UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS - CCJE
FACULDADE NACIONAL DE DIREITO - FND

MANIPULAÇÃO DO MEIO DIGITAL PELO USO DO *DEEPFAKE*: IMPACTOS NOS DIREITOS DA PERSONALIDADE, REGULAMENTAÇÃO E A REPARAÇÃO DE DANOS NO ÂMBITO DA RESPONSABILIDADE CIVIL

ROGER MAGNO DO NASCIMENTO NOVELLO

Rio de Janeiro
2023

ROGER MAGNO DO NASCIMENTO NOVELLO

MANIPULAÇÃO DO MEIO DIGITAL PELO USO DO *DEEPFAKE*: IMPACTOS NOS DIREITOS DA PERSONALIDADE, REGULAMENTAÇÃO E A REPARAÇÃO DE DANOS NO ÂMBITO DA RESPONSABILIDADE CIVIL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, apresentada como requisito para obtenção do grau de bacharel em Direito, sob a orientação da **Professora Dra. Daniela Silva Fontoura de Barcellos**.

Rio de Janeiro
2023

CIP - Catalogação na Publicação

N939m

NOVELLO, ROGER MAGNO DO NASCIMENTO
MANIPULAÇÃO DO MEIO DIGITAL PELO USO DO DEEPFAKE: IMPACTOS NOS DIREITOS DA PERSONALIDADE, REGULAMENTAÇÃO E A REPARAÇÃO DE DANOS NO ÂMBITO DA RESPONSABILIDADE CIVIL / ROGER MAGNO DO NASCIMENTO NOVELLO. -- Rio de Janeiro, 2023.
66 f.

Orientadora: DANIELA SILVA FONTOURA DE BARCELLOS.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2023.

1. Deepfake. 2. Direitos da personalidade. 3. Responsabilidade civil. 4. Proteção post-mortem. 5. Direito à imagem. I. BARCELLOS, DANIELA SILVA FONTOURA DE, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

ROGER MAGNO DO NASCIMENTO NOVELLO

MANIPULAÇÃO DO MEIO DIGITAL PELO USO DO *DEEPFAKE*: IMPACTOS NOS DIREITOS DA PERSONALIDADE, REGULAMENTAÇÃO E A REPARAÇÃO DE DANOS NO ÂMBITO DA RESPONSABILIDADE CIVIL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, apresentada como requisito para obtenção do grau de bacharel em Direito, sob a orientação da **Professora Dra. Daniela Silva Fontoura de Barcellos**.

Data da Aprovação: 27/11/2023.

Banca Examinadora:

_____

Prof.ª Dra. Daniela Silva Fontoura de Barcellos (Orientadora)

_____

Prof.ª Ma. Any Carolina Garcia Guedes

_____

Prof. Me. Pedro Teixeira Pinos Greco

Rio de Janeiro
2023

AGRADECIMENTOS

Aos meus pais, quero dedicar meu mais sincero agradecimento por todo o apoio incondicional, sacrifício e encorajamento que vocês sempre me proporcionaram. Graças a vocês, construí meu caráter e a confiança necessária para enfrentar os desafios da vida, por mais difíceis que pareçam. Obrigado por acreditarem em mim, por me impulsionarem a ser sempre melhor. Este é o resultado de uma jornada conjunta.

À minha avó, pela presença carinhosa e reconfortante desde quando eu me entendo por gente. Sua paciência infinita e sorriso acolhedor sempre foram um refúgio seguro para mim, independentemente das circunstâncias. Suas histórias cheias de experiências e lições de vida moldaram meu entendimento do mundo e influenciaram quem me tornei. Afinal, quem é avó é mãe duas vezes.

À Débora, agradeço por compartilhar essa jornada comigo, por ser minha parceira e por tornar cada dia mais especial. Em cada desafio, você foi meu pilar de apoio, oferecendo orientação e força. Seu amor incondicional é uma bússola que me guia e que carrego comigo a cada passada. Este sucesso é também seu, pois, juntos, superamos os obstáculos. Agora, nos resta celebrar as conquistas e construir as memórias.

À minha orientadora, Professora Daniela Barcellos, pelas valiosas contribuições intelectuais e pela sua paciência ao longo de todo o trabalho. Certamente, suas orientações e sugestões construtivas foram aproveitadas ao máximo. Agradeço, inclusive, por ter acreditado em meu potencial, por desafiar-me a atingir novos patamares e por ser uma presença inspiradora em minha jornada acadêmica.

Aos amigos que a universidade colocou no caminho e que estiveram comigo na minha jornada profissional, por cada gesto de reciprocidade, cada palavra de incentivo e cada momento compartilhado que nos tenham levado a alcançar nossas conquistas. Sempre manterei o lado altruísta com aqueles que sei que fariam o mesmo por mim.

Por último, mas não menos importante, à Faculdade Nacional de Direito pela excelência acadêmica proporcionada por professores dedicados e qualificados, que não apenas transmitiram conhecimento, mas também inspiraram o pensamento crítico e criativo. Cada aula

foi uma oportunidade para aprender, crescer, expandir minha mundividência e entender que as certezas da vida não são tão concretas assim. A bem da verdade, a única certeza concreta é que eu tenho muito orgulho de ter feito parte dessa instituição.

RESUMO

O presente trabalho monográfico objetiva analisar a manipulação do meio digital pelo uso do *deepfake*, assim como suas repercussões e impactos na esfera jurídica. Busca-se, desse modo, diferenciar as nuances entre o uso consentido e o não consentido do *deepfake*, sendo este último observado sob a perspectiva de violação aos direitos da personalidade, por meio do estudo de casos. Com efeito, será compreendido em que medida o ordenamento jurídico brasileiro está preparado para enfrentar a problemática, seja por meio da aplicação do instituto da responsabilidade civil, seja pela elaboração de Projeto de Lei que vise à regulamentação do tema. Com respaldo na revisão bibliográfica, serão abordados os desdobramentos atuais que gravitam a dinâmica da disseminação do *deepfake* no meio digital, isto é, as implicações no âmbito *post-mortem*, a responsabilidade dos usuários pelo compartilhamento da mídia manipulada, a responsabilidade dos provedores de aplicação pela disponibilização do conteúdo de *deepfake*, bem como as limitações concretas para a reparação dos danos no cenário prático.

Palavras-chave: Deepfake; Deepfake news; Inteligência Artificial; Direitos da personalidade; Direito à imagem; Proteção post-mortem; Responsabilidade civil; Responsabilidade pelo compartilhamento; Responsabilidade dos provedores de aplicação; Reparação de danos.

ABSTRACT

The present monographic work aims to analyze the manipulation of the digital environment through the use of deepfake, as well as its repercussions and impacts on the legal sphere. In this way, the goal is to differentiate between the consensual and non-consensual use of deepfake, with the latter being observed from the perspective of violating personality rights through case studies. Consequently, it will be understood to what extent the Brazilian legal system is prepared to address the issue, either through the application of the institute of civil liability or through the development of a Bill aiming to regulate the subject. Supported by the literature review, the current developments surrounding the dynamics of deepfake dissemination in the digital realm will be addressed, including implications in the post-mortem context, user responsibility for sharing manipulated media, provider responsibility for making deepfake content available, as well as the practical limitations for damage reparation.

Keywords: Deepfake; Deepfake news; Artificial Intelligence; Personality rights; Right to image; Post-mortem protection; Civil liability; Sharing responsibility; Provider liability; Damage reparation.

SUMÁRIO

INTRODUÇÃO

A sociedade contemporânea observa, mais do que nunca, uma crescente e acelerada transformação promovida pelo avanço tecnológico. Em um intervalo de tempo surpreendentemente curto, esse progresso vertiginoso conduziu a um cenário de reconfiguração das dinâmicas sociais, econômicas e culturais. Notadamente, a convergência de inteligência artificial, aprendizado de máquina e processamento de dados em larga escala desencadeou uma verdadeira revolução digital que propicia o surgimento de novos paradigmas e, consequentemente, impõe ao ordenamento jurídico a imperiosa necessidade de adaptação.

Diante desse panorama, surge o fenômeno do *deepfake*, que se caracteriza como uma possibilidade de recriação digital do rosto e/ou da voz de pessoas reais – integral ou parcialmente –, visando à alteração da realidade e à criação de novas percepções. Essa técnica, que utiliza algoritmos avançados de aprendizado profundo, permite a produção de conteúdos audiovisuais extremamente convincentes que desafiam a distinção entre o autêntico e o fabricado.

Dessa forma, abriu-se um leque de possibilidades para que a ferramenta fosse utilizada como uma solução para certos contratempos, a exemplo do seu uso na indústria do entretenimento para rejuvenescer um velho ator[1], para ressuscitar grandes figuras da história em museus[2], para dar vida a pinturas icônicas[3], ou, ainda, para trazer uma imersão aos profissionais da saúde em treinamentos de cenários médicos complexos.

Nessa toada, observa-se que a ferramenta pode ser utilizada para os mais diversos fins, incluindo o uso consentido da imagem da pessoa a ser recriada digitalmente. A título de exemplo, tem-se a hipótese de um ator ou atriz permitir, mediante firmação de contrato, que sua imagem seja utilizada pela indústria cinematográfica que, por meio do uso de *deepfake*,

[1] O filme "O Irlandês", lançado no Brasil em 14 de novembro de 2019, contou com a utilização de tecnologia precursora para rejuvenescer seu ator principal, Robert De Niro – que, à época, tinha 76 (anos) – para uma cena em que seu personagem aparece com 20 anos. (HESSEL, 2016). Com o crescente destaque do *deepfake*, as produções cinematográficas estão passando a incorporá-lo em seus trabalhos, como é o caso do seu uso para rejuvenescer o ator Tom Hanks, no filme "*Here*", que ainda estreará nos cinemas. (VOLK, 2023).

[2] Em uma exibição ocorrida no museu do pintor surrealista Salvador Dalí, localizado na cidade de São Petersburgo, Flórida, Estados Unidos, utilizou-se do *deepfake* para criar uma versão digital interativa do pintor, tal como se ele mesmo estivesse apresentando o seu museu. (LEE, 2019).

[3] Em 2019, circulou na internet o vídeo *deepfake* em que o clássico quadro da Monalisa falava e fazia diversas expressões faciais. (TORRES; BARROS, 2019).

disponha sobre seus elementos de imagem e voz para desenvolver uma produção cinematográfica.

