doi: 10.21783/rei.v11i2.858

SUBMETIDO: 13 SET. 2024
ACEITO: 04 MAR. 2025

"*COMO A PROTAGONISTA DA MINHA PRÓPRIA VIDA*": REPERCUSSÕES AO DIREITO À IMAGEM EM "*JOAN IS AWFUL*" DE *BLACK MIRROR* E A PROBLEMÁTICA DAS *DEEPFAKES*

"*LIKE THE MAIN CHARACTER IN MY OWN LIFE*": REPERCUSSIONS TO THE RIGHT TO IMAGE IN JOAN IS AWFUL OF BLACK MIRROR AND THE PROBLEM OF DEEPFAKES

VALERIA SILVA GALDINO CARDIN [1]
RAISSA ARANTES TOBBIN [2]

RESUMO: O trabalho tematiza o direito à imagem à luz do episódio "*Joan is awful*", da série *Black Mirror*, cuja protagonista, Joan, descobre que os acontecimentos de sua vida estão sendo retratados em uma série, que expõe sua vida privada para fins de engajamento e dramatização, já que concordou com as condições de uso de um serviço de *streaming* sem ler o contrato. Apesar do cenário de ficção científica, problematiza-se como tal situação poderia ser contornada diante da teoria dos direitos da personalidade, com ênfase na relação contratual e nos limites de utilização da imagem para evitar abusos e excessos, pontuando também o desafio que as *deepfakes* que são disseminadas nas redes sociais representam para a seara jurídica. Parte-se da hipótese de que o uso da imagem não pode extrapolar os limites do negócio jurídico e que o contrato não é capaz de transferir a titularidade do direito, mas apenas a autorização para o seu uso, sua divulgação e publicação. O objetivo geral consiste em analisar os limites da disposição contratual quanto ao direito à imagem à luz dos direitos da personalidade, bem como a problemática das *deepfakes*, que ameaçam o direito à imagem no contexto das redes sociais. Tem-se por objetivos específicos: descrever o episódio da série que servirá como base para a investigação; analisar a questão do direito à imagem à luz dos termos de uso, da proteção de dados pessoais e do consentimento com base na categoria teórica do "capitalismo de vigilância"; investigar o tema à luz da teoria dos direitos da personalidade; discutir a utilização, o controle e a legitimidade do uso da imagem

[1] Pós-doutorado em Direito pela Universidade de Lisboa; Doutora e mestre em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUCSP); docente da Universidade Estadual de Maringá e no Programa de Pós-Graduação em Ciências Jurídicas pela Universidade Cesumar (UNICESUMAR); Pesquisadora pelo ICETI; Advogada no Paraná.

[2] Doutoranda em Direito pela Universidade Cesumar (UNICESUMAR); Mestre em Ciências Jurídicas pela Universidade Cesumar (UNICESUMAR); graduada em Direito pela Universidade Paranaense (UNIPAR); Graduada em Letras – Português/Espanhol pela Universidade Estadual de Ponta Grossa (UEPG); Advogada no Paraná.

à luz dos avanços tecnológicos; e a problemática das *deepfakes* nas redes sociais. A pesquisa foi perspectivada pelo método hipotético-dedutivo, com base na técnica bibliográfico-documental.

PALAVRAS-CHAVE: *Big Techs*; consentimento; *deepfakes*; direitos da personalidade; inteligência artificial; proteção de dados.

ABSTRACT: The paper addresses the right to image in light of the episode "*Joan is awful*" from the series Black Mirror, whose protagonist, Joan, discovers that the events of her life are being portrayed in a series that exposes her private life for the purposes of engagement and dramatization, since we provide the terms of use of a streaming service without reading the contract. Despite the science fiction setting, it questions how such a situation could be overcome in light of the theory of personality rights, with an emphasis on the contractual relationship and the limits of use of the image to avoid abuse and excesses, also highlighting the challenge that deepfakes that are disseminated on social networks represent for the legal field. It starts from the hypothesis that the use of the image cannot go beyond the limits of the legal transaction and that the contract is not capable of transferring the ownership of the right, but only the authorization for its use, disclosure and publication. The general objective is to analyze the limits of the contractual provision regarding the right to image in light of personality rights, as well as the problem of deepfakes, which threaten the right to image in the context of social networks. The specific objectives are: to describe the episode of the series that will serve as the basis for the investigation; to analyze the issue of the right to image in light of the terms of use, the protection of personal data and consent based on the theoretical category of "surveillance capitalism"; to investigate the topic in light of the theory of personality rights; to discuss the use, control and legitimacy of the use of images in light of technological advances, especially in the face of deepfakes. The research was approached using the hypothetical-deductive method, based on the bibliographic-documentary technique.

KEYWORDS: Big Techs; consent; deepfakes; personality rights; artificial intelligence; data protection.

INTRODUÇÃO

No episódio "*Joan is Awful*"[3], da série *Black Mirror*, a protagonista Joan descobre que sua rotina diária está sendo retratada em uma série, que expõe sua vida privada e exagera suas atitudes para fins de engajamento e dramatização, uma vez que esta teria concordado com as condições de uso de um serviço de *streaming* sem ler os termos do contrato. Assim, a empresa poderia criar multiversos com base em seus dados pessoais, cenário com clara repercussão ao seu direito à imagem e que se

[3] Tradução livre: "Joan é péssima".

relaciona com o fenômeno das *deepfakes*, que podem ser conceituadas como conteúdo que é gerado por sistemas de inteligência artificial (IA) e que manipulam imagens, áudio e vídeo.

Apesar do contexto de ficção científica que ambienta o enredo, diante do avanço tecnológico e da utilização de novas tecnologias, inclusive da inteligência artificial, a pesquisa problematiza como a circunstância enfrentada pela personagem central do episódio analisado poderia ser contornada com base na teoria dos direitos da personalidade, com foco na relação contratual e nos limites de utilização da sua imagem, com o intuito de evitar abusos e excessos, inclusive quanto à criação das *deepfakes*, cuja disseminação nas redes sociais representa atualmente um grande desafio ao Direito.

O estudo parte da hipótese inicial de que o uso da imagem deve obedecer às regras contratuais e que não pode exorbitar os limites do negócio jurídico, uma vez que o contrato pactuado não é capaz de transferir a titularidade do direito à imagem, mas somente a autorização para o seu uso, bem como sua divulgação e publicação. Diante disso, no caso do episódio de série analisado, a anuência do titular não poderia ser utilizada para invocar a legitimidade quanto ao uso do direito à imagem para fins não consentidos ou, ainda, que se mostrassem contrários à tutela da dignidade. Já quanto às *deepfakes*, verifica-se que, muitas vezes, sequer há uma relação contratual, contexto que não tem impedido que a imagem de muitas pessoas, sobretudo figuras públicas, seja atingida negativamente nas redes sociais.

O objetivo geral do artigo consiste em analisar os limites da disposição contratual a respeito do direito à imagem à luz da teoria dos direitos da personalidade, pontuando também a dificuldade atual de controle do uso da imagem nas redes sociais diante das *deepfakes*. Para atingir o objetivo geral foram traçados objetivos específicos, que correspondem às seções de desenvolvimento do artigo: a) na primeira seção, o texto descreve os principais acontecimentos do episódio da série de *streaming* que servirá como pano de fundo para a investigação, tendo em vista os direitos da personalidade nele implicados; b) na sequência, examina-se a questão do direito à imagem a partir dos termos de uso, da proteção de dados pessoais e do consentimento com base na categoria teórica do "capitalismo de vigilância" de Shoshanna Zuboff; c) na terceira seção, investiga-se o tema considerando a teoria dos direitos da personalidade; d) na quarta seção, o texto discute as possibilidades de utilização, controle e legitimidade do uso da imagem diante do avanço tecnológico; e) na última seção, o trabalho analisará a problemática das *deepfakes* que circulam nas redes sociais. Destaca-se que a pesquisa utilizou o método hipotético-dedutivo, com base na técnica bibliográfico-documental.

2. *JOAN IS AWFUL*: UM SUCESSO DO *STREAMING*

Joan is awful é o primeiro episódio da sexta temporada da série *Black Mirror*, produzida pela *Netflix*, com lançamento em junho de 2023, direção de Ally Pankiw

e roteiro de Charlie Brooker. A história começa mostrando a rotina diária de Joan (Annie Murphy). Pela manhã, ela acorda, toma café com seu noivo e segue para o trabalho, onde, dentre as tarefas do dia, é encarregada de despedir uma funcionária com base na decisão de seus superiores.

Após o expediente, na sessão de terapia, Joan descreve com descontentamento sua vida profissional: "*sinto que estou no piloto automático todos os dias*". Também é com pouco entusiasmo que menciona sua relação com o noivo Krish, apesar de suas qualidades, e que tem conversado com um ex-namorado. Sobre a vida no geral, afirma que sente que não é a *protagonista da sua própria história* e que não está no controle de sua vida (Joan, 2023), o que gostaria que fosse mudado de alguma forma (temática que não deixa de ter relação com a "*Great Resignation*"[4]).

Depois da conversa com a psicóloga, Joan resolve se encontrar com o ex-namorado em um restaurante. Lá, beija-o, mas a conversa não é interessante (cheia de passado). Posteriormente, volta para casa e, antes de dormir, decide assistir com seu noivo algo no serviço pago *Streamberry*[5]. Logo que seleciona a série "*Joan is Awful*", o casal ri, já que visualiza na *TV* uma mulher com corte e cor dos cabelos semelhantes aos de Joan, com um *blazer* verde idêntico ao utilizado por ela durante o dia. Estranhamente, o episódio se inicia descrevendo com exatidão todos os acontecimentos da vida de Joan nas últimas 24 horas, inclusive a demissão da funcionária, a conversa com a psicóloga e o encontro com o ex-namorado. A vida real se confunde com a ficção. A diferença é que a personagem da *TV* – interpretada pela atriz Salma Hayek (Salma Hayek) – parece ser muito apática, fria e insensível. Tal como o casal perplexo com tudo o que viu, os amigos e colegas de trabalho também veem a semelhança da série e a associam à Joan. Diante do que foi mostrado no *streaming*, e da clara alusão à realidade, Krish rompe com Joan, que

[4] Tradução livre: "Grande Demissão". Também conhecida como *Big Quit*, é uma tendência econômica mundial de pedido de demissão em massa, que teve início em 2021, após a pandemia da COVID-19, sobretudo nos EUA. Conforme Parker e Horowitz (2022) 63% dos trabalhadores que pediram demissão em 2021 alegaram receber baixos salários; falta de oportunidades de crescimento dentro da empresa (63%) e que se sentiam desrespeitados no local de trabalho (57%). Cerca de metade dos trabalhadores alegou que problemas com cuidados infantis teria sido uma das razões para que deixassem o emprego (48% entre os com um filho menor de 18 anos em casa). Parcela semelhante aponta a falta de flexibilidade dos horários de trabalho (45%) ou não ter bons benefícios, como plano de saúde e folga remunerada (43%). Cerca de 4 em cada 10 adultos que deixaram um emprego em 2021 (39%) dizem que o motivo é que estavam trabalhando muitas horas. Cerca de um terço (35%) cita o desejo de se mudar para um local diferente. 31% dos entrevistados afirmaram que os motivos para deixar o emprego estavam relacionados às repercussões e consequências da pandemia. Homens e mulheres apresentaram motivos semelhantes para deixar um emprego em 2021, mas há diferenças significativas por nível educacional. Os empregados sem diploma universitário (34%) são mais propensos a pedirem demissão do que os que possuem diploma de bacharel ou nível de educação mais elevado (21%).

[5] Em clara alusão sátira à empresa *Netflix*.

também é demitida do trabalho no dia seguinte, já que a personagem da série de TV deixou escapar segredos e assuntos confidenciais da empresa (Joan, 2023).

Joan alega não fez nada de errado. Que é culpa da atriz Salma Hayek, que a interpreta na série. Todos os acontecimentos deste segundo dia também são retratados no *streaming*, como um segundo episódio da série *Joan is Awful*. Inconformada, Joan procura sua advogada, afirmado que a série utiliza sua vida, seu nome, sua carreira e que arruinou seu noivado. Contudo, a defensora afirma que Joan concedeu permissão à *Streamberry* para que pudesse criar um seriado a partir de sua vida, quando concordou com os termos do serviço (Joan, 2023).

Joan pontua que nunca tinha visto nada daquilo. A advogada menciona que o contrato apareceu para Joan pelo celular e ela simplesmente teria clicado em "ACEITAR" e que não importava a sua vontade, já que ela teria aceitado mesmo assim. Joan afirma que poderia processar a atriz Salma Hayek por se passar por ela na série. A advogada contra-argumenta que a empresa de *streaming* estaria utilizando a imagem digital da atriz Salma Hayek. *Joan is awful* seria toda realizada a partir de computação gráfica (CGI)[6], por meio de um computador quântico superavançado. Eles poderiam fazer a atriz Salma Hayek fazer qualquer coisa. A série também seria produzida a partir dos dados coletados de Joan (áudio, vídeo, mensagens etc.). Joan pontua que a série inventa coisas sobre ela: exagera os fatos, faz ela aparecer "pior do que é", o que, para Joan, seria difamação. Contudo, a empresa teria permissão para criar personagens e diálogos para fins dramáticos. O conselho que a advogada conseguiu dar a Joan foi que esta deveria, simplesmente, ignorar a série (Joan, 2023).

