4/688>. Acesso em: 11 set. 2025.

PEARSON, James; ZINETS, Natalia. Deepfake footage purports to show Ukrainian president capitulating. **REUTERS**, 17 mar. 2022. Disponível em: <https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/>. Acesso em: 18 set. 2025.

REUTERS. US FCC chair says EU Digital Services Act is threat to free speech. **Reuters**, 3 mar. 2025. Disponível em: <https://www.reuters.com/technology/eu-content-law-incompatible-with-us-free-speech-tradition-says-fccs-carr-2025-03-03/>. Acesso em: 20 set. 2025.

RODRIGUES, Paulo Gustavo. Deepfakes pornográficas não-consensuais: a busca por um modelo de criminalização. **Revista Brasileira de Ciências Criminais**, v. 199, p. 277-311, set./out. 2023. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/267>. Acesso em: 16 set. 2025.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial: uma abordagem moderna**. 4. ed. Rio de Janeiro: Gen LTC, 2021.

SALIMANS, Tim *et al.* Improved techniques for training GANs. In: **Advances in Neural Information Processing Systems**, v. 29, p. 2234-2242, 2016.

SANER, Emine. Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box'. **The Guardian**, Londres, 31 jan. 2024. Disponível em: <https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box>. Acesso em: 16 set. 2025.

SCHICK, Nina. **Deepfakes: the coming infocalypse**. Londres: Monoray, 2020.

SCHREIBER, Anderson; RIBAS, Felipe; MANSUR, Rafael. Deepfakes: regulação e responsabilidade civil. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org.). **O direito civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020. p. 609-626.

SENADO FEDERAL (BR). Projetos buscam restringir manipulação de imagens com inteligência artificial. **Agência Senado**, 7 fev. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/02/07/projetos-buscam-restringir-manipulacao-de-imagens-com-inteligencia-artificial>. Acesso em: 20 set. 2025.

SÍQUEIRA, Mariana de; ANDRADE, Ester Jerônimo de. Deepfake e privacidade: uma análise jurídica acerca da manipulação da imagem dos usuários. **Revista Foco**, [S. l.], v. 17, n. 8, p. e5679, 2024. Disponível em: <https://ojs.focopublicacoes.com.br/foco/article/view/5679>. Acesso em: 24 set. 2025.

STURGES, Julia. Taylor Swift, Deep-Fakes, and the First Amendment: Changing the Legal Landscape for Victims of Non-Consensual Artificial Pornography. **Georgetown Journal of Gender and the Law**, v. 25, n. 3, p. 555-585, 2024. Disponível em: <https://www.law.georgetown.edu/gender-journal/wp-content/uploads/sites/20/2024/05/Julia-Sturges-Taylor-Swift-Deep-Fakes-and-the-First-Amendment-.pdf>. Acesso em: 17 set. 2025.

TEPEDINO, Gustavo. **Direitos Humanos e Relações Jurídicas Privadas**. Rio de Janeiro: Ministério Público do Estado do Rio de Janeiro, 2021. Disponível em: https://www.mprj.mp.br/documents/20184/2845503/Gustavo_Tepedino.pdf. Acesso em: 21 set. 2025.

THE DALÍ MUSEUM. 'Dalí Lives': Museum brings artist back to life with AI. **The Dalí Museum**, 22 jan. 2019. Disponível em: <https://thedali.org/press-room/dali-lives-museum-brings-artists-back-to-life-with-ai/>. Acesso em: 14 set. 2025.

TOLOSANA, Ruben; *et al.* DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. **Information Fusion**, [S. l.], v. 64, p. 131-148, dez. 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1566253520303110>. Acesso em: 24 set. 2025.

UNITED KINGDOM. **Online Safety Act 2023**. London: UK Parliament, 2023. Disponível em: <https://www.legislation.gov.uk/ukpga/2023/50/contents>. Acesso em: 20 set. 2025.

VAINZOF, Rony. Para além da demonização do 'deepfake'. **FecomercioSP**, 15 ago. 2022. Disponível em: <https://www.fecomercio.com.br/noticia/para-alem-da-demonizacao-do-deepfake>. Acesso em: 13 set. 2025.

VAN DER SLOOT, Bart; WAGENSVELD, Yvette. Deepfakes: Regulatory challenges for the synthetic society. **Computer Law & Security Review**, v. 46, p. 1–15, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922000632>. Acesso em: 16 set. 2025.

VIEIRA, Juliana Rust Batista Felício. Violência digital: deepfakes, o novo rosto da opressão contra mulheres. **Migalhas**, 8 mar. 2025. Disponível em: <https://www.migalhas.com.br/depeso/430699/violencia-digital-deepfakes-o-novo-rosto-da-opressao-contra-mulheres>. Acesso em: 16 set. 2025.

ZANINI, L. E. DE A.; CARNEIRO QUEIROZ, O. N. A IRRENUNCIABILIDADE E A INTRANSMISSIBILIDADE DOS DIREITOS DA PERSONALIDADE. **Revista CEJ**, v. 28, n. 88, 18 fev. 2025. Disponível em: <https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/2846>. Acesso em: 21 set. 2025.