Não obstante haver a possibilidade de um uso consentido da imagem, é notório que, no contexto atual, já se observa que a ferramenta vem sendo utilizada, muitas vezes, sem obter o consentimento dos sujeitos titulares da imagem, com finalidades reprováveis, como para a manipulação de discursos – em especial de políticos e de pessoas famosas –, promoção da desinformação em larga escala com as *deepfake news* e a criação de conteúdo pornográfico a partir da imagem da vítima. Tais usos acarretam diversas consequências sociais e jurídicas, sobretudo a violação aos direitos da personalidade, colocando-se em xeque os aspectos relacionados à imagem, privacidade, honra e identidade das pessoas alvo dessa manipulação.

Nesse sentido, faz-se mister conhecer os riscos desse recurso à luz do Estado constitucional democrático de direitos, uma vez que a liberdade de criação relacionada ao *deepfake* consubstancia questionamentos quanto aos limites éticos de sua utilização, bem como quanto à violação dos direitos personalíssimos.

Afinal, trata-se de uma manipulação do meio digital, que, em um contexto global pautado pela pós-verdade, torna sua prática cada vez mais recorrente e persuasiva. Sobre esse aspecto, discorre a doutrina:

> O mundo virtual permite a potencialização das violações que atingem o bom nome, a imagem, a privacidade, a identidade social das pessoas, a exposição de dados pessoais sensíveis (...), em razão da sua assombrosa capacidade de difusão, em escala assustadoramente gigantesca. Assim, não só o meio digital permite a violação de alguns direitos fundamentais da pessoa, como também propicia uma replicação inimaginável dos danos. (COLOMBO; FACCHINI NETO, 2019, p. 10).

Desse modo, a capacidade de gerar representações hiper-realistas de indivíduos levanta questionamentos cruciais a respeito da autenticidade, da veracidade e da confiabilidade das informações em um cenário onde a manipulação digital tem se tornado cada vez mais sofisticada.

Ressalta-se, oportunamente, o grande potencial de aprofundamento desse tema, observado, por exemplo, na possibilidade de o dano proveniente da manipulação do meio digital

não incidir na pessoa retratada, mas, sim, na família daquele indivíduo, como é o caso do uso de *deepfake* para reproduzir o rosto e a voz de uma pessoa falecida, de maneira não autorizada.

Nesse contexto, deve ser observada com atenção a repercussão do ato ou discurso que foi vinculado à imagem do terceiro, tendo em vista que a manipulação do meio digital possui diversas finalidades, inclusive de propagar um posicionamento político-ideológico – a depender de quem se está retratando – como forma de controle do pensamento. Qual seja a hipótese, há que se falar no dever de responsabilização civil daqueles que praticaram essa conduta.

Em que pese o evidente dever de reparação pelos danos experimentados, atualmente, há uma escassez de legislação específica que regulamente essa matéria no ordenamento jurídico brasileiro, cabendo uma análise profunda dos entendimentos acadêmicos constantes em artigos e doutrinas, para compreender como ocorre a aplicação da responsabilidade civil nos casos de violação aos direitos da personalidade pela utilização de *deepfakes*.

Diante desse cenário, a presente pesquisa buscará investigar o fenômeno do *deepfake*, seus impactos na manipulação da realidade no meio digital e nos direitos da personalidade, bem como compreender a regulamentação e a incidência da responsabilidade civil como caminhos jurídicos para enfrentamento do problema. Nesse sentido, será adotado o método téorico-dogmático, mediante o emprego da técnica de revisão bibliográfica, a fim de compreender como a doutrina em sentido amplo vem percebendo, sob a ótica jurídica, o tema e suas diversas facetas.

Desse modo, o primeiro capítulo objetiva analisar os impactos do *deepfake* nos direitos personalíssimos. Para tanto, serão abordados, precipuamente, os aspectos gerais do fenômeno, com a definição, surgimento e contextualização sobre o seu funcionamento e facilidade de acesso. Em seguida, será analisada a questão do consentimento no uso do *deepfake*, mediante o uso consentido e o uso não consentido. Após, serão investigadas as violações aos direitos da personalidade, em especial aos direitos à imagem, à privacidade, à honra e à identidade. Por fim, analisar-se-á as implicações do instituto no âmbito *post-mortem*, seguido do estudo de casos reais e multifacetados por meio do uso de *deepfake*.

No segundo capítulo serão analisadas a regulamentação do *deepfake* e a incidência de responsabilidade civil em casos de violação a direitos da personalidade, buscando compreender

os mecanismos jurídicos apontados pela doutrina para enfrentamento dos desafios decorrentes do uso abusivo do deepfake. Nessa toada, será estudada, primeiramente, a regulamentação do uso do *deepfake*, por meio da análise do Projeto de Lei n.º 3.592 de 2023 e das técnicas para sua detecção. Posteriormente, será investigada a incidência do instituto da responsabilidade civil nos casos de uso não consentido do *deepfake*, incluindo a análise da responsabilidade pelo compartilhamento de *deepfake* e a responsabilidade dos provedores de aplicação pela remoção do conteúdo de terceiros. Por fim, será feita uma análise acerca da reparação pelos danos decorrentes de *deepfake*, abordando-se as limitações da reparação no contexto fático, bem como a liquidação do dano.

CAPÍTULO 1 – *DEEPFAKE* E SEUS IMPACTOS NOS DIREITOS DA PERSONALIDADE

1.1 ASPECTOS GERAIS DO *DEEPFAKE*

1.1.1 Definição de *deepfake*

O termo *deepfake* é uma combinação das palavras *deep learning* (aprendizado profundo) e *fake* (falso). Refere-se a uma técnica de manipulação da mídia que se utiliza de algoritmos de Inteligência Artificial, especialmente Redes Neurais Artificiais, que identificam e aprendem padrões de traços humanos em um compilado de imagens e áudios sobre determinada pessoa, para criar conteúdos audiovisuais realistas daquela "pessoa-alvo". Com esse método, tornou-se viável reproduzir, de maneira convincente, o rosto e/ou a voz de uma pessoa, tal como se ela própria tivesse originalmente gravado aquela mídia.

Nas palavras de Anderson Schreiber, Felipe Ribas e Rafael Mansur (2020, p. 611), o *deepfake* é

> […] uma técnica de síntese de imagens ou sons por meio de IA. Seu emprego possibilita a substituição de uma pessoa por outra, a modificação do conteúdo da fala, entre inúmeras outras alternativas de edição. Embora usualmente associada à produção de vídeos, nada impede sua aplicação em arquivos de imagens ou áudios, apenas. Na prática, o termo é usado também para identificar o próprio vídeo, áudio ou imagem fruto da manipulação. (SCHREIBER; RIBAS; MANSUR, 2020, p. 611).

Ressalta-se que o *deepfake* pode ser criado com diferentes níveis de sofisticação, desde resultados menos convincentes até os conteúdos extremamente realistas e difíceis de detectar visualmente.

Para que o *deepfake* seja crível, é necessário que a Inteligência Artificial se utilize de uma grande quantidade de informações disponíveis nos bancos de dados, para criar a mídia manipulada. Todavia, excepcionalmente, a finalidade que se pretende alcançar pode ser justamente a de criar um conteúdo não compatível com a realidade, a exemplo do tom cômico dado ao comercial sedutor do perfume feminino *J'adore*, que substituiu a face da atriz principal

pelo rosto do ator britânico Rowan Atkinson, conhecido pela interpretação do personagem *Mr. Bean*. (BESCHIZZA, 2019).

1.1.2 Origem

A origem do termo *deepfake* remonta ao ano de 2017, quando um usuário da rede social *Reddit* apelidado como "*deepfakes*" compartilhou vídeos pornográficos falsos envolvendo celebridades. Esses vídeos foram criados usando uma técnica de aprendizado de máquina chamada Redes Generativas Adversariais (GANs, do inglês Generative Adversarial Networks), que permite a criação de conteúdo falso altamente convincente.

No entanto, as técnicas subjacentes ao *deepfake* não surgiram com os vídeos pornográficos falsos de 2017. O uso de técnicas de aprendizado de máquina para criar imagens e vídeos falsos existe há algum tempo.

Antes do termo *deepfake* ser cunhado, já havia exemplos de manipulação de mídia utilizando técnicas similares, mas essas técnicas não eram tão acessíveis e difundidas como são hoje em dia. O termo *deepfake* se popularizou e se tornou sinônimo desse tipo de manipulação de mídia em larga escala, especialmente com a disseminação de vídeos falsos envolvendo figuras públicas e políticos.

Desde então, o desenvolvimento de *deepfakes* tem sido objeto de preocupação, levantando questões éticas, legais e de segurança, e gerando debates sobre como combater a desinformação e proteger a integridade da mídia e da sociedade.

1.1.3 Funcionamento da ferramenta

O processo de criação de um *deepfake* geralmente envolve o treinamento de um modelo de Rede Neural com um grande conjunto de dados de entrada, isto é, um massivo banco de dados, como vídeos, imagens e áudios de uma pessoa-alvo.

Com base nesses dados, o modelo é capaz de aprender os padrões dos traços e detalhes humanos daquela pessoa, sejam as características faciais, expressões ou nuances específicas –

como, por exemplo, o jeito em que a luz se adapta ao rosto da pessoa-alvo, ou como ocorre a mudança no tom de voz daquela pessoa conforme as palavras que são ditas.

A partir dessas informações, o modelo de Rede Neural passa a atuar sob duas frentes: um gerador e um discriminador. O gerador é responsável por criar diferentes versões do conteúdo falso, enquanto o discriminador será responsável por tentar distinguir a mídia real da mídia falsa, com base nos padrões analisados, cabendo ao discriminador apontar aquilo que não se equiparar com a mídia original.

Assim, a constante competição entre o gerador e o discriminador é o que impulsiona o aprimoramento do gerador ao longo do tempo, que criará conteúdos cada vez mais convincentes e indistinguíveis dos exemplos reais.

1.1.4 Facilidade de acesso

À contramão de toda a complexa teoria envolvida na produção de um conteúdo *deepfake*, na prática, cada vez se torna mais fácil ter acesso a programas e aplicativos que criam essa mídia artificial. É o caso do aplicativo chinês "*Zao*", que, com a utilização de apenas uma imagem do rosto de uma pessoa, consegue replicá-lo em corpos de atores durante cenas de determinados filmes. (LOUBAK, 2019).