Com tal repercussão, do outro lado da história, a atriz Salma Hayek se revolta e afirma que não quer ver sua imagem associada à de Joan, já que esta passou a cometer atos questionáveis na tentativa de impedir a continuação da série de TV. Ironicamente, Joan afirma que ela também não quer ser associada com ela mesma (sua representação exagerada e transformada em um drama de computação gráfica).

Salma confessa que pensou que poderia ter controle sobre sua própria imagem, mas foi enganada. Pontuou que era disléxica, não leu o contrato e que paga seu advogado para protegê-la na seara contratual. A atriz teria vendido seus direitos de imagem para a empresa, o que abrangeria quaisquer atos que a personagem pudesse exibir. Tudo estaria legalmente estabelecido e não haveria procedência em um pedido judicial. Pensando em danos que poderiam ser controlados, seu advogado também compreende que nada seria eficiente para retirar as imagens da série que rapidamente se espalharam pela Internet. Enquanto Salma reclama do pouco que está ganhando com a série, Joan pontua que não está recebendo um centavo (Joan, 2023).

[6] *Computer-generated imagery* (imagens geradas por computador).

Segundo a explicação da *CEO* da *Streamberry*, não haveria nada de especial em Joan para que sua vida fosse retratada na série, que seria apenas o começo, já que a intenção seria lançar conteúdo inédito e sob medida para os 800 milhões de usuários. *Joan* é "*awful*" (péssima) porque o conteúdo negativo ganha muito mais adesão do que o afirmativo. *Joan is* "*awesome*" (é incrível) não teria tanto apelo comercial.

Os momentos egoístas e covardes geravam mais engajamento – já que confirmavam os medos mais profundos dos usuários, a visão neurótica que possuíam sobre si mesmos e os deixavam hipnotizados. Joan e a atriz Salma Hayek arquitetam um plano para destruir o sistema da *Streamberry* que cria a série (o *quamputer* – com conteúdo infinito, capaz de criar multiversos) (Joan, 2023). Em que pese o alcance do resultado pretendido, uma série de novas consequências é apresentada às personagens.

3. TERMOS DE USO, PROTEÇÃO DE DADOS E CRISE DO CONSENTIMENTO: ÓBICES AO PROTAGONISMO DO USUÁRIO EM TEMPOS DE CAPITALISMO DE VIGILÂNCIA

A fala da advogada de Joan, mencionada no tópico anterior, sintetiza o que poderia acontecer em tempos de capitalismo de vigilância, termo cunho por Shoshana Zuboff (2019) para descrever a transformação da "economia política que constitui e expande uma nova forma de capitalismo pautada na exploração do comportamento das pessoas, ou seja, em todos os aspectos da vida cotidiana — para além do paradigma do trabalho". A vigilância no capitalismo atual é determinante e criou uma engenhosa estrutura de mercantilização dos dados pessoais obtidos (Fornasier; Knebel, 2021). No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) considera dado pessoal a "informação relacionada a pessoa natural identificada ou identificável", enquanto os dados pessoais sensíveis dizem respeito à origem racial ou étnica, à "convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político", dado "referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018).

Pontua-se que a Emenda Constitucional nº 115 elevou a proteção dos dados pessoais, inclusive nos meios digitais, ao *status* de direito fundamental, passando a constar expressamente no rol do art. 5º da Constituição Federal (Brasil, 2022). Vale dizer que, no Brasil, não há legislação que proíba o tratamento de dados para fins comerciais, entretanto, tal prática precisa seguir parâmetros éticos e o princípio da não discriminação[7] (art. 6º, IV da LGPD).

[7] Quanto à utilização de algoritmos e a possibilidade de discriminação no contexto do tratamento de dados, Leal e Paulo afirmam que a "a falta de diversidade nos conjuntos de dados usados para treinar os algoritmos pode levar a resultados tendenciosos. O problema, como se vê, não está no utilizador da ferramenta, e por vezes também não está na maldade do programador, mas na baixa diversidade social encontrada na base de dados. O viés algorítmico, na verdade, é sobre isso: vieses que acabam transparecendo sem intencionalidade a partir da leitura realizada pelo algoritmo do

É um desafio superar a visão utilitarista que cerca a monetização de dados, especialmente em um cenário que propaga a ideia de autorregulação por parte das empresas de tecnologia (Hoofnagle, 2018). Conforme Tobbin e Cardin:

> [...] persiste a dúvida quanto ao que será feito com os dados coletados, uma vez que, por mais que o cidadão concorde com os termos de uso e conceda a utilização por páginas, aplicativos e dispositivos, o armazenamento de dados geralmente é feito por empresas ligadas ao ramo da tecnologia, de modo que estas também estão suscetíveis a vazamentos e à utilização indevida, ou seja, não é prática ilegal, mas o seu uso indiscriminado pode repercutir na ofensa a direitos fundamentais e de personalidade dos usuários [...] o simples consentimento, baseado em extensos termos de uso, com simples opções ao final como "Eu aceito", "Concordo", "Autorizo", é pouco eficaz para garantir ao indivíduo o direito de escolha, em especial quando a coleta de dados é o "pagamento" pelo acesso a informações importantes ao usuário, que se vê compelido a aceitar tais termos, a um só clique, para que não seja excluído do tráfego de circulação de informações em rede (Tobbin; Cardin, 2021, p. 256-257).

Destaca-se que, certamente, se soubesse da possibilidade de que o tratamento de seus dados poderia ser utilizado para criar multiversos com base em sua vida privada, que mais pareciam *deepfakes*, Joan não concordaria com tais termos. É questionável a real chance de o usuário ser protagonista neste cenário, obter controle sobre seus dados pessoais ou constatar os reais riscos do compartilhamento de suas informações, sobretudo porque as pessoas costumam não ler as políticas de privacidade e, mesmo que assim fizessem, dificilmente as compreendem diante da linguagem técnica utilizada (Schermer; Custers; Hof, 2014; Tobbin; Cardin, 2021; Rodotà, 2008). Haveria uma limitação cognitiva do titular dos dados quanto à utilização destes no ambiente *online*, em razão da assimetria de sua relação com os agentes responsáveis pelo tratamento de dados. O consentimento tende a ser fictício, já que o cidadão possui duas escolhas: consentir ou não desfrutar de todos os serviços e produtos que cada vez mais influenciam a vida em sociedade (Mendes, 2020). Tal instituto, previsto tanto no Regulamento Geral sobre a Proteção de Dados, no âmbito da União Europeia, como na LGPD, no Brasil, ainda não se mostra, na prática, eficiente para proteger os dados dos cidadãos no ambiente virtual.

O episódio mostra a realidade do indivíduo diante do avanço tecnológico atual, sobretudo no que tange ao fato de que este é renegado à posição de mero consumidor e alimentador passivo e não remunerado de dados fundamentais para

problema apresentado a ele e dos seus subsídios para resolvê-lo, isto é, os dados da sua base" (Leal; Paulo, 2023, p. 179).

o avanço da tecnologia, sobretudo da inteligência artificial. O indivíduo tende a considerar que seus dados pouco têm utilidade para o mercado financeiro ou tecnológico, que o risco é geral e não com base na experiência individual e que as pessoas a sua volta sempre serão mais vulneráveis, isto é, grande parte da população ainda não compreende de forma abrangente qual é a real necessidade da proteção de dados, como se proteger e quais direitos fundamentais e da personalidade poderiam ser afetados pela monetização destes, pelas práticas de vigilância digital e a criação e elaboração de perfis informacionais nos termos da experiência pessoal no ambiente virtual.

Para que o consentimento possa trazer maior autonomia e liberdade ao indivíduo, seria fundamental que as empresas de tecnologia empoderassem seus usuários, o que dificilmente ocorre, sobretudo porque a monetização de dados é o que tende a sustentar tais gigantes do ramo tecnológico, de forma que muitas de suas práticas, como os *cookies*, tendem a vulnerabilizar o cidadão ainda mais e a criar maiores assimetrias entre as experiências digitais. Diante da cada vez maior relevância das *Big Techs* para a realização de atividades da vida cotidiana, o cidadão é transformado em consumidor, já que o consumo é a base do capitalismo. O cidadão é despido de seu caráter político, de reivindicação de direitos e garantias fundamentais, de questionamento acerca de hegemonia destas empresas e de sua possibilidade de crítica. Tendo em vista a necessidade de utilização destes aplicativos, as pessoas acabam concordando com os termos de adesão, sobretudo porque a não concordância significa exclusão de acesso a facilidades, que são pagas com a coleta de dados pessoais.

O neoliberalismo transforma o cidadão em consumidor. "A liberdade do cidadão cede diante da passividade do consumidor. A reivindicação por transparência pressupõe a posição de um espectador a ser escandalizado". Não é uma "demanda de um cidadão engajado, mais de um espectador passivo. A participação ocorre em forma de reclamação e queixa". Povoada "por espectadores e consumidores, a sociedade da transparência funda uma *democracia de espectadores*" (Han, 2020, p. 22). O trabalho compreende que se há uma possibilidade de protagonismo por parte do usuário nos próximos anos, essa se dará, provavelmente, pela exaltação da figura de consumidor passivo, já que é essencial o seu empoderamento (com proteção de dados, autodeterminação informativa e privacidade) para o sustento desta ótica de mercado.

4. O DIREITO À IMAGEM COMO DIREITO DA PERSONALIDADE: UMA ANÁLISE A PARTIR DO EPISÓDIO *JOAN IS AWFUL* DA SÉRIE *BLACK MIRROR*

Verifica-se que parte da problemática do referido episódio da série *Black Mirror* gira em torno do domínio da narrativa sobre a personalidade de Joan. A personalidade se constitui a partir de um conjunto de caracteres que são únicos ao indivíduo, e inerentes à sua dignidade humana. É por meio desta que a pessoa pode adquirir e defender bens e direitos, tais como a vida, a liberdade, a igualdade, a

honra etc. Portanto, engloba a visão de vida e mundo sob uma perspectiva subjetiva e individualizadora, assim como os padrões de comportamento, os pensamentos, a autopercepção, cenário que distingue a pessoa como ser único (Szaniawski, 2002). Para Bittar, os direitos da personalidade seriam direitos "inatos, absolutos, extrapatrimoniais, intransmissíveis, imprescritíveis, impenhoráveis, vitalícios, necessários e oponíveis *erga omnes*" (Bittar, 1999, p. 64).

Para Borges (2007), o objetivo dos direitos da personalidade é a proteção física e/ou psíquica da pessoa e de suas características mais importantes, especialmente porque a intenção é tutelar a sua essência, bem como seus bens e valores mais caros. Já Adriano de Cupis (1967, p. 17-18) observa que existem certos direitos sem os quais a personalidade "restaria uma susceptibilidade completamente irrealizada, privada de todo o valor concreto: direitos sem os quais todos os outros direitos subjetivos perderiam todo o interesse para o indivíduo", isto é, caso não existissem, a pessoa não existiria como tal. Não haveria motivo para proteger outros direitos se os da personalidade não fossem assegurados. Na visão de Zanini *et al*. (2018) os direitos da personalidade seriam direitos privados, ao passo que os direitos fundamentais se enquadrariam no âmbito do Direito Público. Entretanto, afirmam que, atualmente, a dicotomia entre os direitos público e privado só se mostra plausível para fins didáticos.

No Brasil, o Código Civil dedicou um capítulo específico para os direitos da personalidade, entre os arts. 11 e 21 (Capítulo II), dispondo que, com exceção dos casos previstos em lei, eles seriam irrenunciáveis e intransferíveis, não podendo o seu exercício sofrer limitação voluntária. Assim, o titular pode exigir que cesse a ameaça ou a lesão a tais direitos, bem como reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei (Brasil, 2002). O Código disciplina questões ligadas à vida e à sua manutenção, assim como concedeu autonomia e liberdade para a pessoa em circunstâncias que possam exigir o seu consentimento, com base na ética, na moral e na tentativa de inibir práticas de objetificação e coisificação do ser humano, sobretudo para fins econômicos e de capitalismo predatório (Tobbin; Cardin, 2022).

Autores como Tepedino (2004) e Szaniawski (2002), entendem que o rol de direitos da personalidade do Código Civil não seria taxativo, de modo que outros direitos, não contemplados pelo *codex*, também seriam fundamentais para o desenvolvimento da personalidade humana, especialmente em razão da evolução social e dos obstáculos enfrentados do Direito para acompanhar e regular todas as esferas da ordem social ao tempo que estas são identificadas e reconhecidas[8]. A

[8] Conforme pontuam Ikeda e Teixeira (2022, p. 146-147), os autores que entendem pela inexistência de uma cláusula geral de proteção da personalidade se fundamentam na insegurança jurídica. O debate acerca da existência ou não de uma cláusula geral tem o condão de aprofundar os estudos acerca dos direitos da personalidade. Pontua-se que as principais correntes convergem quanto à necessidade de "necessidade de proteção dos atributos da personalidade em sua extensão

ausência de previsão legal no que tange a determinado direito da personalidade não implicaria, necessariamente, em inexistência, sobretudo em razão de que esta deriva do reconhecimento da dignidade humana e não de regulamentação legal[9]. Verifica-se que o presente trabalho se filia à corrente que compreende que o rol de direitos da personalidade previsto no Código de 2002 não é taxativo, mas exemplificativo, especialmente diante da necessidade de proteção da pessoa ante ao avanço tecnológico, que faz surgir relações e cenários nunca antes pensadas, que culminam em novas situações jurídicas e problemáticas.

Observa Moraes (2008), que, ao intérprete incumbe, em razão do reconhecimento da cláusula geral da tutela dos direitos da pessoa, privilegiar valores existenciais sempre que estes estiverem em oposição aos patrimoniais, sobretudo porque as normas de Direito Civil devem ser interpretadas à luz da Constituição de 1988, para proteger a dignidade e a personalidade. Alguns autores compreendem que o princípio da dignidade da pessoa humana, previsto no art. 1º, inciso III, da Constituição Federal (Brasil, 1988), seria uma cláusula geral de proteção da personalidade, tutelando o ser em sua totalidade em situações que envolvessem ofensa à individualidade, essencial para o desenvolvimento da personalidade (Szaniawski, 2002). Sarlet (2007) assevera que a dignidade da pessoa é a qualidade intrínseca e distintiva que pode ser reconhecida em cada ser humano.

Sob a ótica constitucional (que vai de encontro com a perspectiva dos instrumentos internacionais de proteção dos direitos humanos, bem como de sua tendência de universalização) (Piovesan, 2013), o ser humano é merecedor de dignidade pelo simples fato de ser pessoa. Assim, deve ser protegido por direitos e garantias fundamentais, bem como direitos da personalidade, que tutelem o que ele tem de mais valioso. Como observa Sarmento, o princípio da dignidade da pessoa humana é o epicentro "axiológico da ordem constitucional", irradiando "efeitos sobre todo ordenamento jurídico e balizando não apenas os atos estatais, mas também toda a miríade de relações privadas que se desenvolvem no seio da sociedade e no mercado" (Sarmento, 2004, p. 109).

Para Fermentão (2006, p. 246), "a pessoa humana traz em si valores que lhe são privativos, e esses valores integram a sua personalidade e lhe potenciam

máxima, colocando-se o problema na segurança jurídica pela sua natureza absoluta ou *erga omnes*". De qualquer forma, é necessário analisar a expansão ou o aumento de direitos da personalidade de forma cautelosa, pois "não se trata apenas de confirmar uma vitória histórica da posição da pessoa nos ordenamentos jurídicos", já que a consagração de direitos deve ser "seguida de sua efetivação, e em harmonia com os demais direitos da personalidade e fundamentais de terceiros, sob pena de sua violação continuada ou sua convolação em mero símbolo".

[9] Nos termos do Enunciado 274 da IV Jornada de Direito Civil, "os direitos da personalidade, regulados de maneira não-exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida noart. 1º, inc. III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação" (CJF, 2006).

desenvolver-se em sociedade. A dignidade da pessoa humana é o centro de sua personalidade". A tutela dos direitos da personalidade é essencial para o delineamento de parâmetros éticos para a concretização e a expansão da tecnologia. Um exemplo disso é que, para Doneda (2011), os dados pessoais podem ser considerados no contexto atual como uma expressão da personalidade, já que representam os gostos, as preferências, os interesses e as características físicas, biológicas e referentes à saúde, educação, profissão, condição social, religião etc. Magrani (2019) destaca que para a assegurar a dignidade é fundamental garantir a proteção dos dados pessoais do usuário.

Com o lançamento da série, a cada novo episódio, Joan enfrentou verdadeiro terror psíquico com toda a situação. Visivelmente, a situação envolveu pânico, ansiedade, incerteza, desespero, choro, o medo de ser mal interpretada, de perder o emprego e o relacionamento amoroso e de ter a vida exposta na TV. Assim, Joan teve seu direito à integridade psíquica severamente abalado, com reflexos, inclusive, ao direito à saúde. A integridade física de Joan também foi ameaçada, já que ela passou a ser hostilizada pelos vizinhos e conhecidos. Não se pode olvidar que ela também poderia ser odiada pelos espectadores, que poderiam a confundir com a personagem da série, fator que poderia resultar em exclusão, discriminação, xingamentos e ataques nos planos físico e virtual. Destaca-se que os direitos à vida e à integridade físico-psíquica "protegem a inviolabilidade do corpo do indivíduo, sendo certo que a pessoa não pode suportar interferências contra o seu desejo", com exceção aos "casos de exigência médica e que não resulte em redução da integridade física permanentemente ou contrarie os bons costumes (Silva; Neves; Gottems, 2023, p. 90)".

A empresa de *streaming* passou a utilizar o nome de Joan sem sua anuência ou que esta concordasse com todos os desdobramentos a partir da série. O direito ao nome, tanto da pessoa natural quanto da jurídica, é tutelado pelos artigos 16 a 19 do Código Civil e pela Lei de Registros Públicos (LRP – Lei nº 6.015/1973). Trata-se de "uma das maiores particularidades do indivíduo, pois se refere ao modo de conhecimento deste perante a sociedade" (Silva; Neves; Gottems, 2023, p. 90). Conforme o Código Civil, toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome. O nome da pessoa não pode ser empregado por outrem "em publicações ou representações que exponham ao desprezo público, ainda quando não haja intenção difamatória". Além disso, "sem autorização, não se pode usar o nome alheio em propaganda comercial" (arts. 16 ao 18 CC/02) (Brasil, 2002).

O nome e outros sinais que identificam o indivíduo são elementos básicos que permitem a associação nos núcleos da sociedade, com a família, os relacionamentos, os negócios, a vida social etc. O nome individualiza a pessoa e evita que esta seja confundida com outra (Marcelino; Fermentão, 2007, p. 545). De acordo com França, quanto ao direito ao nome, o "bem jurídico tutelado é a identidade, que se considera como atributo ínsito na personalidade humana" (França, 1958; Marcelino; Fermentão, 2007, p. 544). O direito essencial é o nome,

mas também recebem proteção jurídica os acessórios do nome (Marcelino; Fermentão, 2007), como o pseudônimo. Pontua-se, também, que a série atingiu a honra[10] de Joan perante a sociedade. O conceito que as pessoas tinham a respeito dela foi alterado. O enredo exagerava as atitudes da personagem para que esta parecesse uma pessoa de má índole, tudo para garantir o engajamento dos espectadores. A narrativa sobre a própria personalidade foi modificada. Para fins de entretenimento, a série alterou seus valores éticos e morais. O direito à honra faz "referência à forma como o indivíduo se vê perante a sociedade e como ela o vê. Pode ser subclassificada ainda em honra subjetiva (autoestima) e honra objetiva (repercussão social)" (Silva; Neves; Gottems, 2023, p. 90). Como observam Silva, Freire e Fontes, em uma sociedade capitalista e neoliberal, a reputação social "contribui diretamente para o que o indivíduo possa progredir no meio social e conquistar o lugar almejado socialmente" (Silva; Freire; Fontes, 2023, p. 17).

A intimidade de Joan foi severamente ofendida, já que suas conversas privadas, seus pensamentos e sentimentos foram explorados pela série, o que repercutiu em sua relação de trabalho, sua convivência com os funcionários/subordinados na empresa e em seu relacionamento amoroso. Os sentimentos de Joan foram expostos, o que ela pensava sobre suas relações e a visão que tinha sobre seu noivo (Joan, 2023).

A série expôs seu encontro secreto com o ex-namorado e a demonstração de afeto, atingindo sua vida afetiva, sexual e denunciando sua eventual infidelidade. Como sua vida passou a ser pública, as pessoas não queriam mais se relacionar com ela intimamente, a exemplo de seu ex-namorado, que afirmou que não gostaria de ver sua vida exposta por meio de um personagem em *Joan is awful* (Joan, 2023). Conforme o art. 21 do Código Civil, "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (Brasil, 2002). É importante destacar que Sarlet diferencia direito à privacidade, do direito à proteção de dados e da autodeterminação informativa[11]. Para o autor, a proteção de dados e a autodeterminação informativa vão além da privacidade e de sua proteção, caracterizada por uma perspectiva de "recolhimento" e "exposição" (Sarlet, 2020).

O bem jurídico protegido pela privacidade gira em torno da informação e do sigilo, já o da proteção de dados abarca a informação, a circulação e o respectivo

[10] Nos termos do art. 5º, inciso X, da Constituição Federal de 1988, são invioláveis a intimidade, a vida privada, a honra e a imagem, sendo assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

[11] A autodeterminação informativa, de acordo com Mendes possui sua origem atrelada ao Tribunal Constitucional Federal Alemão, e representa a capacidade do indivíduo de se manifestar fundamentalmente acerca da coleta de dados pessoais e a forma como esses serão utilizados e processados. Para a autora, o princípio da autodeterminação informativa pressupõe que não existem dados "insignificantes nas circunstâncias modernas do processamento eletrônico de dados" (Mendes; Fonseca, 2020).

controle. Portanto, o objeto do direito à proteção de dados é mais amplo – abrange todos os dados que dizem respeito à pessoa natural, sendo irrelevante "a qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática (Sarlet, 2020, p. 33)[12]". Para Sarlet (2020, p. 33), a dinamicidade das inovações tecnológicas acabou confirmando a insuficiência de um direito à autodeterminação informativa, que também não substituiu pura e simplesmente outros direitos, como a privacidade. Análises de risco que antes não poderiam ser feitas, hoje ganham espaço e podem tanto diminuir (mesmo que isso signifique vigilância excessiva e eventual ofensa à privacidade) como enrijecer o custo de serviços a partir do estilo de vida do indivíduo (Morozov, 2018).

É importante destacar que a coleta de dados para a composição da série também envolveu a renderização do corpo de *Joan* com base em seu engajamento *online* (dados coletados da experiência na plataforma de *streaming*, por meio de celular e eventual uso de *wearables*[13]), termo que é utilizado para designar o processamento de uma combinação de dados que consistem em imagens, áudio, vídeos, transições, legendas.

A renderização do corpo ocorre mediante a análise de uma série de dados fisiológicos, de modo a ser possível realizar previsões complexas. A renderização é a captura de *superávit comportamental* – à medida que o indivíduo passa a ser representado pelos seus dados. Na maioria dos países, a utilização destes dispositivos não é sujeita às leis de privacidade ou referentes à saúde e, mesmo nos que há legislação, esta parece não levar o fenômeno do capitalismo de vigilância

[12] "o que se pode afirmar, sem temor de incorrer em erro, é que, seja na literatura jurídica, seja na legislação e jurisprudência, o direito à proteção de dados vai além da tutelada privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade" (Sarlet, 2020, p. 33).

[13] As tecnologias vestíveis "fazem parte do ramo da Internet das Coisas (do inglês *Internet of Things* - IoT) e são dispositivos tecnológicos que podem ser acoplados ao corpo humano (relógios, pulseiras, joias e tecidos inteligentes) para medir sinais fisiológicos, como batimentos cardíacos, pressão arterial, qualidade de sono, calorias perdidas, ciclo menstrual, saturação do oxigênio e monitorar sintomas de pacientes pela via remota. São muito utilizadas na área da saúde e dos esportes de alta performance, mas o seu uso também pode se dar para fins de acompanhamento da produtividade e otimização de tarefas, sendo considerados objetivos pessoais que agregam tecnologia, moda e *design*. Esses dispositivos coletam dados pessoais, que são mostrados por meio de uma interface e transmitidos para outros dispositivos e bancos de dados da empresa fabricante (ex: *FitBit*, *Apple*, *Google* etc.)". A tecnologia incorporada "envolve uma interação mais profunda com o corpo humano, que pode se dar por meio cirúrgico ou mediante implantes com *chips* sob a pele, e tem a capacidade de coletar mais dados pessoais do que *smartwatches*, tecidos inteligentes e smartphones, o que também pode representar maior risco em relação a questões quanto à privacidade" (Tobbin; Cardin, 2022, p. 116).

(Zuboff, 2019). A privacidade funcionaria, neste contexto, como moeda de troca para a obtenção de benefícios.

Como consequências pontuais diante da ofensa aos direitos da personalidade pela série de TV, Joan perdeu seu emprego, o que comprometeu sua dignidade, já que o fato de não mais auferir renda poderia comprometer a possibilidade de existência digna em sociedade e o acesso a um mínimo existencial[14]. O término do relacionamento também poderia acarretar repercussão no âmbito do Direito de Família, já que esta vivia com seu noivo (em aparente união estável).

5. UTILIZAÇÃO, CONTROLE E LEGITIMIDADE DO DIREITO À IMAGEM DIANTE DO AVANÇO TECNOLÓGICO

Com a série, o direito à imagem[15] de Joan passou a ser explorado. A personagem possuía figurino e corte de cabelo idênticos ao de Joan. Chamava atenção que a personagem tinha, inclusive, o mesmo estilo de mechas brancas adotado por Joan no cabeleireiro. A série não passava despercebida pelas pessoas a sua volta, tendo em vista que amigos e colegas imediatamente a associavam à imagem de Joan.

Para Silva, Neves e Gottems (2023, p. 92-93), o direito à imagem "é uma espécie dos direitos da personalidade, mas é considerado autônomo, visto que sua proteção não depende da violação de outro direito, como a honra, por exemplo". O dever de indenizar que medida que se impõe pela simples violação ao direito à imagem (Fachin, 1999), de modo que a Constituição Federal fez questão de evidenciá-lo no rol dos bens tutelados. O uso indevido da imagem, por si só, pode acarretar grande repercussão na jurisdição pátria e na vida íntima do indivíduo prejudicado (Silva; Neves; Gottems, 2023).