Desde já, cumpre destacar que essa facilidade de acesso à produção de *deepfake*, custou um certo preço, tendo em vista que a política de privacidade da Zao permitia que as imagens dos rostos enviadas pelos usuários pudessem ser fornecidas a terceiros. (DOFFMAN, 2019).

Cria-se, portanto, um panorama em que o *deepfake* tem se tornado mais acessível devido ao avanço das tecnologias e ao surgimento de ferramentas e algoritmos disponíveis publicamente.

Ainda que a criação de *deepfakes* de qualidade requeira expertise técnica e conhecimento em aprendizado de máquina, não se parece distante o momento em que tais requisitos deixarão de ser imprescindíveis, motivo pelo qual se tem levantado preocupações acerca da disseminação de conteúdo falso pelo uso indevido dessa tecnologia.

1.2 CONSIDERAÇÕES ACERCA DAS POSSIBILIDADES DE USO DO DEEPFAKE

Não se pode negar que o *deepfake* abriu novos horizontes – antes inimagináveis – como uma fonte inesgotável de possibilidades de uso e, sem dúvidas, como um meio livre de expressão artística. Por outro lado, a liberdade em excesso, no contexto do *deepfake*, pode implicar na ausência de limites, e, por consequência, na violação de direitos personalíssimos, na indevida propagação de notícias falsas e, até mesmo, no cometimento de fraudes, razão pela qual há que se falar num uso cauteloso do *deepfake*.

1.3 A QUESTÃO DO CONSENTIMENTO

Tratando-se de *deepfake*, há que se falar na questão do consentimento, eis que a tecnologia funciona com base na análise de imagens reais da pessoa-alvo para fabricar aquela artificial. A obtenção dessas imagens geralmente requer acesso a fotografias ou vídeos da pessoa, que podem ter sido obtidos de forma legítima, mas sem a intenção de serem usados para criar conteúdo falso. Portanto, utilizar essas imagens sem o consentimento explícito da pessoa em questão, traz preocupações éticas e legais. O consentimento informado é essencial para garantir que a privacidade e a autonomia da pessoa sejam respeitadas e que ela tenha controle sobre o uso de sua própria imagem.

Há quem fale de uma noção de consentimento tácito, compreendido pela situação em que uma pessoa, por meio de suas ações ou circunstâncias, permite ou concorda implicitamente com o uso de sua imagem por terceiros, sem a necessidade de um consentimento explícito. Objeta-se, contudo, que nessas situações não haveria consentimento tácito propriamente dito, mas, sim, uma série de limites impostos ao direito à imagem da pessoa pelo interesse público, o que tornaria desnecessária a autorização do titular. Tais limites se diferenciariam da autorização tácita, pois se se estivesse “tratando de autorização, ainda que implícita, haveria o poder de oposição do titular à publicação”. (LOUREIRO, 2005, p. 80).

A questão do consentimento também esbarra na produção *deepfake post-mortem*, isto é, após a morte de uma pessoa – conforme será mais aprofundado em tópico próprio. Nesses casos, a obtenção de imagens ou gravações da pessoa falecida é ainda mais delicada, uma vez que ela não pode mais expressar sua vontade ou consentir com o uso de sua imagem ou voz.

A criação de *deepfakes* pós-morte levanta questionamentos sobre a preservação da dignidade da pessoa mesmo após seu falecimento, bem como o impacto que isso pode ter em seus entes queridos. É essencial considerar a autorização de seus familiares, o respeito à memória e aos direitos da pessoa falecida, bem como a privacidade e o bem-estar emocional de sua família.

Acerca do consentimento vinculado ao Direito à Imagem, explica Filipe José Medon Affonso (2021, p. 256) que:

> O consentimento parece ser, assim, um assunto não resolvido completamente na doutrina. Todavia, é certo que por mais frequentes que sejam tais situações de exposição em público, 'em uma sociedade caracterizada pela presença constante da mídia e pelo anseio de exposição pública, a necessidade de consentimento inequívoco do retratado deve continuar a ser vista como regra, nunca como exceção'. Desse modo, a busca constante deve ser pela obtenção do consentimento inequívoco do titular da imagem violada, dado o potencial lesivo que sua divulgação pode ter, sobretudo com a mola propulsora da internet, que, em poucos minutos, consegue tornar mundialmente conhecida uma imagem obtida com o recurso da câmera de um smartphone. (AFFONSO, 2021, p. 256).

1.3.1 O uso consentido

Em que pesem as preocupações éticas e os riscos associados ao uso não consentido do *deepfake*, é importante reconhecer que o uso consentido e responsável dessa tecnologia pode trazer benefícios em diversos setores. Para a indústria do entretenimento, certamente, o *deepfake* veio a calhar. Tornou-se cada vez mais fácil solucionar problemas envolvendo a participação de atores nos filmes. Desse modo, com o uso do *deepfake* nas produções, passou a ser possível rejuvenescer atores, fazer com que um ator com distúrbio que afeta habilidades cognitivas voltasse a atuar[4], ou, até mesmo, ressuscitar um ator digitalmente, possibilitando a continuidade de uma grande franquia cinematográfica[5].

Além dos atores, também é possível "ressuscitar" personagens históricos digitalmente, como o caso do vídeo interativo de Salvador Dalí, que apresenta o seu museu aos visitantes.

[4] O ator Bruce Willis, que sofre do distúrbio de afasia – a qual compromete a linguagem falada e, por consequência, suas interpretações nos filmes –, pode voltar a atuar com a ajuda do *deepfake*, uma vez que as cenas que envolvem suas falas seriam geradas digitalmente. (ALECRIM, 2022).

[5] No filme *Star Wars: Rogue One* (2016), o ator James Dean, que interpretava um personagem fundamental para a franquia, foi ressuscitado digitalmente, por meio do *deepfake*, para que fosse possível contar a história originária da saga. (PLACIDO, 2019).

(LEE, 2019). Ainda que se afirme que a ressurreição digital de pessoas falecidas pode ser uma forma de honrar sua memória e preservar suas contribuições culturais e históricas – sobretudo, mantendo-se vivo o seu legado às gerações futuras –, é preciso pontuar que o uso do *deepfake* para esses fins, pode levantar questões sobre consentimento e privacidade.

É difícil determinar se uma pessoa falecida teria concordado com a recriação digital de sua imagem e voz, e se isso seria considerado um uso adequado de sua identidade. Além disso, a possibilidade de usar *deepfake* para manipular a história ou criar discursos e declarações falsas em nome de pessoas falecidas é um risco real, tendo como consequência a distorção da verdade, o aumento da desinformação e o abalo de confiança nos registros históricos. Nesse sentido, afigura-se justo e plausível que a família do falecido seja responsável por autorizar, ou não, o uso do *deepfake* de seu familiar.

Na seara da educação, o uso consentido *deepfake* tem o potencial de impactar positivamente, oferecendo novas oportunidades e abordagens de ensino. Desse modo, destaca-se a importância do *deepfake* na criação de simulações realistas que permitem aos alunos vivenciar situações práticas e desafiadoras, a exemplo dos estudantes de medicina, que podem se beneficiar de simulações de cirurgias ou diagnósticos médicos, enquanto estudantes de engenharia podem experimentar simulações de projetos complexos[6].

Não obstante, o *deepfake* pode ser utilizado para produzir materiais educacionais personalizados e interativos, de modo que professores e alunos possam criar vídeos e apresentações em que personalidades virtuais – baseadas em pessoas que consentiram com o uso da sua imagem – explicam conceitos complexos ou realizam demonstrações práticas.

Em paralelo, ao aprender sobre o potencial e os riscos do *deepfake*, os alunos desenvolvem habilidades críticas de mídia e literacia digital. Portanto, há uma formação de um senso crítico para se identificar e analisar *deepfakes*, para que, ao fim e ao cabo, compreenda-se como a tecnologia pode ser usada para manipular o meio digital e enganar as pessoas.

[6] Nesses casos, o *deepfake* não é necessariamente aplicado para replicar rostos ou vozes específicas de pessoas reais em simulações educacionais interativas. Em vez disso, a ênfase está na criação de experiências práticas e envolventes para os alunos, onde a tecnologia de simulação, juntamente com outros recursos digitais, pode ser utilizada para simular situações do mundo real.

Na indústria da moda, diversas companhias estão utilizando o *deepfake* para impulsionar suas vendas no meio virtual. A criação de provadores virtuais permitiu aos consumidores a possibilidade de "experimentar" roupas e acessórios sem precisar estar fisicamente em uma loja. Com base no reconhecimento de características corporais do consumidor, como altura, forma do corpo e proporções, o *software* aplica algoritmos de aprendizado de máquina para mapear a peça de roupa ou acessório sobre a imagem do usuário, criando uma representação visual realista de como a peça ficaria nele.

1.3.2 O uso não consentido

Embora haja pontos positivos concernentes ao *deepfake*, a sua má fama, decorrente do uso não consentido, contribui para que ele não seja bem-quisto socialmente – pelo menos até o momento. Como já mencionado, desde sua origem, o *deepfake* esteve envolvido em fortes polêmicas, sobretudo, em relação ao seu uso para a criação de conteúdo pornográfico. A manipulação da imagem, nessa prática específica, é altamente invasiva e viola a privacidade das pessoas, já que seus rostos são colocados em contextos sexuais sem o seu consentimento.

Nesse sentido, o *deepfake* pornográfico também contribui para a objetificação e a exploração sexual, perpetuando a cultura do *revenge porn* e do *cyberbullying*. Como consequência, as vítimas desse tipo de conteúdo muitas vezes enfrentam constrangimento, estigmatização e trauma psicológico, sendo alvo de assédio e discriminação.

Talvez a prática mais recorrente do uso não consentido e prejudicial do *deepfake*, seja o chamado "*deepfake news*", que se refere à disseminação de informações falsas e enganosas por meio do uso de *deepfakes*. As *deepfake news* têm o potencial de se tornarem uma arma poderosa na disseminação de desinformação, e geralmente estão atreladas às figuras de autoridades. Esses vídeos falsos podem ser usados para difamar, desacreditar ou influenciar a opinião pública de maneira maliciosa.

Uma das principais preocupações com as *deepfake news* é o seu impacto na esfera política. Os *deepfakes* podem ser usados para criar vídeos falsos de políticos, distorcendo suas declarações e ações, levando a uma erosão da confiança no sistema político e prejudicando a integridade das eleições. Por outro lado, as *deepfake news* podem ser usadas para propagar

teorias da conspiração, manipular narrativas e polarizar ainda mais a sociedade – basta criar um conteúdo que atinja determinado nicho.

Outra área afetada pelas *deepfake news* é o jornalismo. Com a facilidade de criar vídeos falsos convincentes, é cada vez mais difícil distinguir entre conteúdo autêntico e *deepfakes*. Isso coloca em risco a credibilidade da mídia tradicional, prejudica a confiança nas fontes de informação e dificulta a tarefa dos jornalistas em fornecer informações precisas e verificadas. Em paralelo, há a possibilidade de se levar a sociedade ao pânico, ao medo e à desinformação generalizada quando informações falsas são propagadas através de *deepfakes*, causando danos significativos à confiança pública e à democracia.

Nem mesmo o mundo jurídico está blindado. Isso porque, o uso de *deepfakes* para forjar provas é uma das aplicações mais preocupantes e eticamente questionáveis dessa tecnologia. Ao criar vídeos ou áudios falsos com a aparência de autenticidade, o *deepfake* pode ser utilizado para manipular evidências e distorcer a verdade em investigações criminais, litígios judiciais ou questões políticas. A capacidade de gerar conteúdo altamente realista pode tornar extremamente difícil para as partes envolvidas e para os especialistas em forense digital distinguirem provas genuínas dos *deepfakes*.

É importante ressaltar que o uso de *deepfakes* para forjar provas viola os princípios fundamentais do devido processo legal e do direito à um julgamento justo, além de pôr em risco a integridade do sistema judiciário, com o proferimento de decisões injustas ou baseadas em informações falsas. Numa perspectiva mais profunda relacionada ao realismo do *deepfake*, é pertinente conjecturar a hipótese de uma pessoa que foi filmada cometendo ato ilícito, alegar, em sua defesa, que o vídeo em questão se trata de *deepfake* – amparando-se na dificuldade em se constatar a veracidade da mídia.

Outrossim, constata-se a possibilidade de uso não consentido do *deepfake* para a obtenção de vantagens fraudulentas. Nesse sentido, a fraude se aproveitará da tecnologia para se passar por alguém próximo ou de confiança da vítima. As chamadas fraudes de identidade, utilizam o *deepfake* para criar vídeos ou áudios falsos de pessoas reais, permitindo que os fraudadores se passem por elas.

Isso pode ser utilizado em tentativas de *phishing*, onde os fraudadores se apresentam como pessoas de confiança para obter informações pessoais, senhas ou acesso a contas. Já as chamadas fraudes financeiras, se utilizam do *deepfake* para criar vídeos falsos de executivos de sociedades-empresárias ou líderes financeiros, enganando investidores, acionistas ou funcionários para tomar decisões financeiras prejudiciais.

Mais especificamente, no mercado de capitais, as possibilidades de fraude com o uso de *deepfake* não consentido parecem ser mais rebuscadas. Isso porque, a título ilustrativo, é possível produzir um conteúdo *deepfake* de um alto executivo de certa companhia, no qual ele admite publicamente que declarará falência da sociedade-empresária.

O movimento natural do mercado seria vender as ações daquela companhia, despencando o seu preço em pouco tempo. A fraude estaria na compra das ações a um preço irrisório, considerando que os preços retornariam ao seu patamar original, assim que fosse descoberto que o vídeo do alto executivo era falso.

Entretanto, o *deepfake* não consentido também pode ser usado de forma crítica, proporcionando uma plataforma para a sátira política, paródias e críticas sociais. Através da sátira e do humor, permite-se que os criadores explorem a tecnologia para questionar, criticar e comentar sobre eventos atuais, figuras públicas e instituições.

A questão por trás dessa possibilidade é que a disseminação de *deepfakes* satíricos requer um público consciente e informado, capaz de distinguir entre a sátira e a realidade. Isso enfatiza a importância de promover a alfabetização digital e a literacia de mídia para garantir que as pessoas possam interpretar e contextualizar adequadamente o conteúdo gerado por *deepfake* com cunho crítico, evitando, em última análise, a desinformação.

1.4 IMPACTOS NOS DIREITOS DA PERSONALIDADE

Os direitos da personalidade – ou também conhecidos como direitos personalíssimos – são um conjunto de direitos intrínsecos e inalienáveis que se relacionam à própria pessoa, protegendo aspectos subjetivos essenciais, tal como a imagem, a privacidade, a honra e a identidade de um indivíduo.

Cumpre esclarecer que a personalidade não constitui um direito em si, mas, sim, representa a base que sustenta os direitos e deveres decorrentes dela. É nesse sentido que se entende que os direitos da personalidade nada mais são do que permissões dadas pelo ordenamento jurídico, de modo a se viabilizar que cada pessoa possa tutelar pelo que lhe é próprio, isto é, a vida, a liberdade, o próprio corpo, a identidade, a própria imagem, a honra etc. (TELLES JÚNIOR, 1977).

Por essa lógica, afirma-se que, no momento em que o indivíduo adquire personalidade, consubstanciando-se uma aptidão para deter direitos e assumir deveres, o ser humano ganha a possibilidade de resguardar o que é intrínseco a si, abrangendo sua vida, sua integridade física e mental, seu corpo, sua carga intelectual, sua moral, sua honra pessoal ou pública, sua imagem e sua privacidade. (TARTUCE, 2019).

A origem dos direitos personalíssimos remonta à longínqua época do Direito Romano, em que pese a consolidação do instituto só vir a ocorrer no pós-Segunda Guerra Mundial, período em que se verificou a necessidade de se conter os anseios oriundos daquele contexto geopolítico por meio da elaboração de tratados internacionais que visassem à proteção dos direitos humanos. A despeito da detalhada trajetória de consolidação dos direitos da personalidade, confira-se:

> O reconhecimento dos direitos da personalidade como categoria de direito subjetivo é relativamente recente, porém sua tutela jurídica já existia na Antiguidade, punindo ofensas físicas e morais à pessoa, através da *actio injuriarum*, em Roma, ou da *dike kakegorias*, na Grécia. Com o advento do Cristianismo houve um despertar para o reconhecimento daqueles direitos, tendo por parâmetro a ideia de fraternidade universal. Na era medieval entendeu-se, embora implicitamente, que o homem constituía o fim do direito, pois a Carta Magna (séc. XIII), na Inglaterra, passou a admitir direitos próprios do ser humano. Mas foi a Declaração dos Direitos de 1789 que impulsionou a defesa dos direitos individuais e a valorização da pessoa humana e da liberdade do cidadão. Após a Segunda Guerra Mundial, diante das agressões causadas pelos governos totalitários à dignidade humana, tomou-se consciência da importância dos direitos da personalidade para o mundo jurídico, resguardando-os na Assembleia Geral da ONU de 1948, na Convenção Europeia de 1950 e no Pacto Internacional das Nações Unidas. Apesar disso, no âmbito do direito privado seu avanço tem sido muito lento, embora contemplados constitucionalmente. O Código Civil francês de 1804 os tutelou em rápidas pinceladas, sem defini-los. Não os contemplaram o Código Civil português de 1866 e o italiano de 1865. O Código Civil italiano de 1942 os prevê nos arts. 5º a 10; o atual Código Civil português, nos arts. 70 a 81, e o novo Código Civil brasileiro, nos arts. 11 a 21. Sua disciplina, no Brasil, tem sido dada por leis extravagantes e pela Constituição Federal de

> 1988, que com maior amplitude deles se ocupou, no art. 5º em vários incisos e ao dar-lhes, no inc. XLI, uma tutela genérica ao prescrever que a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais. (DINIZ, 2012, p. 132-133).

Tal como no passado, "as exigências do mundo contemporâneo e a diversidade de orientações nos vários países conclamaram os juristas a dar maior ênfase ao assunto [direitos da personalidade]". (PEREIRA, 2017, p. 202). Dessa vez, se está diante de um cenário em que a utilização das novas tecnologias pode impactar profundamente os direitos personalíssimos, sobretudo, quando se trata de *deepfake*.

É claro que, *a priori*, a criação de novas tecnologias não possui a finalidade exclusiva de ocasionar danos aos direitos da personalidade. Porém, em se tratando de uma tecnologia ainda não regulamentada, que, como o caso do *deepfake*, consegue replicar fidedignamente o rosto e a voz de praticamente qualquer pessoa sem que ela tenha necessariamente consentido, e que possibilita que a imagem desse indivíduo-alvo seja utilizada para adotar comportamentos vexatórios e proferir falas reprováveis; torna-se necessário uma análise aprofundada dos seus impactos nos direitos personalíssimos.

1.4.1 Direito à imagem

O direito à imagem é um dos direitos da personalidade que se baseia no princípio de controle sobre a utilização da representação visual de um indivíduo. Essa representação visual pode incluir fotografias, ilustrações, vídeos ou qualquer outra forma de imagem que represente a pessoa. O cerne desse direito reside na capacidade do indivíduo de autorizar ou vetar o uso de sua imagem, visando proteger sua identidade e privacidade – não por acaso, outros direitos personalíssimos.

Em termos conceituais, esse direito envolve a prerrogativa de impedir a reprodução, exposição ou distribuição da imagem de alguém sem seu consentimento. Isso significa que, em princípio, qualquer uso da imagem de uma pessoa para fins comerciais, publicitários, ou outros que envolvam exposição pública, requer a autorização prévia da pessoa retratada.

A previsão legal do direito à imagem está estabelecida no artigo 20, do Código Civil de 2002, por meio do qual: "(…) a exposição ou a utilização da imagem de uma pessoa poderão

ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais" (BRASIL, 2002).

Sobre a temática, discorre a doutrina que:

> O retrato de uma pessoa não pode ser exposto, ou reproduzido, sem o consentimento dela, salvo se assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de política ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos ou de fatos de interesse público, ou que em público hajam decorrido. Proíbe-se a reprodução, ou exposição, quando o fato atenta contra a honra, a boa fama e a respeitabilidade da pessoa retratada, admitindo-se, que, nesses casos, possa o ofendido requerer a proibição e pleitear indenização do dano que sofreu. Tais, em síntese, as regras relativas ao direito à imagem. (GOMES, 2016, p. 118-119).