Destaca-se que, no passado, o conceito de imagem era restrito à representação visual, de forma que a imagem era limitada ao que fosse esculpido, fotografado ou cinematografado, todavia, o avanço tecnológico impactou severamente o contexto da captação e da divulgação da imagem, bem como os bens que por ela devem ser protegidos. Por imagem, passou-se a "entender não só os aspectos físicos, mas também as características pessoais, comportamentos e atitudes, índole, que caracterizam e individualizam os indivíduos em relação às outras pessoas" [16]

[14] Ver FACHIN, Luiz Edson. **Estatuto jurídico do patrimônio mínimo**. Rio de Janeiro: Renovar, 2001.

[15] "Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, adivulgação 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. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes" (Brasil, 2002).

[16] "Além de não se restringir à representação fotográfica, o direito à imagem engloba toda e qualquer representação plástica, gráfica ou fotográfica de uma pessoa ou de um objeto, ou, ainda, por qualquer outro meio de caracterização de seus atributos" (Siqueira; Vieira, 2022, p. 4).

(Siqueira; Vieira, 2022, p. 3). O direito à imagem pode ser divido em "imagem-retrato (atributos físicos da pessoa) e imagem-atributo (repercussão social da imagem)"[17] (Silva; Neves; Gottems, 2023, p. 90). Para Maria Helena Diniz:

> [...] a imagem-retrato é a representação física da pessoa, como um todo ou em partes separadas do corpo (nariz, olhos, sorriso etc.) desde que identificáveis, implicando o reconhecimento de seu titular, por meio de fotografia, escultura, desenho, pintura, interpretação dramática, cinematografia, televisão, sites etc., que requer autorização do retratado (CF, art. 5°, X). A imagem-atributo é o conjunto de caracteres ou qualidades cultivadas pela pessoa, reconhecidos socialmente (CF, art. 5°, V), como habilidade, competência, lealdade, pontualidade etc. A imagem abrange também a reprodução, romanceada em livro, filme, ou novela, da vida de pessoa de notoriedade (Diniz, 2015, p. 147).

O uso indevido deste direito é passível de dano patrimonial, na medida e que a imagem pode ser explorada para fins lucrativos sem a permissão do titular, "o mesmo ocorre quando a utilização indevida da imagem de terceiro gerar prejuízos em sua reputação" (Silva; Neves; Gottems, 2023, p. 90). O contexto muda se a exposição da imagem for feita com a anuência do titular. "O direito à imagem possui íntima relação com o consentimento do sujeito retratado" (Siqueira; Vieira, 2022, p. 6). Contudo, o direito à indenização por danos morais ainda é possível, mesmo com a concordância do indivíduo, caso a utilização da imagem for de maneira desrespeitosa ou vergonhosa, de modo a ofender a honra (Silva; Neves; Gottems, 2023, p. 94). O direito à imagem não se confunde com o direito à honra. Entretanto, mesmo com a "autorização da pessoa, se a utilização da imagem ultrapassar os limites estabelecidos e se tornar vexatória pode ainda ferir a honra do sujeito, cabendo a devida indenização e responsabilidade do ofensor" (Silva; Neves; Gottems, 2023, p. 94).

Quanto à Salma Hayek, a renomada atriz se sentia vendida. De uma hora para outra, não tinha mais vez no mundo da atuação. Sua imagem poderia ser utilizada e controlada pelo *streaming* como este bem entendesse. O papel e o trabalho dos artistas são postos em xeque, sobretudo diante do avanço da inteligência artificial. A IA já é capaz de simular a voz de um cantor famoso, criar um mundo paralelo

[17] Como asseveram Silva, Neves e Gottems, "a distinção de imagem-retrato e imagem-atributo, feita pela maioria da doutrina, parece ser muito certeira, na medida em que a lei busca efetivamente repelir as duas, no que se refere aos direitos da personalidade. A proteção ofertada pelo ordenamento jurídico engloba as características relacionadas aos atributos físicos, tais como a aparência, a voz, e também as características relacionadas à sua identidade pessoal, ou seja, a projeção da personalidade perante a sociedade" (Silva; Neves; Gottems, 2023, p. 94).

com computação gráfica e escrever roteiros e textos, tanto em benefício do indivíduo como em seu prejuízo.

Destaca-se a necessidade de discussão acerca de questões ligadas à garantia da privacidade, da memória e da proteção da imagem das pessoas falecidas, sobretudo quando o assunto é herança digital e o uso da inteligência artificial no contexto pós-morte. Existem inúmeros casos de pessoas já falecidas, que deixaram redes sociais e que continuam sendo alimentadas pelos herdeiros. Internacionalmente, tem-se alguns casos famosos, como o *Instagram* dos cantores Michael Jackson, Elvis Presley e Whitney Houston, assim como no plano nacional, há os perfis da cantora Marília Mendonça, do apresentador Gugu Liberato e, até mesmo, da banda Mamonas Assassinas, todos com selo de verificação de autenticidade. Frisa-se que alguns desses nomes mencionados faleceram quando sequer existiam as redes sociais, porém, elas foram criadas e o conteúdo é produzido para alimentar a memória, até mesmo com a finalidade de captação e venda de produtos licenciados. De qualquer forma, urge o questionamento acerca desta herança digital e dos limites de uso trazidos pelos herdeiros (Figueira; Renzetti Filho; Luca, 2023, p. 533):

> [...] pode-se considerar que os bens digitais são bens imateriais, alguns apreciáveis economicamente e outros sem conteúdo econômico a depender da relação jurídica a qual se refere, explica-se. Um *e-book* trata-se de um bem digital com conteúdo econômico, portanto um bem jurídico apreciável economicamente. Os dados de um usuário em uma rede social, para este, tratam-se de um bem digital sem conteúdo econômico – bem jurídico imaterial sem apreciação econômica, pois ligado a faceta da pessoalidade daquele usuário. Contudo, pode-se afirmar que o conjunto de informações extraídas dos vários perfis de redes sociais, para o provedor, trata-se de um bem digital com conteúdo econômico – bem jurídico imaterial com apreciação econômica, visto que pode ser usado para traçar perfis de consumidores, ou até mesmo ser cedido de forma onerosa a terceiros se previsto em termos de uso de serviço (Almeida, 2019, p. 42).

A cantora internacional Madonna, após ficar internada gravemente, elaborou modificações em seu testamento, restringindo o uso de sua imagem, caso viesse a falecer, vedando que herdeiros monetizassem seu holograma. A atriz Whoopi Goldberg proibiu em seu testamento que sua imagem seja reproduzida em holograma digital após sua morte (Decaris, 2023). No Brasil, em 2023, ganhou repercussão o comercial da *Volkswagen*, que comemorava os 70 anos da marca, utilizando IA e computação gráfica para unir Elis Regina (1945-1982) a sua filha Maria Rita, para juntas cantarem "Como Nossos Pais", de Belchior. Questionou-se a utilização ética e moral da imagem da cantora, sobretudo quanto à sua aprovação para a utilização da imagem associada à marca e questões ideológicas e políticas, o

que motivou, inclusive, a abertura de processo ético perante o Conselho de Autorregulamentação Publicitária (CONAR). A empresa afirmou que o objetivo era criar um momento único e a utilização da imagem da cantora já falecida teria sido permitida pela família (Figueira; Renzetti Filho; Luca, 2023).

A greve dos roteiristas e atores de *Hollywood*, ocorrida em 2023, teve como uma de suas reivindicações regras claras e justas em relação à utilização da IA nas produções, o que tem se tornado cada vez mais frequente. As discussões abrangem o direito ao uso de imagem, a substituição por IA e a precarização das relações trabalhistas. Em um espaço relativamente curto de tempo de trabalho, é possível replicar a voz[18], o rosto, os movimentos e os gestos de profissionais sem precisar que estes estejam sempre filmando. Os *softwares* de IA podem replicar cenas inteiras a partir do material um dia coletado. Constata-se que a tecnologia pode utilizar a identidade humana como matéria-prima, basta que estes direitos sejam negociados[19]. Já os roteiristas são contra a utilização de trabalhos já realizados para alimentar e ensinar *chatbots* a escreverem e gerarem escrita em estilo semelhante ou que serviços de IA reescrevam ou refinem rascunhos de trabalhos para cenas ou programas inteiros (Lopez; Jackson, 2023; Barnes; Koblin, 2023). O futuro do trabalho[20] de toda uma indústria se encontra, de certa forma, ameaçado.

No que se refere ao direito à imagem, verifica-se que o titular pode dispor de sua imagem em situações determinadas, contudo, este não perde o controle sobre esta, pois, sob a perspectiva do Código Civil, este direito da personalidade seria intransmissível (Siqueira; Vieira, 2022). A autorização do titular não encerra o controle quanto à legitimidade para o uso da imagem, pelo contrário, deve ser apenas um ponto de partida. Em que pese a autorização, o uso da imagem deve ser

[18] Em 2024, a atriz norte-americana Scarlett Johansson se insurgiu contra a empresa *OpenIA*, depois que usuários da plataforma de inteligência artificial apontaram a semelhança de sua voz com a da opção de voz "*Sky*" do *ChatGPT* (robô virtual – *chatbot*). Em pronunciamento, a atriz afirmou que, meses antes, chegou a receber oferta para emprestar sua voz ao sistema, mas que teria recusado por motivos pessoais. A empresa negou ter utilizado a voz da atriz e se pronunciou no sentido de que alteraria a opção (McMahon, 2024).

[19] "O trabalho sem corpo da era do *software* não mais amarra o capital: permite ao capital ser extraterritorial, volátil e inconstante. A descorporificação do trabalho anuncia a ausência de peso do capital. Sua dependência mútua foi unilateralmente rompida: enquanto a capacidade do trabalho é, como antes, incompleta e irrealizável isoladamente, o inverso não mais se aplica. O capital viaja esperançoso, contando com breves e lucrativas aventuras e confiante em que não haverá escassez delas ou de parceiros com quem compartilhá-las" (Bauman, 2021, *online*).

[20] "o trabalho perdeu a centralidade que se lhe atribuía na galáxia dos valores dominantes na era da modernidade sólida e do capitalismo pesado. O trabalho não pode mais oferecer o eixo seguro em torno do qual envolve fixar autodefinições, identidades e projetos de vida. Nem pode ser concebido com facilidade como fundamento ético da sociedade, ou como eixo ético da vida individual" (Bauman, 2021, *online*).

controlado de forma contínua, com o intuito de evitar abusos e excessos, até porque, não se pode permitir que a anuência seja utilizada para invocar a legitimação do uso de imagem que, por razões óbvias, não seriam consentidos pela pessoa, ou ainda, que se mostrem contrários à tutela da dignidade (Schreiber, 2014).

O contrato, portanto, não seria capaz de transferir a titularidade do direito à imagem, mas apenas a autorização para o seu uso, bem como a divulgação e a publicação. "A exposição e o uso desse conteúdo devem estar contextualizados à circunstância em que foi cedido voluntariamente pelo usuário" (Siqueira; Vieira, 2022, p. 21). Assim, no caso do episódio *Joan is awful*, tanto Joan como Salma poderiam fazer cessar, a qualquer momento (Zanini, 2018, p. 245), o uso da imagem que extrapolasse os limites do negócio jurídico.

6. DIREITO À IMAGEM E A AMEAÇA DAS *DEEPFAKES* NAS REDES SOCIAIS

Em que pese a proteção jurídica concedida ao direito à imagem pelo ordenamento jurídico brasileiro, sobretudo em relação à conceituação e à sua proteção como um direito fundamental e da personalidade, previsto tanto na Constituição Federal de 1988 como no Código Civil de 2002, verifica-se que ainda existe uma lacuna quanto à utilização da imagem nas redes sociais, sobretudo diante das *deepfakes*, já que, inúmeras vezes, sequer existe uma relação contratual entre o ofensor e a vítima, contexto que não tem impedido que a imagem de muitas pessoas, sobretudo figuras públicas, seja atingida negativamente no âmbito virtual. Como pontua Filipe Medon (2021, p. 252), as técnicas de reconstrução digital impactam consideravelmente "não só a estrutura do que se entende por imagem, como, sobretudo, as formas de se causar danos imagem de uma pessoa, elevando esse potencial lesivo a patamares impensados num passado não muito distante".

Vive-se, atualmente, um cenário em que todo conteúdo *online*, antes de ser levado a sério, deve ser checado. Na Internet, perfis são criados para a exploração de terceiros, "visando finalidades maliciosas ou comerciais, ante a ausência de uma regulamentação clara, que aborde tais aspectos" (Figueira; Renzetti Neto; Luca, 2023, p. 536). É o que ocorre, por exemplo, com o Dr. Dráuzio Varella, cuja imagem é constantemente utilizada em vídeos adulterados nas redes sociais, que fazem parecer que o médico conhecido nacionalmente endossa legendas mentirosas ou vende produtos não autorizados por agências sanitárias, assim como que as vacinas seriam transgênicas, alterariam o DNA e causariam câncer (Domingos, 2024).

A expressão "*deepfake*" passou a ser utilizada para "designar os vídeos falsos desenvolvidos em sistemas de Aprendizado Profundo e IA" (Siqueira; Vieira, 2022, p. 16). As *deepfakes* podem ser conceituadas como conteúdo gerado por IA que manipula imagens, áudio e vídeo (Fragale; Grilli, 2024). Como destacam Mulholland e Oliveira (2021), Kietzmann *et al*. (2020) e Citron e Chesney (2019), as *deepfakes* são um fenômeno recente, sendo que as primeiras manipulações digitais hiper-realistas e de grande ubiquidade que receberam tal nome remetem ao ano de 2017. A sua utilização abrange desde a criação de vídeos humorísticos e de cunho

educacional até a falsificação de vídeos de conteúdo pornográfico, geralmente utilizados para fins de *revenge porn*, e a manipulação de falas de políticos e celebridades. Apesar de seus benefícios[21], inúmeros são os riscos e as ameaças postas por essa nova tecnologia.