No contexto atual, o direito à imagem está enfrentando novos desafios decorrentes da rápida evolução da tecnologia, em especial, a disseminação dos *deepfakes*. Desse modo, é necessário reconhecer que o *deepfake* apresenta um dilema significativo para o direito à imagem, uma vez que permite a manipulação das representações visuais de uma pessoa de maneira altamente convincente e realista, sem a necessidade de consentimento.

Conforme visto, a questão do consentimento é fundamental para se compreender a essência do direito à imagem. Uma pessoa retratada em um *deepfake* frequentemente não deu permissão para que sua imagem fosse usada daquela maneira, o que reclama a tutela envolvida nesse direito personalíssimo. Com efeito, a ausência de permissão para a reprodução da imagem pode implicar em sua proibição pela própria pessoa retratada, caso o fato atinja sua honra, boa fama ou respeitabilidade – medida essa respaldada pela norma jurídica.

Nessa toada, cumpre destacar a ressignificação do próprio conceito de imagem, no contexto hodierno. Aos olhos dos novos entendimentos doutrinários, o conceito jurídico de imagem passou a abarcar a figura da projeção moral face à sociedade. (GUERRA, 2001). Assim, a violação do direito à imagem, que, outrora, estava quase que exclusivamente ligado à questão do consentimento, agora passa a abarcar a possibilidade de vincular qualquer ato ou discurso à imagem de um terceiro, sem que de fato aquilo tenha ocorrido.

A despeito desse ponto, surge um aspecto reflexivo intrigante que envolve a interseção entre o *deepfake* e o direito à imagem. Historicamente, a proteção subjetiva da imagem

concentrou-se em situações concretas, como a salvaguarda de fotografias ou vídeos não autorizados que tipicamente documentavam eventos reais.

No entanto, com a capacidade de criar imagens virtuais de pessoas em cenários fictícios, inclusive difamatórios, que nunca ocorreram na realidade, por meio do *deepfake*, o escopo do direito à imagem se ampliou para abranger a mera representação artificial da pessoa retratada. Nesse contexto, a origem da imagem – se foi capturada de maneira natural ou gerada virtualmente – tornou-se uma distinção não mais relevante.

Em paralelo, tratando-se de *deepfake*, há que se salientar a inefetividade da norma legal do Código Civil de 2002, no que diz respeito à possibilidade de proibição, pela pessoa retratada, da exposição ou utilização da imagem que esteja afetando sua honra, boa fama ou a respeitabilidade. Essa ineficácia decorre da facilidade de acesso às ferramentas de *deepfake*, bem como da rápida disseminação de conteúdo manipulado nas plataformas digitais.

A dinâmica da internet e das redes sociais permite que *deepfakes* se espalhem rapidamente, tornando difícil para a pessoa retratada identificar e controlar a propagação dessas representações fraudulentas de sua imagem. Além disso, o dano causado por *deepfakes* à reputação e à integridade moral das vítimas pode ser imenso e, em muitos casos, irreparável.

Nesse sentido, outra dimensão de extrema relevância a ser considerada é o impacto psicológico que recai sobre as "vítimas" de *deepfakes*. Quando indivíduos se deparam com representações falsas e possivelmente prejudiciais de si mesmos, isso pode acarretar sérias repercussões emocionais e psicológicas. O direito à imagem desempenha um papel crucial na proteção da integridade moral das pessoas, e essa proteção é substancialmente desafiada no contexto da proliferação desenfreada de *deepfakes*.

Em um mundo onde *deepfakes* podem retratar alguém em situações fictícias, muitas vezes difamatórias, as implicações para a saúde mental e emocional das pessoas retratadas podem ser profundas. A percepção de que alguém pode ser colocado em contextos que comprometem sua reputação, dignidade e até mesmo sua honra sem consentimento, mina a confiança no controle sobre sua própria imagem e identidade. Isso pode levar a sentimentos de vulnerabilidade, ansiedade, perda de privacidade e, em casos extremos, até mesmo danos psicológicos significativos.

A exposição pública a *deepfakes* enganosos pode gerar estigma, ostracismo social e dúvidas sobre a autenticidade das próprias ações. As "vítimas" podem experimentar uma sensação de impotência perante a disseminação de *deepfakes* difamatórios, já que essas representações podem ser utilizadas para comprometer relacionamentos pessoais e profissionais. Além disso, o constante medo de que suas imagens e identidades sejam exploradas de maneira injusta ou difamatória pode criar um ambiente de ansiedade generalizada e estresse.

Em suma, o impacto psicológico de *deepfakes* não deve ser subestimado, e a proteção do direito à imagem é fundamental para preservar a integridade moral das pessoas em uma era marcada pela proliferação de tecnologias enganosas. Isso realça a importância de abordar de maneira holística as implicações éticas e legais associadas ao uso de *deepfakes* – conforme será mais bem aprofundado.

1.4.2 Direito à privacidade

O direito à privacidade é um dos pilares fundamentais dos direitos humanos e do direito civil em muitas jurisdições ao redor do mundo. Ele se baseia na premissa de que os indivíduos têm o direito de manter aspectos de suas vidas pessoais, familiares e íntimas fora do alcance do escrutínio público, do governo e de outras partes. A privacidade é uma parte essencial da dignidade e da autonomia das pessoas, permitindo-lhes controlar informações sobre si mesmas e determinar como essas informações são compartilhadas e utilizadas.

Cumpre destacar que a tutela jurídica do direito à privacidade, para além da sua previsão Constitucional[7], está também estipulada no artigo 21 do Código Civil de 2002, com a seguinte redação: “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).

[7] Confira-se: “Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988).

Sua origem está muito associada ao âmbito familiar e à vida íntima, razão pela qual se compreende que em sua primeira versão, o direito à privacidade, na verdade, estava mais correlacionado a um direito “a ser deixado sozinho”, ou ainda, um direito à intimidade. (SCHREIBER, 2014). Com efeito, esse conceito foi ganhando ressignificações ao longo do tempo, notadamente, pelo avanço das novas tecnologias, para abarcar, hoje em dia, a ideia de proteção aos dados pessoais.

Com o súbito e vultuoso número de dispositivos conectados, redes sociais e coleta de dados em larga escala, a privacidade dos indivíduos se tornou um tema crítico. Isso levou ao desenvolvimento de regulamentações, como o RGPD na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, que estabelecem diretrizes para a coleta, o armazenamento e o uso de dados pessoais.

Em um mundo onde informações pessoais estão cada vez mais expostas e vulneráveis, a proteção do direito à privacidade tornou-se uma preocupação essencial, equilibrando o progresso tecnológico com a necessidade de preservar a dignidade e a autonomia das pessoas. Nesse contexto, a evolução contínua do direito à privacidade reflete a adaptabilidade do sistema legal para enfrentar os desafios da era digital.

No contexto do *deepfake*, a relação com o direito à privacidade se torna evidente. O *deepfake* não apenas desafia a concepção clássica do direito à intimidade, mas também coloca em foco a proteção de dados pessoais, uma vez que envolve a manipulação e a criação de conteúdo digital que pode afetar a reputação e a vida privada das pessoas.

Desse modo, o dano pelo *deepfake* ao direito à privacidade, em seu sentido de vida íntima, é denotado ao se manipular o meio digital para criar vídeos, áudios ou imagens falsas que parecem retratar determinada pessoa em situações comprometedoras ou que representam, de maneira enganosa, sua vida íntima.

Por outro lado, caracteriza-se a violação do *deepfake* ao direito da privacidade em sua concepção de proteção aos dados pessoais, na medida em que o processo de criação do conteúdo digital manipulado depende, necessariamente, do compilamento de imagens e áudios da vítima, que servirão como a base do banco de dados para a Inteligência Artificial produzir a mídia de *deepfake*.

1.4.3 Direito à honra

A despeito do conceito de honra, é necessário indicar que se trata de um valor que abrange a boa reputação, a consideração e o respeito que uma pessoa desfruta na sociedade. O direito à honra, por sua vez, está associado a aspectos como a imagem pública, a reputação, a integridade moral e a consideração social. Assim, proteger a honra de um indivíduo é fundamental para preservar sua dignidade e sua qualidade de vida.

No âmbito jurídico, a doutrina atribui classificação à ideia de honra, compreendendo-se o seu lado ora subjetivo, ora objetivo. Assim, a honra subjetiva é definida pela autoestima, sendo aquilo o que o sujeito pensa de si, enquanto, noutro passo, a honra objetiva abrangeria a ideia da repercussão social, notadamente, pelo que os outros pensam de alguém. (TARTUCE, 2019). É relevante o destaque de que, nessa ótica, a honra objetiva teria uma definição similar à imagem-atributo.

No entanto, existe uma distinção clara entre a ideia de honra objetiva e imagem-atributo, na medida em que:

> A imagem-atributo, com a qual mais se tende a relacionar a honra, não abriga necessariamente aspectos positivos, que podem ser negativos ou mesmo dotados de neutralidade sem que isso altere significativamente a reputação do indivíduo. Nesse sentido, a doutrina traz o exemplo de um pacifista que concede entrevista e, na edição, publicam, equivocadamente, que ele votaria em plebiscito a favor do comércio de armas. Neste caso, haveria uma violação à sua imagem-atributo, mas não à honra, porque ser contra ou a favor do comércio de armas não tem nenhuma relação com a honra do sujeito. Já se um crime é imputado a alguém, além de se cometer calúnia, ofende-se a imagem-atributo se o ofendido tiver uma imagem de sujeito correto. (AFFONSO, 2021, p. 260).

Analisando a violação do direito à honra, no contexto de *deepfake*, verifica-se que uma das formas mais evidentes é por meio da difamação. Quando *deepfakes* são usados para criar vídeos ou imagens que retratam uma pessoa em situações comprometedoras, falsas ou difamatórias, isso pode ter um impacto significativo na reputação da vítima. A disseminação de informações falsas e prejudiciais pode levar outras pessoas a acreditar em algo que não é verdade, prejudicando assim a honra da pessoa retratada.

Além disso, *deepfakes* também podem se enquadrar no âmbito da calúnia. Se o conteúdo criado por meio de *deepfake* incluir acusações falsas de crimes, comportamento imoral ou desonestidade, isso constitui uma calúnia. A calúnia envolve a divulgação de informações falsas que prejudicam a reputação de uma pessoa, o que é uma clara violação ao direito à honra.

Ademais, há que observar que os *deepfakes* também podem ter repercussões profissionais negativas. Quando *deepfakes* difamatórios são amplamente divulgados, eles podem afetar a reputação da pessoa perante seus colegas de trabalho, empregadores e associados, prejudicando assim sua honra objetiva. Considerando que esse aspecto é relacionado à percepção da sociedade em relação à pessoa retratada, é mister concluir a possibilidade de um impacto significativo na carreira profissional da vítima do *deepfake*.

Em que pese ser fundamental sua tutela jurídica, o direito à honra não é absoluto e deve ser equilibrado com outros direitos e interesses, como a liberdade de expressão e a liberdade de imprensa. O exercício responsável da liberdade de expressão não deve infringir injustamente o direito à honra de terceiros. Sob esse prisma, é interessante o embate do *deepfake* com o direito à honra, quando a mídia manipulada fora elaborada embasada no direito de sátira.

Por um lado, tem-se o *deepfake* criado exclusivamente com fins satíricos – o que em última análise, é um desdobramento da liberdade de expressão –, enquanto, do outro, há uma pessoa, geralmente pública, que entendeu que sua honra subjetiva foi atacada, não ficando satisfeita com as críticas oriundas da sua representação no *deepfake*.

1.4.4 Direito à identidade

O direito à identidade é o princípio legal que assegura a cada indivíduo o reconhecimento e a proteção de sua singularidade pessoal, abrangendo elementos como nome, gênero, religião e orientação sexual. Este direito visa garantir a autodeterminação e igualdade, proibindo discriminação com base em características pessoais. Nesse sentido, o direito à identidade é essencial para a dignidade humana e é uma parte fundamental dos direitos humanos.

Com efeito, destaque-se que:

> Conquanto não desfrute de previsão legal expressa, o direito à identidade pessoal assegura a identificação da pessoa com base nas suas escolhas de vida, de modo de a se retratar, com fidedignidade, suas características a partir de suas legítimas opções. Tutela-se o sujeito que se vê lesado na sua dignidade por ser retratado com caracteres identificativos incompatíveis com aqueles que escolhera para guiar sua vida pessoal e social. O direito à identidade pessoal refere-se, portanto, ao direito de ser identificado de forma condizente com suas genuínas escolhas de vida. (TEPEDINO; OLIVA, 2023, p. 165).

Traçando um perfil histórico, é possível constatar que o instituto sofreu transformações conceituais ao longo do tempo – tal como o direito à imagem. Nessa toada, cumpre destacar que o direito à identidade pessoal estava vinculado, na maioria dos casos, ao conceito de imagem-atributo, deixando de ser somente compreendido pelas características de como determinada pessoa se apresenta perante a sociedade, para abranger, sob a ótica digital, a ideia de tutela da personalidade, à luz do princípio da dignidade humana, vista pelo direito de livre construção da própria identidade a partir do reconhecimento das peculiaridades e preferências do indivíduo. (KONDER, 2018).

Nesse sentido, cabe salientar dois exemplos sobre hipóteses em que a verificação da violação ao direito à identidade pessoal não se confunde com qualquer outro dano ao direito da personalidade. Veja-se:

> O professor que, por exemplo, tem repetidamente associada a si uma tese científica que jamais defendeu sofre um desrespeito à sua dignidade. Não se trata de violação à sua honra (a tese, note-se, pode ser admirável, só não é sua), nem tampouco de violação à sua privacidade ou à sua imagem. Trata-se de violação ao seu nome em um sentido bem mais amplo, que corresponde à sua própria identidade pessoal. É também o que ocorre com o sujeito que vem associado, em certa reportagem, a uma orientação política ou religiosa da qual não partilha. O direito à identidade pessoal protege a pessoa humana contra esses atos que a coloquem, na eloquente expressão italiana, *sotto falsa luce* (sob falsa luz), apresentando-a de modo errôneo no meio social. (SCHREIBER, 2014, p. 214).

Devidamente apresentada a conceituação do direito à identidade pessoal, passasse a se analisar como a manipulação do meio digital pelo *deepfake* impacta esse direito personalíssimo. Em um primeiro plano, depreende-se que o *deepfake* viola o direito à identidade pessoal, na medida em que ele reproduz os traços únicos e característicos da vítima, para manipular a sua identidade dentro de um conteúdo digital intangível.

A sensação de se deparar com uma reprodução própria e perfeita no meio digital, mesmo que falsa, pode ser perturbadora para qualquer pessoa. Nesse contexto, a violação a esse direito também transgride o princípio da autodeterminação, de modo que a mídia manipulada pode adotar um comportamento que a vítima nunca teria adotado na realidade. Por essa razão, a tutela do direito à identidade pessoal é fundamental para que se garanta a dignidade e a autonomia de cada indivíduo.

Em um segundo panorama, constata-se a ameaça do *deepfake* ao direito à identidade ao viabilizar que terceiros controlem e distorçam a imagem e a voz de alguém de forma enganosa, para fins de fraude. Pior ainda, o cenário em que se realiza o *deepfake* de pessoa socialmente influente, para induzir um número indeterminado de pessoas a caírem em algum golpe ou a cometerem ato ilícito[8].

1.5 IMPLICAÇÕES NO ÂMBITO *POST-MORTEM*

À medida em que as novas tecnologias são implementadas no cotidiano social, cada vez mais o ordenamento jurídico brasileiro enfrenta desafios, precisando realizar uma constante atualização e adequação das suas normas, de modo a prestar repostas aos anseios dos sujeitos de direito. É nessa perspectiva, que a manipulação do meio digital pelo uso do *deepfake* demanda uma readequação do ordenamento jurídico, sobretudo, no âmbito pós-morte.

Como é consabido, "a personalidade se extingue com a morte do sujeito, sendo intransmissível". (TEPEDINO; OLIVA, 2023, p. 180). Tal afirmativa é uma interpretação direta derivada do artigo 6º do Código Civil de 2002. Nesse sentido, não há como se admitir lesão aos direitos da personalidade após a morte do sujeito, tendo em visto que esses restaram extintos no momento do óbito.

Não obstante, é relevante concluir que a prática que tenha como pressuposto atingir o *de cujus* ainda pode reclamar a responsabilização pela conduta. Isso porque se admite a possibilidade de aplicação do conceito de dano por ricochete, compreendido pela extensão dos

[8] Com efeito, cabe mencionar a situação envolvida com o *youtuber* James Stephen Donaldson ("Mr.Beast"), reconhecido na internet pelas suas ações de filantropia, na qual foram recriados seus rosto e voz por meio de *deepfake*, com o único propósito de se aplicar golpes – o que era levado a efeito com a divulgação de anúncios falsos com a versão *deepfake* desse influenciador. (TI INSIDE, 2023).

danos causados por um ato ilícito a terceiros que não foram diretamente afetados, mas sofreram consequências em decorrência do evento.

A despeito da temática do dano por ricochete, veja-se o seguinte ensinamento doutrinário:

> É que quando uma ofensa é dirigida diretamente a uma pessoa já falecida não produz qualquer efeito jurídico, na medida em que o morto não mais ostenta personalidade jurídica, por motivos óbvios. No entanto, ao atingir, diretamente alguém que já faleceu o dano termina por reverberar sobre os seus familiares vivos, indiretamente. É dizer: o dano é diretamente dirigido ao falecido, mas atinge, obliquamente, pessoas que estavam atreladas afetivamente a ele. (FARIAS; ROSENVALD, 2016).

No caso de *deepfake* no âmbito *post-mortem*, um aspecto relevante é a possibilidade de autorização do uso da imagem e da voz do falecido para a criação desse conteúdo manipulado. A legislação e regulamentação podem estabelecer diretrizes para obter essa autorização, como por meio de disposições testamentárias ou acordos prévios. Essa abordagem permitiria um equilíbrio entre o respeito à vontade do falecido e a proteção de sua imagem, ao mesmo tempo em que imporia limites para evitar abusos ou fins ilícitos.

Em meio à inexistência de uma legislação específica que regulamente a matéria, cumpre pontuar que determinada corrente doutrinária propõe a estrita observação do artigo 11 do Código Civil de 2002, uma vez que “[...] os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". (BRASIL, 2002). Em paralelo, seria imperioso analisar o artigo 24, IV, da Lei nº 9.610/1998, que disciplina que certos direitos do autor são transmitidos aos seus herdeiros e sucessores, restando, a eles, a incumbência de "assegurar a integridade da obra, opondo-se a quaisquer modificações ou à prática de atos que, de qualquer forma, possam prejudicá-la ou atingi-lo, como autor, em sua reputação ou honra". (BRASIL, 1998).

Para Alexandre Freire Pimentel (2023), os dispositivos acima mencionados permitem, em primeiro lugar, a extração da ideia de que a imagem da pessoa falecida faz parte dos direitos vitais da personalidade, que são inalienáveis e não podem ser renunciados, não se encaixando na categoria de herança digital. Entretanto, os direitos morais e financeiros das obras autorais da pessoa falecida são transmitidos aos herdeiros e sucessores, ou seja, eles têm o direito de

obter lucro a partir das criações do falecido, mas não têm o direito de utilizar a imagem, corpo, voz, criar vídeos fora de contexto, empregar hologramas, *deepfakes* ou tecnologias similares de Inteligência Artificial para simular a interação da pessoa falecida em situações não vivenciadas, especialmente com fins lucrativos, o que supostamente violaria o artigo 11 do Código Civil.

Contudo, essa conclusão não parece a mais precisa, considerando que o legislador, à época da elaboração da norma, não tinha como prever a existência da tecnologia do *deepfake*. A aplicação literal do artigo 11 do Código Civil, desconsidera, por exemplo, a livre disposição da imagem do *de cujus* por vontade testamentária, posto que intransmissíveis os direitos da personalidade. Desse modo, depreende-se, respeitosamente, que a aplicação gramatical do artigo 11 do Código Civil de 2002, nesse caso específico de *deepfake*, incorreria na violação do princípio constitucional da razoabilidade.

É por essa razão que se torna necessária a criação de uma legislação específica que regule a matéria. Durante o seu ínterim, cabe ao Poder Judiciário solucionar as matérias provocadas pelos casos de *deepfake* no âmbito *post-mortem*, utilizando-se da interpretação teleológica e ampliativa das normas vigentes.