Uma *deepfake* pode ser utilizada para fazer crer que alguém disse algo que nunca diria, fez algo que nunca faria ou esteve em uma situação que jamais aconteceu. Tal contexto também pode gerar golpes, fraudes e tentativas de manipular a agenda pública e o debate democrático, o que inclui a possibilidade de obter dados pessoais sensíveis, senhas bancárias e contas de e-mail, fingir que parentes ou amigos estão pedindo empréstimo ou transferências bancárias ou exigir pagamento de resgate diante de falso sequestro (Brasil, 2024).

Segundo seu relatório anual, a empresa *Sensity* (2024) identificou, no ano de 2024, 2.298 ferramentas de troca de rosto, sincronização labial, *face reenactment* e avatares de IA; 10.206 ferramentas para a geração de imagens de IA; 1.018 ferramentas para a geração de voz de IA e clonagem de voz; e 47 ferramentas para *deepfake* com injeção de *KYC*. Como destaca Medon (2021, p. 263):

> [...] seja qual for o meio tecnológico adotado para se criar uma imagem falsa, já se pode apontar dois traços característicos, quais sejam, o emprego de técnicas computacionais avançadas, comumente de inteligência artificial, assim como o grau tão elevado de realidade que faz com que seja quase impossível se detectar a fraude, o que é especialmente perigoso nos tempos atuais, marcado pela "economia da atenção".

No âmbito internacional, Fragale e Grilli (2024) destacam a preocupação atual com a utilização de *deepfakes* no cenário político e de eleições. Em 2024, Elon Musk, *CEO* da rede social *X* (antigo *Twitter*), compartilhou em seu perfil na plataforma uma paródia da campanha de Kamala Harris, então candidata à presidência dos Estados Unidos. O vídeo, com versão manipulada por IA, utilizava a imagem e a voz da Kamala para expô-la como uma candidata incompetente. Ainda, pontuam a utilização de *deepfakes* para a manipulação política nas redes sociais e a disseminação de desinformação no âmbito do conflito entre a Rússia e a Ucrânia.

[21] Conforme pontuam Siqueira e Vieira (2022, p. 17), "o desenvolvimento desta tecnologia traz consigo uma série de benefícios, como na indústria cinematográfica, a diminuição de custos para execução de efeitos especiais, cenas de risco para atores e dublês virtualmente adicionadas, envelhecimento ou rejuvenescimento dos atores, a criação de cenas ou até documentários e filmes com atores já falecidos. Os *softwares* poderiam auxiliar na terapia por videoconferência e garantir o sigilo daqueles que não querem se identificar. Ou, ainda, para entrevistas de emprego sem vieses de gênero ou raça. Também, celebridades e influenciadores digitais poderiam vender suas imagens para anunciantes sem precisar comparecer às filmagens".

Outro conflito atual em que há exponencial utilização de ferramentas de IA para a manipulação político-ideológica é o entre Israel e a organização de ideologia religiosa islâmica (sunita) Hamas. A propaganda do Hamas tem feito uso de imagens geradas por IA para retratar moradores de Gaza, sobretudo crianças, ao lado de escombros de casas com pessoas mortas e feridas. Já do lado israelita, verificou-se a criação de imagens retratando grandes multidões com suas bandeiras militares e vídeos com sincronização labial e clonagem de voz, bem como celebridades globais expressando seu apoio a Israel (Sensity, 2024).

Em janeiro de 2025, durante a temporada de incêndios que assolou bairros em Los Angeles, na Califórnia, várias *deepfakes* se espalharam na rede, incluindo fotos e vídeos que mostravam o letreiro de *Hollywood*[22] e outros locais em chamas, de modo que, posteriormente, precisaram ser desmentidos (Garcia, 2025; Reuters, 2025; USA Today, 2025).

Nos Estados Unidos, a discussão das *deepfakes* gira em torno da irresponsabilidade das plataformas. Autores como Chesney e Citron, com base no *Communications Decency Act (CDA)*, apontam que não seria possível proibir de forma abstrata tal conteúdo. Para não frear a inovação tecnológica, a saída para a responsabilização seria exigir prova da intenção de enganar e a comprovação da evidência de prejuízo. Destacam que a Constituição americana não proíbe o discurso falso, com base na concepção de que a sua proibição arrefeceria o discurso verdadeiro. Logo, a mentira só não é protegida em três hipóteses: a) difamação de pessoas privadas; b) fraudes; c) em caso de tentativa de furto de identidade de oficias do governo (Medon, 2021; Chesney; Citron, 2019). Em razão da gravidade das *deepfakes* para fins de pornografia de vingança (*revenge porn*), tal prática chegou a ser criminalizada por vários estados americanos, a exemplo de Maryland, da Virgínia e da Califórnia (Medon, 2021; Molina; Berenguel, 2022).

Em julho de 2020, por exemplo, a empresa *Sensity* apurou a propagação de mais de cem mil imagens de conteúdo pornográfico que foram criadas por usuários da rede social *Telegram* a partir de imagens utilizadas por mulheres, de todas as idades, incluindo crianças e adolescentes, em redes sociais. Pontua-se que tal estimativa não compreendeu as *deepfakes* criadas e não compartilhadas na rede (Pinto; Oliveira, 2023).

Uma das tentativas de evitar maiores prejuízos diante das *deepfakes* é rotular o conteúdo nas plataformas, indicando a utilização de IA nas postagens. Como destacam Fragale e Grilli (2024, *online*), a rotulagem de conteúdo gerado por IA "melhora a transparência e a confiança, ajudando os usuários a reconhecerem

[22] "Assim que o incêndio do Sunset começou a devastar Runyon Canyon, em Hollywood Hills, na noite de quarta-feira, uma foto gerada por IA do letreiro de Hollywood em chamas estava circulando rapidamente nas redes sociais. Esse foi apenas um exemplo de desinformação sobre os incêndios na área de Los Angeles se espalhando nas redes sociais, e especialistas alertam que informações falsas durante desastres naturais atrapalham os esforços de recuperação e prejudicam a confiança da comunidade" (Garcia, 2025, *online*, tradução nossa).

material gerado por máquina e permitindo que os indivíduos tomem decisões informadas sobre o conteúdo que consomem". Na visão dos autores, a transparência está aumentando, com plataformas "garantindo que os usuários sejam informados sempre que encontrarem imagens aprimoradas por IA aparecendo em suas telas, uma vez que essa mídia pode ser uma ferramenta poderosa para persuasão e engano".

Em 2023, a rede social *Tiktok* anunciou que havia desenvolvido uma ferramenta para detectar e divulgar conteúdo gerado por inteligência artificial e postado por criadores na plataforma. Em 2024, a empresa *Meta* lançou tecnologias para detectar e rotular o conteúdo gerado por IA nas redes sociais *Facebook*, *Instagram* e *Threads*, tendo por intuito que os usuários saibam que a IA está envolvida no processo de criação das postagens, bem como marcas d'água invisíveis e metadados em arquivos de imagem e vídeo (Fragale; Grilli, 2024).

Em agosto de 2024, entrou em vigor no âmbito da União Europeia o *AI Act*, com o intuito de regular sistemas de inteligência artificial e combater notícias falsas (*fake news*). O Regulamento (UE) 2024/1689 estabelece regras para a utilização da IA e aborda seus riscos, tendo por objetivo garantir que os sistemas de IA respeitem direitos fundamentais, a segurança e princípios éticos. A normativa classifica[23] os sistemas de IA de acordo com os riscos que acarretam e impõem obrigações específicas de transparência aos desenvolvedores e provedores. O artigo 99 da Lei de IA descreve penalidades para a não conformidade de desenvolvedores e implantadores: o não cumprimento das regras implica uma penalidade financeira de 35 milhões de euros ou, se superior, 7% do faturamento anual mundial do ano financeiro anterior. Assim, a execução das obrigações sob a Lei de IA é garantida por multas administrativas (Fragale; Grilli, 2024; UE, 2024).

Para Fragale e Grilli (2024) o *IA Act* e outras intervenções legislativas podem contribuir para promover maior vigilância quanto aos sistemas de IA, fornecer diretrizes para o desenvolvimento e garantir que as *deepfakes* sejam mais rapidamente detectadas. Os autores questionam se as penalidades financeiras seriam suficientes para efetivamente coibir infrações, considerando especialmente a rapidez com que o conteúdo é compartilhado nas redes e contextos sensíveis e que podem influenciar a opinião pública e prejudicar os processos democráticos, como a época de eleições. Compreendem que é necessária a combinação de fortes tecnologias de detecção, com parcerias intersetoriais e a conscientização do público das redes sociais de que está lidando com conteúdo gerado por IA, isto é, é crucial realizar uma análise plausível de notícias, imagens e outras mídias, questionar

[23] Por exemplo, "a tecnologia de IA usada em infraestruturas críticas, como transporte, é considerada de alto risco, sendo capaz de colocar a vida e a saúde dos cidadãos em risco e, portanto, está sujeita a regulamentação mais rigorosa; por outro lado, filtros de spam e videogames habilitados para IA são classificados como de risco mínimo e, como tal, estão sujeitos a pouca ou nenhuma regulamentação" (Fragale; Grilli, 2024, *online*, tradução nossa).

fontes e considerar que as postagens podem ter sido criadas com ferramentas de IA. Como ressaltam Molina e Berenguel (2022, p. 7), "é alarmante o número de pessoas que repassam *fake news* sem ao menos verificar a fonte ou tal informação".

Fragale e Grilli (2024) pontuam eventuais dificuldades advindas após a aprovação do *IA Act*, citando que os países da União Europeia possuem estruturas regulatórias variadas, o que dificulta a criação de uma abordagem única para a questão das *deepfakes*. A Lei de IA não especificou qual regulador deveria atuar como autoridade de vigilância, de modo que os Estados-Membros da UE devem adotar as próprias estruturas nacionais quanto às penalidades, o que gera diferenciação na aplicação entre os Estados. Os autores mencionam que a Espanha criou um órgão regulador *ad hoc* para observar o desenvolvimento da IA, já a Itália aprovou um projeto de lei sobre IA. Por outro lado, países como a França ainda não têm uma lei ou um órgão dedicado a regular a IA. Além disso, as obrigações de transparência podem entrar em conflito com o *Digital Service Act* (DAS), legislação de 2022, que passou a ser totalmente aplicável em fevereiro de 2024 e que incorpora obrigações para as plataformas *online* quanto à responsabilidade, a mecanismos de apelação, avaliação de risco sistêmico e publicidade *online*.

Ainda, Fragale e Grilli (2024) alertam que, a depender da sofisticação da *deepfake*, esta pode escapar até mesmo dos sistemas de detecção. Quanto às penalidades estabelecidas pela normativa da UE, compreendem que estas podem ser eficazes como um impedimento, já que tendem a impactar mais organizações financeiramente relevantes, sendo, muitas vezes, insuficientes para coibir atores menores e que atuam em jurisdições em que a fiscalização ainda é muito deficitária.

Pinto e Oliveira (2022) destacam o exemplo da Alemanha, que se tornou referência mundial diante da entrada em vigor da Lei de Fiscalização da Rede (*NetzDG*), que possibilitou a autorregulação das plataformas e estabeleceu o prazo de 24 horas para a remoção de conteúdo após uma simples notificação, sob pena de multa, além da obrigatoriedade de divulgação de relatórios para fins de transparência, de forma que tal solução para a remoção e o bloqueio do conteúdo ilícito não necessita de atuação do Poder Judiciário. Apesar da inovação, a lei foi alvo de críticas diante da possibilidade de dar margem ao *overblocking* de publicações que tivessem em conformidade com a legislação, o que, de fato, aconteceu logo após sua entrada em vigor. De igual modo, identificou-se que grande parte das denúncias eram referentes a conteúdo que não infringia a legislação, de modo que cabia aos provedores a responsabilidade de interpretar quais seriam as publicações realmente ofensivas, o que abriria espaço para interpretações equivocadas.

No Brasil, em 2024, o tema das *deepfakes* ganhou relevância no âmbito do Supremo Tribunal Federal (STF) diante da criação do Programa de Combate à Desinformação, em parceria com a Rede Nacional de Combate à Desinformação (RNCD), objetivando transmitir aos jovens informações sobre o combate a *fake news* a partir de ferramentas digitais disponíveis, estimulando a produção de conteúdo

com responsabilidade (STF, 2024). O referido Tribunal também lançou o "Guia Ilustrado contra as *Deepfakes*", cujo escopo é apresentar, em linguagem facilitada, informações essenciais para a plena compreensão do problema, incluindo instruções para que as pessoas possam identificar, evitar e denunciar a circulação de *deepfakes*. Nos termos do guia, as *deepfakes* podem ser consideradas "uma versão sofisticada de *fake news*. São, portanto, ferramentas de engano mais modernas e mais perigosas, capazes de imitar pessoas e simular acontecimentos reais, criando falsidades difíceis de serem detectadas" (Brasil, 2024).

Como menciona o material, as formas mais comuns de *deepfake* envolvem: a) a substituição de um rosto por outro (ex.: *face-swap* ou troca-de-face); b) a clonagem de voz: trejeitos e aparência, para gerar um vídeo em que a pessoa clonada reproduz todas as falas e os movimentos realizados por um ator (*pupper-master* ou jogo do ventríloquo); c) a adulteração da região da boca, de modo que o movimento dos lábios acompanha um áudio acrescentado (*lip-sync* ou sincronização labial) (Brasil, 2024).