1.6 ESTUDO DE CASOS

Cada caso de *deepfake* deve ser analisado individualmente para determinar se há violação de direitos legais ou éticos. É necessário considerar fatores como o consentimento da pessoa envolvida, a finalidade do *deepfake*, o impacto na reputação ou privacidade da pessoa e se há qualquer forma de exploração, difamação ou uso indevido de sua imagem. Além disso, é importante que a legislação seja adaptada e atualizada para enfrentar os desafios específicos dos *deepfakes*.

Desse modo, é necessário conscientizar a sociedade sobre os riscos e implicações dos *deepfakes*, para que as pessoas estejam cientes de seus direitos e possam identificar possíveis violações. A educação sobre a detecção e prevenção de deepfakes, bem como o conhecimento dos recursos legais disponíveis, pode ajudar a mitigar o impacto negativo dessa tecnologia. Para tanto, urge a necessidade de se analisar os mais recentes casos em que se utilizou o *deepfake* com alguma finalidade que não tenha encontrado amparo das disposições legais do Estado Democrático de Direito.

1.6.1 *Deepfake* como arma de guerra

Em março de 2022, durante a Guerra na Ucrânia, circulou nas redes sociais um vídeo *deepfake* de Volodymyr Zelensky, presidente ucraniano, no qual ele parecia pedir aos ucranianos que se rendessem à Rússia. A cena mostrava Zelensky atrás de um pódio presidencial branco, com uma voz distorcida e um corpo quase imóvel, exceto pela cabeça. Esse vídeo falso viralizou rapidamente e foi identificado como um *deepfake*.

O caso de Zelensky evidencia o potencial de impacto da utilização dos *deepfakes*, podendo ser equiparada a uma das armas bélica desse conflito armado. Além do vídeo de Zelensky, também circulou outro *deepfake* retratando o presidente russo, Vladimir Putin, supostamente declarando paz na guerra da Ucrânia. Essa utilização de *deepfakes* para influenciar pessoas durante uma guerra é particularmente perniciosa, uma vez que a desinformação pode semear confusão e gerar consequências perigosas.

A disseminação de *deepfakes* durante uma guerra traz desafios adicionais para combater a desinformação. Durante o conflito entre Rússia e Ucrânia, as redes sociais têm sido inundadas com informações em tempo real, tanto verdadeiras quanto falsas. A natureza visual e emocional dessas informações torna ainda mais difícil discernir rapidamente o que é real do que é falso. Especialistas em desinformação alertam que, uma vez que a confiança nas informações é abalada, a própria noção de verdade é comprometida. (METZ, 2022).

Isso pode ter um impacto significativo em uma sociedade, gerando uma falta de confiança generalizada em todas as informações. Portanto, é crucial desenvolver mecanismos eficazes para identificar e combater os *deepfakes*, garantindo a autenticidade e a confiabilidade das informações.

A detecção automatizada de *deepfakes* tem avançado, com algoritmos sendo desenvolvidos para identificar sinais de adulteração nos vídeos. No entanto, essas técnicas enfrentam desafios à medida que os *deepfakes* se tornam mais sofisticados. A detecção manual por especialistas humanos ainda é considerada essencial para identificar *deepfakes* com precisão. Algumas iniciativas propõem o envolvimento do público em geral, oferecendo

recompensas para pessoas que encontrarem e denunciarem *deepfakes*, complementando os esforços das empresas de tecnologia.

O caso de *deepfake* durante a guerra na Ucrânia ressalta a necessidade de uma abordagem mais ampla para combater a desinformação online. As empresas de mídia social desempenham um papel crucial, mas é importante que elas atuem de forma mais proativa e eficaz na identificação e remoção de conteúdo enganoso. Além disso, iniciativas governamentais e legislações específicas podem ajudar a abordar o problema, estabelecendo diretrizes e restrições para a disseminação de *deepfakes*.

Em última análise, combater o uso de *deepfakes* como arma de guerra requer uma abordagem multidimensional que envolva tecnologia avançada, esforços humanos e políticas regulatórias. A sociedade como um todo deve estar atenta aos desafios impostos pelos *deepfakes* e trabalhar em conjunto para proteger a integridade da informação e evitar consequências prejudiciais.

1.6.2 *Deepfake* na pornografia

O aplicativo *DeepNude* ganhou destaque em 2019 devido à sua capacidade de criar imagens realistas de mulheres nuas a partir de fotos vestidas, utilizando técnicas de *deep learning*. No entanto, o aplicativo foi alvo de controvérsias significativas em relação à privacidade, ética e o potencial para o uso indevido de suas funcionalidades.

O *DeepNude* foi criticado por muitos por sua clara exploração e objetificação do corpo feminino, alimentando preocupações sobre a disseminação de imagens pornográficas não consensuais. Além disso, a natureza invasiva do aplicativo gerou preocupações sobre o consentimento e a privacidade das pessoas cujas imagens foram utilizadas sem sua permissão.

A rápida disseminação de imagens geradas pelo *DeepNude* também levantou questões sobre o potencial para o *bullying*, assédio e *cyberstalking*. O aplicativo facilitou a criação de conteúdo pornográfico falso e não consensual, o que pode causar danos emocionais e prejudicar a reputação e a dignidade das pessoas envolvidas. Em resposta a essas preocupações e à pressão da sociedade, o desenvolvedor do *DeepNude*, ciente das implicações éticas e legais de seu aplicativo, removeu-o do mercado e interrompeu seu desenvolvimento e distribuição.

O caso do *DeepNude* destaca a necessidade de um diálogo contínuo sobre o uso ético e responsável da tecnologia. Essa tecnologia deve ser usada com consideração aos direitos individuais, consentimento informado e respeito à dignidade humana. A legislação também desempenha um papel fundamental na proteção das vítimas de *deepfakes* e na responsabilização dos criadores desses conteúdos manipulados.

É essencial que as pessoas estejam cientes dos riscos associados a aplicativos como o *DeepNude* e que exijam transparência e responsabilidade dos desenvolvedores. Além disso, é fundamental promover a educação sobre os perigos dos *deepfakes* e fornecer suporte às vítimas afetadas por seu uso indevido.

Em resumo, o caso do aplicativo *DeepNude* ilustra as complexidades éticas e legais associadas ao uso de tecnologias de manipulação de imagens. Esse tipo de aplicativo levanta preocupações significativas em relação à privacidade, consentimento e objetificação do corpo humano. É necessário promover uma discussão aberta sobre os impactos negativos dessas tecnologias e adotar medidas para proteger os direitos individuais e evitar a disseminação de conteúdo prejudicial.

1.6.3 Vazamento de dados por aplicativo gerador de *deepfake*

O aplicativo ZAO foi lançado na China em 2019 e permitia aos usuários inserir seus rostos em cenas de filmes e programas de televisão famosos, utilizando a tecnologia de *deepfake*. No entanto, em setembro de 2019, surgiram preocupações sobre a segurança e privacidade dos usuários em relação ao ZAO. (ITFORUM, 2019).

Relatos indicaram que o aplicativo coletava uma quantidade significativa de dados pessoais dos usuários, incluindo fotos faciais e informações de identificação. Essas informações poderiam ser usadas para alimentar seus algoritmos de *deepfake* e melhorar a qualidade das manipulações de rosto.

No entanto, o que levantou preocupações foi a forma como esses dados estavam sendo armazenados e utilizados. Houve alegações de que os termos de serviço do ZAO permitiam que a empresa detentora dos dados, a Momo Inc., usasse e compartilhasse essas informações de

maneiras não especificadas, levantando preocupações sobre a privacidade e a segurança dos usuários.

O vazamento de dados é uma séria violação da privacidade e pode ter consequências negativas para os usuários. Informações pessoais e imagens faciais podem ser usadas de forma inadequada, como para a criação de *deepfakes* sem consentimento ou até mesmo para atividades criminosas, como o roubo de identidade.

No caso específico do ZAO, não houve relatos de um vazamento de dados em larga escala, como ocorreu em outros incidentes envolvendo aplicativos e empresas. No entanto, a polêmica em torno dos termos de serviço e a coleta excessiva de informações sensíveis geraram preocupações significativas sobre a segurança e privacidade dos usuários.

Esse caso destaca a importância de os usuários estarem cientes dos termos de serviço e das políticas de privacidade dos aplicativos que utilizam. É essencial entender como suas informações pessoais são coletadas, armazenadas e utilizadas, bem como quais medidas de segurança estão em vigor para proteger esses dados.

Para garantir a segurança e a privacidade, é recomendável que os usuários adotem boas práticas, como ler atentamente os termos de serviço, limitar o compartilhamento de informações pessoais e utilizar aplicativos de fontes confiáveis e bem estabelecidas.

Além disso, a regulamentação adequada e a fiscalização das práticas de coleta de dados pelos governos também são fundamentais para proteger os direitos dos usuários e evitar vazamentos e abusos de dados.do presente trabalho é analisar a aplicação da responsabilidade civil pelas violações aos direitos à imagem e à identidade pessoal decorrentes da manipulação articulada pelo uso de perfis falsos e de *deepfakes* na internet.

Nesse sentido, pretende-se investigar de que modo os direitos à imagem e à identidade do terceiro são violados no ambiente digital; quais figuras podem ser responsabilizadas pela utilização indevida dessas novas tecnologias; e quais são os posicionamentos adotados pela jurisprudência e pela doutrina quanto à reparação apropriada ao terceiro que fora influenciado pela manipulação do meio digital.

1.6.4 *Deepfake* como ferramenta de espionagem

O caso de *deepfake* envolvendo Katie Jones chamou a atenção da mídia e dos especialistas em segurança cibernética, em 2019. Katie Jones era uma suposta especialista em políticas internacionais e que possuía conexões com pessoas da Rússia em várias redes sociais, incluindo *LinkedIn* e *Twitter*.

No entanto, descobriu-se que Katie Jones não era uma pessoa real, mas sim um perfil criado com a ajuda de tecnologia de *deepfake*. O objetivo por trás da criação desse perfil falso de Katie Jones ainda é objeto de especulação, mas há indícios de que ele pode ter sido criado para estabelecer conexões com indivíduos influentes e obter informações privilegiadas. Acredita-se que a técnica de *deepfake* tenha sido utilizada para criar uma imagem e identidade convincentes de Katie Jones, de modo que seus alvos passassem a confiar nela.