As *deepfakes* mais sofisticadas são produzidas com o uso de redes generativas adversárias (conhecidas como GANs, GENERATIVE ADVERSARIAL NETWORKS). Em uma GAN, dois algoritmos competem entre si: o primeiro possui a função de gerar conteúdo falso indetectável, já o segundo tenta descobrir e apontar as falhas do primeiro. Assim, o primeiro algoritmo é constantemente aprimorado, de forma que consegue produzir resultados cada vez mais reais. Há casos de *deepfakes* que são criadas a partir de técnicas menos complicadas, como a simples redução da velocidade da fala, o que faz parecer que o sujeito está bêbado. Tais vídeos adulterados recebem o nome de "*cheapfakes*", por se tratarem de falsificação menos sofisticada (Brasil, 2024).

O guia cita possíveis falhas que podem ser observadas e que denunciam que o conteúdo é fraudulento: a) *deepfake* de vídeo: diferença entre o tom da pele do corpo e a tonalidade do rosto; anormalidade no movimento dos olhos ou falta de naturalidade nas expressões; ausência de marca da pessoa, como uma tatuagem, uma pinta ou um sinal; alterações, ainda que leves, no sotaque, na entonação ou na voz; falta de sincronia entre o movimento dos lábios e a fala; rigidez ou falta de naturalidade no movimento corporal; elementos com aparência artificial, como a iluminação, o cenário, as cores e a própria expressão das pessoas reproduzidas no vídeo; b) *deepfake* de imagens: sombra apagada ao redor dos olhos; o fundo ou a paisagem não condiz com o local dos fatos; tonalidade da cor diversa das demais partes do corpo; assimetria visível - ex.: ausência de brinco em uma das orelhas; encaixe imperfeito entre a cabeça e o pescoço e algo estranho no interior da boca, tendo em vista que as ferramentas não são boas em reproduzir a língua; detalhes estranhos, como rosto, braços e pernas desproporcionais; roupas incompatíveis com o lugar ou as demais pessoas que aparecem no registro; c) *deepfake* de áudio: voz, entonação, sotaque e/ou vocabulário incompatíveis com os registros vocais ou o modo de ser da pessoa em questão; inconsistência no tempo e quanto à reação

entre as falas dos interlocutores em um diálogo; falta de diferença de volume ou equalização entre as falas; interrupções abruptas de palavras, ideias ou frases, o que denuncia a presença de cortes ou edições (Brasil, 2024).

O material alerta que, em razão do grau de sofisticação e da qualidade, as *deepfakes* representam "riscos à saúde do debate público, a direitos individuais, como a honra, a imagem e o acesso a informações adequadas, e à normalidade de processos sociais sensíveis, como as eleições" (Brasil, 2024). Orienta que as falsidades profundas podem ser denunciadas por meio dos canais destinados ao "envio de apontamentos sobre violação de regras de comunidade ou termos de uso". Já se a falsidade representar atentado contra as eleições, a exemplo de *deepfakes* contra a urna eletrônica ou o trabalho realizado pela Justiça Eleitoral, as "as denúncias podem ser feitas no seguinte endereço: https://www.tse.jus.br/eleicoes/sistema-de-alertas". Além disso, as denúncias sobre desinformação e o processo eleitoral em redes sociais podem ser encaminhadas ao Tribunal Superior Eleitoral (TSE) "por telefone, por meio do disque-denúncia SOS Voto[24], através do número 1491" (Brasil, 2024). Diante da preocupação com a manipulação da informação durante as eleições municipais de 2024, o TSE regulamentou o uso da inteligência artificial na propaganda de partidos, federações partidárias e candidatas e candidatos. A Corte aprovou 12 resoluções, relatadas pela vice-presidente do TSE, a Ministra Cármem Lúcia, que tinham por objetivo disciplinar as regras aplicadas ao processo eleitoral daquele ano (TSE, 2024).

Alterando a Resolução nº 23.610/2019, que trata de propaganda eleitoral, o TSE dispôs sobre a proibição das *deepfakes*, a obrigação de aviso quanto ao uso de IA na propaganda eleitoral, a restrição da utilização de robôs para intermediar o contato com o eleitor (a campanha não poderia simular diálogo com um candidato ou qualquer outra pessoa) e a responsabilização das *big techs* que não retirassem do ar, de forma imediata, conteúdo com discurso de ódio, desinformação, ideologia nazista e/ou fascista, além de antidemocrático, racista e homofóbico. O art. 9º-C proibiu a utilização, na propaganda eleitoral, 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", sob pena de caracterizar "abuso de utilização dos meios de comunicação, acarretando cassação do registro ou do mandato, bem como apuração das responsabilidades, nos termos do artigo 323 do Código Eleitoral". Enquanto o art. 9º-E estabeleceu a "responsabilização solidária dos provedores, de forma civil e administrativa, caso não retirem do ar, imediatamente, determinados conteúdos e contas, durante o período eleitoral" (TSE, 2024).

[24] "O SOS Voto funciona de segunda a sexta, das 8h às 20h, e no sábado das 9h às 17h, tendo capacidade para receber até mil ligações diárias. Por fim, se as *deepfakes* envolverem a possibilidade de crime, como usurpação de identidade, golpes ou atentados contra a honra ou a imagem das pessoas, é possível reportá-las pelo telefone, acessando o Disque Denúncia (181)" (Brasil, 2024).

Em consulta no *site* do Supremo Tribunal Federal (STF) pelo termo "*deepfake*", a presente pesquisa encontrou 1 (um) julgado, referente aos autos de Ação Penal nº 1021, com julgamento em 18 de agosto de 2020. No caso em questão, o Deputado Federal Jean Wyllys de Matos Santos imputou ao Deputado Federal Eder Mauro a prática de crime de difamação agravada (artigos 139 c/c art. 141, II e III, do Código Penal), tendo em vista uma publicação ofensiva à honra do querelante, divulgada na página do querelado na rede social *Facebook*, em 2015. O vídeo continha um trecho recortado da fala de Jean Wyllys em uma reunião da Comissão Parlamentar de Inquérito, previamente editado, de modo a inverter seu conteúdo. No material fraudulento, o Deputado aparece falando o seguinte: "uma pessoa negra e pobre é potencialmente perigosa, é mais perigosa do que uma pessoa branca de classe média, essa é a verdade, então, dito isso [...]" (Brasil, 2020).

Conforme consta nos autos, a publicação havia recebido 14.834 aprovações ("curtidas"), 252.458 visualizações e 12.272 compartilhamentos, gerando impacto substantivo e absolutamente negativo, até que foi excluída após decisão da 14ª Vara Cível de Brasília/DF, de 28 de agosto de 2015. A Corte julgou procedente a acusação para o fim de condenar o réu Éder Mauro pela prática do crime de difamação agravada, no sentido de que:

> [...] restou evidenciado o conhecimento da edição voltada à adulteração do conteúdo por parte do Réu, porquanto se tratava de manifestação absolutamente contrária à proferida pelo parlamentar Autor, em debate do qual o próprio réu participou e cujo conteúdo era de seu inteiro conhecimento. Aliás, provou-se, no interrogatório judicial, a plena consciência do Réu de que o vídeo divulgado em seu perfil no Facebook, com centenas de milhares de visualizações, atribuía ao Autor, Jean Wyllys, ideias diametralmente opostas às que identificam a plataforma política deste parlamentar. (e) A divulgação do conteúdo fraudado, invertendo-lhe o sentido com finalidade de difamar o Autor, constitui etapa da execução do crime, estabelecendo a autoria criminosa do divulgador, a qual não exclui a do programador visual ou do editor responsável pela execução material da fraude, quando promovidas por outros agentes em coautoria [...] (Brasil, 2020).

Além disso, consta no *site* do STF uma decisão monocrática proferida nos autos de Reclamação nº 72.310/ES, com julgamento em 4 de outubro de 2024. A ação discutiu a retirada de conteúdo do veículo de imprensa Espaço Ócio Criativo Comunicação Ltda., que foi compelido a retirar a matéria publicada em seu *site*: 'Exclusivo: Gravações revelam que secretário de obras de Vitória negocia planilhas com empreiteiros'. A Corte considerou que, diante da análise do conteúdo e dos áudios divulgados na matéria, havia exposição do nome do autor (Paulo Marcelo Paranhos Retto de Queiroz) que ultrapassava o mero direito à informação, eis que

lhe seriam imputados fatos como se fossem verdadeiros, sem qualquer notícia concreta de que seriam reais. O texto da matéria levava a crer que o autor estaria negociando obras e planilhas com empreiteiros. Os áudios teriam qualidade acústica comprometida, necessitando de verificação quanto à integralidade. O conteúdo extrapolava o caráter informativo e veiculava fatos de caráter supostamente caluniosos, de modo que foi deferida a tutela de urgência para determinar a retirada da matéria, fixada multa diária em caso de descumprimento e o reconhecimento de que não havia ocorrido censura prévia do conteúdo publicado, tendo sido negado o seguindo da reclamação (Brasil, 2024).

Já a consulta de jurisprudência pelo *site* do Superior Tribunal de Justiça (STJ) com o termo "*deepfake*" encontrou duas decisões monocráticas (nos autos de *Habeas Corpus* nº 972.309 e Resp nº 2.089.383). O HC nº 972.309, com julgamento em janeiro de 2025, discutia suposta prática dos crimes de violência política, associação criminosa, ameaça e injúria racial contra a Deputada Estadual do Rio Grande do Sul e sua filha, diante do recebimento de *e-mail* proferindo ofensas e ameaças. Também foi alegada a utilização de *deepfake* e de inteligência artificial pelo acusado, mas este não era o cerne da discussão. O *writ* não foi conhecido por ausência de regularidade formal, diante da inadequação da via eleita (Brasil, 2025).

Já quanto ao Recurso Especial nº 2.089.383/SP, interposto pelo *Facebook* contra o acórdão do Tribunal de Justiça do Estado de São Paulo, o agravante foi condenado em ação de obrigação de fazer para o fim de excluir de sua rede social todos os compartilhamentos do *link* de uma notícia falsa e fornecer os registros de acesso da pessoa que fez o primeiro compartilhamento na rede, limitados às informações disponíveis em seus servidores. Em grau de apelação, foi reconhecida a obrigação de fornecimento da porta lógica de origem. A Corte se manifestou no sentido de impossibilidade de discussão dos termos que levaram à formação do julgado na referida sede processual, assim também pontuando (Brasil, 2023):

> [...] se é ou não possível pelo título da reportagem ilícita, que foi milhares de vezes compartilhada com o mesmo teor, localizar quem o fez primeiro, tal questão diz respeito à expertise tecnológica, não sendo a seara do recurso especial o ambiente processual propício para tal verificação técnica. Com o avanço tecnológico tão acelerado no mundo contemporâneo, como por exemplo com o crescente número de aplicativos que realizam a técnica do *deepfake*, não é a instância especial do STJ a seara processual adequada para investigar se realmente não há tecnologia eficiente para identificação do primeiro usuário compartilhador da referida notícia falsa[25] (Brasil, 2023).

[25] Ainda conforme decisão da referida Corte: "ao contrário, na hipótese concreta, está devidamente especificada a postagem que se busca remover, qual seja, um *link* que foi compartilhado mais de 71 mil vezes. O texto do referido link é único e indubitavelmente incontroverso, e, conforme explicitado na instância originária, as postagens podem ser facilmente identificadas até porque a

Pontua-se que, no caso relatado, objetivava-se remover uma postagem específica, cujo *link* havia sido compartilhado mais de 71 mil vezes na plataforma, bem como o rastreamento e a identificação do usuário que primeiro postou o conteúdo (Brasil, 2023).

No Brasil, a responsabilidade civil das plataformas é regulada, sobretudo, pelo Marco Civil da Internet. A regra real do art. 18 da normativa dispõe que o "provedor de conexão a` internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros". Já o seu art. 19 menciona que "responsabilidade civil do provedor de aplicações inicia-se a partir do recebimento da ordem judicial, que, ao cumpri-la, afasta uma possível responsabilização de ilícitos por terceiro". Enquanto o art. 21 pontua que a retirada de conteúdo pornográfico se dará mediante a notificação extrajudicial do usuário, de modo que o único critério estabelecido pelo legislador pela retirada do conteúdo é que os participantes não tenham autorizado a divulgação do vídeo (Medon, 2021; Gonçalves, 2017). Ressalta-se que, em 2018, o Código Penal brasileiro passou a prever a criminalização das montagens de *deepfake* que incluam o indivíduo em cena de nudez ou de ato sexual libidinoso de caráter íntimo, conforme o art. 216-B[26] (Medon, 2021).

Quanto à possibilidade de lucro com a intervenção, Medon (2021) cita como precedente o caso da atriz Giovanna Antonelli, julgado pelo STJ nos autos de Recurso Especial nº 1.698.701/ RJ, de relatoria do Ministro Ricardo Villas Bôas Cueva, em que a Corte entendeu que pela devida indenização à atriz diante de utilização não autorizada de sua imagem pela sociedade empresária Dermo

parte recorrente possui contador de número de compartilhamentos de cada postagem, conforme admitido por ela mesma, podendo ser feito, de consequência, a identificação do usuário que postou em primeiro lugar exatamente em decorrência da possibilidade admitida de rastreamento do conteúdo. Portanto, o caminho para identificação do usuário que fez a primeira postagem já está faticamente explícito, que é o rastreamento do *link* com o texto sabido de todos [...]. O Facebook, por seu turno, possui em sua plataforma contador do número de compartilhamentos de cada postagem, cabendo-lhe o rastreamento do conteúdo para fins de identificação de sua origem, tendo em vista que se cuida de ferramenta por ele próprio disponibilizada, competindo-lhe a observância do princípio da vedação do anonimato e de sua obrigação legal de guarda e disponibilização de dados que permitam a identificação dos usuários de seu provedor" (Brasil, 2023).

[26] CP - Art. 216-B. "Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes: Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa. Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo" (Medon, 2021).

Formulações Farmácia de Manipulação Ltda. em campanha publicitária do produto "Detox". A indenização não se deu apenas com base em ofensa a atributos morais da imagem, mas também diante do enriquecimento proporcionado à indústria.

Como destaca Medon (2021, p. 276), hodiernamente, chegou-se a um ponto em que "a sofisticação tecnológica demanda respostas ainda mais criativas, dada a velocidade na transmissão de conteúdos na internet e o potencial lesivo daí resultante". Como observa o autor, "trata-se, assim, de um problema novo, que ainda precisa ser encarado de forma mais detida pela doutrina e, sobretudo, pela sociedade civil", pautando-se o "debate pela inafastável certeza de que a educação digital das pessoas tem o poder de contribuir para diminuir os impactos da desinformação e da circulação de imagens manipuladas". Ao mesmo tempo, ressalta o importante papel a ser desempenhado pelas plataformas e da criação de sistemas de IA e algoritmos capazes de auxiliar na identificação de conteúdo falso.

Mulholland e Oliveira (2021) pontuam que a Internet e as redes sociais não causaram o declínio da democracia representativa ou dos meios de expressão e participação política, de modo que as *deepfakes* dificilmente o farão. A partir dos argumentos de Jeanette Hoffmann, pontuam que é necessário compreender a *Internet* como um "campo de treinamento para se experimentar novas formas de agir democrático, tendo em mente que muitas das vezes os experimentos que realizamos (como as *deepfakes*) não deixarão as democracias inalteradas". Não se trataria, portanto, de tentar "prevenir ou abolir todos os efeitos negativos das *deepfakes*, mas sim de pensar como controlá-los e mediar seus efeitos problemáticos".

No Brasil, como pontuam Siqueira e Vieira (2022, p. 29), embora não exista uma norma específica que regule a IA, verifica-se como suficientes, em um primeiro momento, as normas civilistas sobre "os direitos de personalidade, o direito à imagem, a responsabilização civil e a reparação por danos ao uso indevido da imagem". De qualquer forma, é crucial a elaboração de uma norma que contenha diretrizes éticas e legais específicas sobre o uso da IA. Como pontuam os autores, "embora a tecnologia tenha transformado a forma de se captar a imagem de outrem, o direito à imagem, sua representação, utilização e divulgação devem cumprir com a função primária" de "assegurar à pessoa humana o livre desenvolvimento dos atributos de sua personalidade que, juntamente à imagem, compõem a dignidade humana".

Como destacam Oliveira e Ávila (2024, p. 16-17), a tecnologia "transforma a cada dia a forma de se capturar a imagem, mas permanece atual a advertência de que o norte de todo o esforço hermenêutico deve ser garantir que o direito à imagem" cumpra sua "função primacial de assegurar à pessoa humana o livre desenvolvimento dos atributos de sua personalidade, que compõem a sua dignidade".

Com base nos autores pesquisados, verifica-se que não seria viável, ou mesmo interessante, sob o ponto de vista da inovação tecnológica, coibir a criação e a utilização de *deepfakes* nas redes sociais, sobretudo diante da necessidade de respeito à liberdade de expressão. Contudo, a utilização da imagem para fins contrários aos pretendidos pelo indivíduo, tais como a possibilidade de criação de vídeos difamatórios, de conteúdo pornográfico ou que ensejassem ofensas a direitos fundamentais e da personalidade, bem como para o fim de gerar lucro sem o consentimento ou a autorização do titular, como ocorre no episódio *Joan is Awful*, da série *Black Mirror*, que introduziu a análise do presente trabalho, deve ser coibida para o fim de preservação da imagem e da dignidade da pessoa.

Constata-se que ainda há grande impasse no cenário mundial quanto à responsabilização das plataformas e à necessidade de retirada de conteúdo manipulado por IA das redes, o que também esbarra na questão da interpretação das postagens com ofensivas ou não pelos usuários e pelas próprias plataformas diante da decisão de retirada ou não do conteúdo e dos riscos de acenar somente para uma autorregulação por parte das plataformas.

6. CONCLUSÃO

O trabalho analisou a repercussão ao direito à imagem no episódio "*Joan is Awful*", da série *Black Mirror*, tendo em vista a utilização da imagem da personagem central por um serviço de *streaming* para fins vexatórios e alheios ao seu consentimento quando da assinatura e concordância com os termos de uso da plataforma. Em que pese o cenário utópico do enredo, o estudo problematizou como a circunstância enfrentada por Joan poderia ser contornada considerando a teoria dos direitos da personalidade, com ênfase na relação contratual e nos limites de utilização da imagem, para o fim de evitar abusos e excessos.

A hipótese inicial da pesquisa era a de que o uso da imagem não pode exorbitar os limites do negócio jurídico e que o contrato não é capaz de transferir a titularidade do direito, mas somente a autorização para o seu uso, bem como sua divulgação e publicação. O objetivo geral do trabalho consistiu em analisar os limites da disposição contratual a respeito do direito à imagem a partir da teoria dos direitos da personalidade, pontuando também a dificuldade atual de controle do uso da imagem nas redes sociais diante das *deepfakes*.

Para isso, foram traçados os seguintes objetivos específicos: descrever os principais acontecimentos do episódio da série de *streaming* que serviu como como pano de fundo para a investigação, tendo em vista os direitos da personalidade nele implicados; examinar a questão do direito à imagem à luz dos termos de uso, da proteção de dados pessoais e do consentimento com base na categoria teórica do "capitalismo de vigilância" de Shoshanna Zuboff; investigar o tema considerando a teoria dos direitos da personalidade; d) discutir as possibilidades de utilização, controle e legitimidade do uso da imagem diante do avanço tecnológico; e) analisar a problemática das *deepfakes* que circulam nas redes sociais.

A problemática explorada no episódio versa sobre a crise de consentimento do usuário das plataformas digitais, que para ter acesso a informações e serviços acaba concordando com os termos e as condições de uso das *Big Techs* sem ler o seu conteúdo ou compreender a real dimensão da coleta de dados e como estes podem ser utilizados no âmbito do capitalismo de vigilância, delineado por Zuboff. Hodiernamente, os dados pessoais são o principal insumo dos mercados financeiro e tecnológico (este último em expansão exponencial), já que as redes sociais, as páginas, os *sites* e os aplicativos, que costumam ser de utilização gratuita, coletam todos os dias informações sobre seus usuários e que podem impulsionar seu engajamento e aumentar seu valor de mercado e também ser úteis para empresas privadas e para o Estado.

Com a escalabilidade proporcionada pelo ambiente *online*, as plataformas digitais se tornaram grande vitrine para a publicidade e para pessoas/empresas que desejam anunciar negócios e serviços aos usuários destas redes. Assim, é um engano considerar que o usuário não paga pelo acesso a estes dispositivos, uma vez que a moeda de troca são seus dados, que se convertem em publicidade de produtos/bens/serviços de forma direcionada, com base em seus interesses, suas preferências e seus padrões de comportamento *online*. Esta economia que gira em torno dos dados dos usuários no ambiente virtual sustenta o capitalismo de vigilância.

Diante deste contexto e da cada vez maior relevância das *Big Techs* para a realização de atividades da vida cotidiana, o cidadão é transformado em consumidor, já que o consumo é a base do capitalismo. O cidadão é despido de seu caráter político, de reivindicação de direitos e garantias fundamentais, que questionamento acerca de hegemonia destas empresas e de sua possibilidade de crítica. Tendo em vista a necessidade de utilização destes aplicativos, ele acaba concordando com seus termos de adesão, sobretudo porque a não concordância significa exclusão de acesso a facilidades, que são pagas com a coleta de seus dados.

É interessante observar na série o conformismo com o qual os operadores do direito são retratados, o que releva também a atual dificuldade da seara jurídica de propor respostas a questões que giram em torno da tecnologia e da inteligência artificial. O papel e o trabalho dos artistas também são postos em xeque, sobretudo diante do avanço da inteligência artificial, com repercussões ao direito à imagem, mas também à intimidade, à honra, à privacidade e ao nome.

A inteligência artificial já é capaz de simular a voz de um cantor famoso, criar um mundo por meio de computação gráfica com a imagem de um ator renomado e escrever roteiros e textos, cenário que exige maior observância aos direitos da personalidade, a atualização de conceitos e da dimensão de proteção de direitos para tutelar o cidadão, que é renegado à posição de mero consumidor e alimentador passivo e não remunerado de dados fundamentais para o avanço da tecnologia, sobretudo da inteligência artificial.

A partir do problema suscitado e dos objetivos delineados no começo do trabalho, com base na teoria dos direitos da personalidade, foi possível confirmar que a hipótese de que a anuência do titular do direito à imagem não pode ser utilizada para invocar a legitimidade quanto ao uso para fins não consentidos ou, ainda, que se mostrassem contrários à tutela da dignidade, uma vez que isso significaria extrapolar os limites do negócio jurídico. O contrato, portanto, não é capaz de transferir a titularidade do direito, mas apenas a autorização para o seu uso, bem como sua divulgação e publicação. A autorização do titular não encerra o controle quanto à legitimidade para o uso da imagem, devendo ser apenas um ponto de partida. Desta forma, tanto a personagem Joan quanto a personagem Salma poderiam fazer acessar a lesão ou ameaça ao direito à imagem que extrapolasse os limites indicados no negócio jurídico.

Em que pese a proteção concedida pelo ordenamento jurídico brasileiro à imagem, um direito fundamental e da personalidade, verifica-se que as *deepfakes* espalhadas pelas redes sociais representam atualmente verdadeiro desafio ao Direito, sobretudo diante da velocidade com que as informações e publicações são criadas, postadas e compartilhadas nas plataformas. A retirada do conteúdo ofensivo *online* tem sido a solução até então encontrada para que a imagem das pessoas atingidas por este tipo de conteúdo seja preservada, assim como outros direitos. Contudo, tal medida envolve a interpretação quanto à falsidade ou não das informações tanto pelos usuários, que podem denunciar o conteúdo, como pelas próprias redes sociais.

Outra possibilidade destacada pelo presente trabalho é a de sinalização pelas plataformas de que o conteúdo foi manipulado por IA, como forma de demonstrar ao usuário que aquela postagem possui cunho falso/duvidoso. A pesquisa ressaltou a criação de leis e regulamentos ao redor do mundo, como o *NetzDG*, na Alemanha, o *IA Act*, no âmbito da União Europeia, e o Marco Civil da Internet, no Brasil, que tentam propor medidas e punições às plataformas e aos indivíduos que perpetrarem as ofensas em rede. Ao mesmo tempo, demonstrou que houve esforço das redes nos últimos anos para sinalizar e combater a desinformação, o que também pode ser observado no que se refere ao Poder Judiciário, especialmente quanto à manipulação da informação em períodos eleitorais e diante do risco aos processos democráticos estabelecidos. No Brasil, pontua-se como crucial a elaboração de uma lei específica que contenha diretrizes éticas e legais para regular tal problemática, ensejando maior proteção aos direitos fundamentais e da personalidade, como o direito à imagem.

REFERÊNCIAS

ALMEIDA, Juliana Evangelista de. **Testamento digital**: como se dá a sucessão dos bens digitais. Porto Alegre: Fi, 2019.

BARNES, Brooks; KOBLIN, John. On day 146, screenwriters reach deal with studios to end their strike. **The New York Times**, 5 set. 2023. Disponível em: https://www.nytimes.com/2023/09/25/business/media/hollywood-writers-strike-deal.html. Acesso em: 13 jun. 2024.

BAUMAN, Zygmunt. **Modernidade líquida**. Tradução: Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2021.

BITTAR, Eduardo Carlos Bianca. Direitos do consumidor e direitos da personalidade: limites, intersecções, relações. **Revista de Informação Legislativa**, Brasília, ano 36, n. 143, p. 63-70, jul./set. 1999.

BORGES, Roxana Cardoso Brasileiro. **Direitos da personalidade e autonomia privada**. 2. ed. São Paulo: Saraiva, 2007.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 13 jun. 2024.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 13 jun. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm?ref=blog.suitebras.com. Acesso em: 13 jun. 2024.

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]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 jun. 2024.

BRASIL. Superior Tribunal de Justiça (STJ). ***Habeas Corpus* nº 972.309**. Relator: Min. Reynaldo Soares da Fonseca, 9 de janeiro de 2025. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?livre=DEEPFAKE&operador=e&b=DTXT&thesaurus=JURIDICO&p=true&tp=T. Acesso em: 24 jan. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 2.089.383**. Relator: Min. Humberto Martins, 22 de setembro de 2023. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?livre=DEEPFAKE&operador=e&b=DTXT&thesaurus=JURIDICO&p=true&tp=T. Acesso em: 24 jan. 2025.

BRASIL. Supremo Tribunal Federal. Programa de Combate à Informação: sociedade informada, democracia forte. **Guia ilustrado contra as *deepfakes***. Brasília, DF: STF, 2024. Disponível em: https://portal.stf.jus.br/desinformacao/doc/Guia%20ilustrado%20Contra%20DeepFakes_ebook%20(1).pdf. Acesso em: 4 jun. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Penal nº 1.021**. Relator: Min. Luiz Fux, 18 de agosto de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur434530/false. Acesso em: 5 jan. 2024.

BRASIL. Supremo Tribunal Federal. **Reclamação nº 72.310/ES**. Relator: Min. Alexandre de Moraes, 4 de outubro de 2024. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/despacho1577236/false. Acesso em: 4 jan. 2024.

CHESNEY, Bobby; CITRON, Danielle. *Deep Fakes*: A looming challenge for privacy, democracy and national security. **California Law Review**, v. 107, p. 1753-1820, 2019.

COMBATE à desinformação: formas de *deep fake* são tema de último vídeo feito em parceria com STF: O projeto faz parte do Programa de Combate à Desinformação do STF, que está divulgando os vídeos produzidos por alunos da rede pública de Santos (SP). **Supremo Tribunal Federal (STF)**, 7 jan. 2024. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=493309&ori=1. Acesso em: 4 jun. 2024.

CUPIS, Adriano de. **Os direitos da personalidade**. Tradução: Adriano Vera Jardim e Antonio Miguel Caeiro. Lisboa: [s. n.], 1961.

DECARIS, Fernanda. Madonna proíbe uso de hologramas após sua morte. **Rolling Stone**, 11 jul. 2023. Disponível em: https://rollingstone.uol.com.br/noticia/madonna-proibe-uso-de-hologramas-apos-sua-morte/. Acesso em: 13 jun. 2024.

DINIZ, Maria Helena. **Curso de Direito Civil brasileiro**: teoria geral do direito civil. 32. ed. São Paulo: Saraiva, 2015.

DOMINGOS, Roney. É #FAKE que Drauzio Varella diz em vídeo que vacina da dengue é transgênica, altera o DNA e provoca câncer. **G1**, 20 fev. 2024. Disponível em: https://g1.globo.com/fato-ou-fake/noticia/2024/02/20/e-fake-que-drauzio-varella-diz-em-video-que-vacina-da-dengue-e-transgenica-altera-o-dna-e-provoca-cancer.ghtml. Acesso em: 13 jun. 2024.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FACHIN, Luiz Edson. **Estatuto jurídico do patrimônio mínimo**. Rio de Janeiro: Renovar, 2001.

FACHIN, Zulmar Antonio. **A proteção jurídica da imagem**. São Paulo: Celso Bastos Editor, 1999.

FACT Check: Hollywood sign not affected by Los Angeles wildfires. **Reuters**, 2025. Disponível em: https://www.reuters.com/fact-check/hollywood-sign-not-affected-by-los-angeles-wildfires-2025-01-09/. Acesso em: 10 jan. 2025.

FERMENTÃO, Cleide Aparecida Gomes Rodrigues. Os direitos da personalidade como direitos essenciais e a subjetividade do direito. **Revista Jurídica Cesumar – Mestrado**, v. 6, n. 1, p. 241-266, 2006.

FIGUEIRA, Hector Luiz Martins; RENZETTI FILHO, Rogério Nascimento; LUCA, Guilherme Domingos de. Herança digital e o caso Elis Regina: implicações jurídicas no uso da imagem de pessoas mortas pela inteligência artificial. **Revista Jurídica - UNICURITIBA**, v. 3, n. 75, p. 527-545, 2023.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como o sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, v. 12, n. 2, p. 1002-1033, 2021.

FRAGALE, Mauro; GRILLI, Valentina. Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation. **Columbia Journal of European Law**, 11 nov. 2024. Disponível em: https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/. Acesso em: 3 dez. 2024.

FRANÇA, Limongi. Nome Civil. *In*: SANTOS, João Manoel Carvalho (org.). **Repertório Enciclopédico do Direito brasileiro**. Rio de Janeiro: Borsoi, 1958.

GARCIA, Karen. L.A. firestorms bring waves of fire myths, disinformation. Here's how to debunk it and not get fooled. **The Los Angeles Times**, 10 jan. 2025. Disponível em: https://www.latimes.com/california/story/2025-01-10/debunking-social-media-fire-myths-no-the-hollywood-sign-didnt-burn. Acesso em: 10 jan. 2025.

GONÇALVES, Victor Hugo Pereira. **Marco Civil da Internet comentado**. São Paulo: Atlas, 2017.

HAN, Byoung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Veneza: Âyiné, 2020.

HERANÇA digital: advogada explica como ficam os bens após a morte. **Migalhas**, 25 jul. 2023. Disponível em: https://www.migalhas.com.br/quentes/390556/heranca-digital-advogada-explica-como-ficam-os-bens-apos-a-morte. Acesso em: 13 jun. 2024.

HOOFNAGLE, Chris Jay. Post Privacy's Paternalism. *In*: DIX, Alexander *et al*. (eds.). **Informationsfreiheit Und Informationsrecht**. Jahrbuch. Lexxion, 2012.

IKEDA, Walter Lucas; TEIXEIRA, Rodrigo Valente Giublin. Direitos da personalidade: terminologias, estrutura e recepção. **Revista Jurídica Cesumar – Mestrado**, v. 22, n. 1, p. 129-152, 2022.

JOAN is awful (temporada 6, ep. 1). Black Mirror [Seriado]. Direção: Ally Pankiw. Produção: Charlie Brooker e Annabel Jones. Estados Unidos: Netflix, 2023. 1 DVD (56 min.), son., color.

LEAL, Mônica Clarissa Hennig; PAULO, Lucas Moreschi. Algorítmos discriminatórios e jurisdição constitucional: os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial de amplo acesso. **Revista de Direitos e Garantias Fundamentais**, v. 24, n. 3, p. 165-187, 2023.

LOPEZ, German; JACKSON, Lauren. A Deal in Hollywood. **The New York Times**, 25 set. 2023. Disponível em: https://www.nytimes.com/2023/09/25/briefing/writers-strike-hollywood.html. Acesso em: 13 jun. 2024.

LUÑO, Antonio Enrique Pérez. **Derechos humanos, estado de derecho y constitucion**. 6. ed. Madri: Editorial Tecnos, 1999.

LUZ SEGUNDO, Elpídio Paiva; COUTO, Eliane Lopes. A Proteção de Dados e a Hipervulnerabilidade do Consumidor sob a Perspectiva do Consentimento e Privacidade na Internet. **Revista Jurídica Cesumar - Mestrado**, v. 22, n. 3, p. 551-566, set./dez. 2022.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade.
2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MARCELINO, Aldrey G. Meneghetti; FERMENTÃO, Cleide Aparecida Gomes Rodrigues. O direito ao nome e os direitos da personalidade. **Revista Jurídica Cesumar - Mestrado**, v. 7, n. 2, p. 531-548, 2007.

MCMAHON, Liv. Por que o ChatGPT vai deixar de usar voz parecida com a de Scarlett Johansson. **BBC News Brasil**, 21 maio 2024. Disponível em: https://www.bbc.com/portuguese/articles/cgll8eydde7o. Acesso em: 18 jun. 2024.

MEDON, Filipe. O direito à imagem na era das *deepfakes*. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 27, p. 251-277, jan./mar. 2021.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, v. 6, n. 2, p. 507-533, maio/ago. 2020.

MOLINA, Adriano Cezar; BERENGUEL, Orlando Leonardo. *Deepfake*: a evolução das *fake news*. **Research, Society and Development**, v. 11, n. 6, e56211629533, 2022.

MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. *In*: José Ribas Vieira (org.). **20 anos da Constituição cidadã de 1988**: efetivação ou impasse institucional? Rio de Janeiro: Forense, 2008. p. 369-388.

MOROZOV, Evgeny. **A ascensão dos dados e a morte da política**. São Paulo: Ubu, 2018.

MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues de. Uma nova cara para a política? Considerações sobre *deepfakes* e democracia. **Revista Direito Público**, v. 18, n. 99, 2021.

OLIVEIRA, Giovanna Aleixo Gonçalves; ÁVILA, Gustavo Noronha de. *Deep fake*, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital.
Revista Eletrônica do Curso de Direito da UFSM, v. 19, p. 1-19, 2024.

OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. *Cookies* de computador e história da internet: desafios à lei brasileira de proteção de dados pessoais. **Revista de Estados Jurídicos UNESP**, ano 22, n. 36, p. 307-388, 2018.

OTERO, Cleber Sanfelici; MASSARUTTI, Eduardo Augusto de Souza. Em conformidade com o direito fundamental à saúde previsto na Constituição brasileira de 1988, é possível exigir do estado a prestação de fosfoetanolamina sintética para pessoas com câncer? **Revista Jurídica Cesumar - Mestrado**, v. 16, n. 3, p. 847-876, 2016.

PARKER, Kim; HOROWITZ, Juliana Menasce. Majority of workers who quit a job in 2021 cite low pay, no opportunities for advancement, feeling disrespected. **Pew Research Center**, 9 mar. 2022. Disponível em: https://www.pewresearch.org/fact-tank/2022/03/09/majority-of-workers-who-quit-a-job-in-2021-cite-low-pay-no-opportunities-for-advancement-feeling-disrespected/. Acesso em: 13 jun. 2024.

PHOTO of burned Ohio mansion falsely linked to Diddy amidst 2025 fires | Fact check. **USA Today**, 15 jan. 2025. Disponível em: https://www.usatoday.com/story/news/factcheck/2025/01/15/diddy-mansion-burned-2025-fires-fact-check/77697526007/. Acesso em: 15 jan. 2025.

PINTO, Felipe Chiarello de; OLIVEIRA, Gabriela Franklin de. Não acredite em tudo que vê: *deepfake pornography* e responsabilidade civil no ordenamento jurídico brasileiro. **Direito & Política**, v. 18, n. 2, 2022.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 14. ed. São Paulo: Saraiva, 2013.

RAVINDRANATH, Mohana. How your health information is sold and turned into 'risk scores'. **Político**, 3 de fev. 2019. Disponível em: https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978. Acesso em: 13 jun. 2024.

SARLET, Ingo Wolfgang. As dimensões da dignidade da pessoa humana: construindo uma compreensão jurídico-constitucional necessária e possível. **Revista Brasileira de Direito Constitucional**, n. 9, p. 361-388, jan./jun. 2007.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (coords.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2020. p. 21-59.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. Rio de Janeiro: Lumen Juris, 2004.

SCHERMER, Bart Willem; CUSTERS, Bart; HOF, Simone, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. **Ethics and Information Technology**, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418#references-widget. Acesso em: 13 jun. 2024.

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

SENSITY. **The State of Deepfakes 2024**. 2024. Disponível em: https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SODF%202024.pdf. Acesso em: 20 jan. 2025.

SILVA, Marcelo Mauricio; FREIRE, Rasland Costa de Luna; FONTES, Raíssa Garcia da Costa. Liberdade de expressão x direito à honra: as expressões populares como meio de transmissão de discriminação social. **Revista Eletrônica do Curso de Direito da UFSM**, v. 18 n, 2, p. 1-37, 2023.

SILVA, Guilherme César dos Santos; NEVES, Fabiana Junqueira Tamaoki; GOTTEMS, Claudinei. O direito de imagem introduzido nos direitos da personalidade. **Revista Jurídica Cesumar – Mestrado**, v. 23, n. 1, p. 87-99, 2023.

SIQUEIRA, Dirceu Pereira; VIEIRA, Ana Elisa Fernandes. Os limites à reconstrução digital da imagem na sociedade tecnológica. **Revista Eletrônica do Curso de Direito da UFSM**, v. 17, n. 3, p. 1-36, 2022.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo: Revista dos Tribunais, 2002.

TARTUCE, Flávio. **Direito civil**: Lei de Introdução e parte geral. 18. ed. Rio de Janeiro: Forense, 2022.

TEPEDINO, Gustavo. **Temas de direito civil**. 3. ed. Rio de Janeiro: Renovar, 2004.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Política de cookies e a "crise do consentimento": Lei Geral de Proteção de Dados e a autodeterminação informativa. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 47, p. 241-262, 2021.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Tecnologias vestíveis e capitalismo de vigilância: do compartilhamento de dados sobre saúde e a proteção dos direitos da personalidade. **Revista de Direito, Governança e Novas Tecnologias**, v. 7, n. 1, p. 126- 147, 2021.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Biohacking e ciborguismo: o melhoramento humano à luz dos direitos da personalidade. **Opinião Jurídica**, v. 20, n. 35, p. 110-138, 2022.

TSE proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições: entre as novidades da propaganda eleitoral deste ano, estão a proibição de "*deepfakes*" e o aviso obrigatório de uso da IA em conteúdo divulgado. **Tribunal Superior Eleitoral (TSE)**, 28 fev. 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes. Acesso em: 4 jun. 2024.

UNIÃO EUROPEIA (UE). **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024** que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n. 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Acesso em: 5 jan. 2025.

ZANINI, Leonardo Estevam de Assis. **Direito à imagem**. Curitiba: Juruá, 2018.

ZANINI, Leonardo Estevam de Assis; OLIVEIRA, Edmundo Alves de; SIQUEIRA, Dirceu Pereira; FRANCO JUNIOR, Raul de Mello. Os direitos da personalidade em face da dicotomia direito público – direito privado. **Revista de Direito Brasileira**, São Paulo, v. 19, n. 8, p. 208- 220, jan./abr. 2018.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. São Paulo: Intrínseca, 2019.