Esse caso ilustra o potencial de manipulação e engano que os *deepfakes* podem oferecer. Ao criar um perfil falso com informações e fotos fictícias, os criadores do *deepfake* podem facilmente enganar e estabelecer relações com indivíduos que, de outra forma, poderiam ser mais cautelosos em interagir.

O caso de Katie Jones destaca a importância de uma verificação cuidadosa das identidades *online*, especialmente quando se trata de conexões profissionais e relacionamentos de confiança. Também ressalta a necessidade contínua de desenvolver tecnologias de detecção de *deepfake* mais avançadas para combater a disseminação de informações falsas e proteger a integridade das comunicações online.

Além disso, casos como esse levantam questões sobre a necessidade de regulamentação e legislação adequadas para combater o uso malicioso de *deepfakes*. É essencial que sejam estabelecidos mecanismos legais para responsabilizar aqueles que criam e distribuem *deepfakes* com a intenção de enganar, prejudicar ou obter vantagens indevidas. O caso de Katie Jones serve como um lembrete da importância de manter um pensamento crítico e cautela ao interagir com pessoas online, bem como de buscar fontes confiáveis de informações e adotar medidas de segurança adequadas para proteger a privacidade e a identidade pessoal.

A disseminação de *deepfakes* pode ter consequências prejudiciais, e é fundamental estar alerta e informado sobre essa ameaça em constante evolução. Em última análise, o caso de Katie Jones destaca a necessidade de conscientização e educação sobre os riscos e impactos dos *deepfakes*. É essencial que indivíduos, empresas e governos trabalhem juntos para enfrentar os desafios apresentados por essa tecnologia, desenvolvendo estratégias de defesa, implementando políticas de segurança cibernética mais rigorosas e promovendo uma cultura de responsabilidade e ética digital.

1.6.5 *Deepfake post-mortem*: Elis Regina e o comercial da Volkswagen

A Volkswagen lançou uma campanha para celebrar seu septuagésimo aniversário no mercado brasileiro, surpreendendo o público com um comercial que uniu a cantora Elis Regina, falecida em 1982, e sua filha, Maria Rita, em uma interpretação da icônica canção “Como Nossos Pais”.

A agência de publicidade AlmapBBDO, encarregada da campanha, buscou combinar elementos de nostalgia com inovação para destacar a marca como um elo entre diferentes gerações e demonstrar seu compromisso com veículos elétricos. O comercial, que foi desenvolvido ao longo de nove meses, gerou discussões sobre o uso de tecnologia de inteligência artificial e *deepfake* na publicidade, levantando questões sobre ética e autenticidade.

Por meio do *deepfake*, foi possível para recriar a imagem de Elis Regina, o que envolveu mapear milhares de fotos e vídeos da cantora. Posteriormente, esses dados foram aplicados sobre a imagem de uma atriz que participou do comercial, com auxílio da inteligência artificial, transformando-a no rosto de Elis Regina.

As reações nas redes sociais foram diversas, com algumas pessoas elogiando a união entre mãe e filha no comercial e a homenagem à memória de Elis Regina. No entanto, houve críticas quanto ao uso do *deepfake* para representar uma pessoa falecida, bem como o uso de sua imagem para um comercial cuja empresa fora apontada no relatório da Comissão Nacional

da Verdade (CNV) de 2014[9] como cúmplice da repressão ocorrida na época da ditadura militar brasileira – regime do qual Elis Regina era declaradamente opositora. (SPLASH, 2023).

A partir desse panorama, depreende-se dois pontos relevantes envolvendo *deepfake*, no contexto *post mortem*, a serem enfrentados pelo ordenamento jurídico nos próximos anos. O primeiro aspecto é sobre a possibilidade de se dispor sobre a imagem e voz após a morte, de modo a autorizar os seus usos para a criação de *deepfake* do falecido. Sobre esse ponto, não há nenhum óbice legal para que se elabore um testamento predispondo acerca do futuro uso da imagem e da voz, até mesmo porque, em se tratando de Direito das Sucessões, deve ser observado o princípio da vontade manifestada.

No caso concreto, Elis Regina não deixou testamento que se houvesse manifestação nesse sentido. Contudo, seus herdeiros autorizaram o uso da imagem da cantora. À vista disso, em que pese a omissão normativa, não se verificam razões para obstar a realização do comercial nos moldes propugnados. Importante mencionar ainda, a Decisão proferida pelo Ministro Barros Monteiro nos autos do Recurso Especial n.º 86.109/SP, em que se entendeu que a "utilização da imagem da pessoa, com fins econômicos, sem a sua autorização ou do sucessor, constitui locupletamento indevido, a ensejar a devida reparação". (BRASIL, 2001).

Sob um segundo prisma, indaga-se se Elis Regina concordaria em participar da propaganda de empresa que pode ter relações com o regime autoritário de 1964, do qual a cantora era manifestamente opositora. Apesar de a pergunta não poder ser respondida, não se afigura razoável indicar que, ao ter "participado" do comercial, causou-se dano à imagem, honra ou identidade da cantora, isso porque os direitos da personalidade pressupõem a existência da pessoa natural, que, por força do artigo 6º do Código Civil de 2002[10], se extingue com a morte do sujeito.

[9] Sobre o caso, veja-se a matéria jornalística: "A montadora de origem alemã, cuja cumplicidade com a repressão nos anos de chumbo já havia sido apontada no relatório da Comissão Nacional da Verdade (CNV) de 2014, assumiu o compromisso de destinar 36,3 milhões de reais tanto a ex-empregados presos, perseguidos ou torturados como a iniciativas de promoção de direitos humanos". (VENDRUSCOLO, 2020).

[10] *In verbis*: "Art. 6º A existência da pessoa natural termina com a morte; presume-se esta, quanto aos ausentes, nos casos em que a lei autoriza a abertura de sucessão definitiva" (BRASIL, 2002).

CAPÍTULO 2 – A REGULAMENTAÇÃO DO *DEEPFAKE* E A QUESTÃO DA RESPONSABILIDADE CIVIL

2.1 REGULAMENTAÇÃO DO USO DO *DEEPFAKE*

À míngua de uma norma específica e inspirado pelos casos recentes de *deepfake* – notadamente, o comercial da Volkswagem que "reviveu" a cantora Elis Regina por meio da tecnologia do *deepfake* –, fora apresentado em meados de julho de 2023, um Projeto de Lei de autoria do senador Rodrigo Cunha (Podemos-AL), por meio do qual se buscou disciplinar e estabelecer regras para a utilização do conteúdo manipulado pelo *deepfake*, principalmente quando for o caso de pessoas já falecidas.

Nesse contexto, o Projeto de Lei recebeu o número 3.592/2023, contendo, ao todo, 09 (nove) artigos. Veja-se os dispositivos mais relevantes:

> Art. 2º O uso da imagem de uma pessoa falecida por meio de IA requer o consentimento prévio e expresso da pessoa em vida ou, na ausência deste, dos familiares mais próximos.
> Parágrafo único. O consentimento deve ser obtido de forma clara, inequívoca e documentada, e deve especificar os fins para os quais a imagem ou áudio serão utilizados.
> Art. 3º Os herdeiros legais da pessoa falecida têm o direito de preservar a memória e a imagem do falecido, bem como o direito de controlar o uso dessa imagem.
> Parágrafo único. Os herdeiros têm o direito de recusar o uso da imagem ou áudio da pessoa falecida por meio de IA, mesmo que o consentimento tenha sido dado anteriormente.
> Art. 4º O uso da imagem e áudio da pessoa falecida por meio de IA para fins comerciais precede de autorização expressa dos herdeiros legais ou da pessoa falecida em vida.
> Art. 5º Caso o falecido tenha expressado, em vida, sua vontade de não permitir o uso de sua imagem após seu falecimento, essa vontade deverá ser respeitada. (CUNHA, 2023).

Em relação ao artigo 2º e seu parágrafo único, verifica-se que foi estabelecida a necessidade de obter o consentimento prévio e expresso da pessoa em vida ou, na falta deste, dos familiares mais próximos, para o uso da imagem de uma pessoa falecida por meio de IA.

O parágrafo único enfatiza a clareza, inequivocidade e documentação desse consentimento, exigindo que sejam especificados os fins para os quais a imagem ou áudio serão

utilizados. Esse dispositivo visa garantir que a vontade da pessoa ou de seus familiares seja respeitada na utilização da imagem pós-morte, promovendo transparência e controle.

Já quanto ao artigo 3º e seu parágrafo único, confere-se aos herdeiros legais o direito de preservar a memória e a imagem do falecido, bem como o direito de controlar o uso dessa imagem.

O parágrafo único estabelece que os herdeiros podem recusar o uso da imagem ou áudio da pessoa falecida por meio de IA, mesmo que o consentimento tenha sido dado anteriormente. Isso garante que os herdeiros tenham poder de veto sobre a utilização da imagem pós-morte, assegurando o respeito aos desejos da família e a preservação da reputação do falecido.

Por outro lado, o artigo 4º estipula que o uso da imagem e áudio da pessoa falecida por meio de IA para fins comerciais só é permitido com autorização expressa dos herdeiros legais ou da pessoa falecida em vida. Esse dispositivo protege os direitos econômicos da família e da própria pessoa falecida, evitando que terceiros lucrem com sua imagem de forma não autorizada.

Por fim, o artigo 5º determina que, se a pessoa falecida tiver expressado, em vida, sua vontade de não permitir o uso de sua imagem após o falecimento, essa vontade deve ser respeitada. Isso reforça a importância do respeito aos desejos da pessoa falecida, garantindo que suas escolhas sejam mantidas após sua morte.

No geral, esse projeto de lei busca equilibrar os interesses da privacidade, memória e direitos econômicos das pessoas falecidas e seus herdeiros. Ele estabelece diretrizes claras para o uso da imagem e áudio por meio de IA, visando à proteção dos direitos pós-morte e a prevenção de abusos. Ademais, identifica-se uma certa busca por um equilíbrio entre o respeito à autonomia do falecido e a proteção de sua imagem, garantindo que os herdeiros e a própria pessoa em vida possam controlar o uso de sua imagem póstuma, especialmente em contextos comerciais.

Enquanto o Projeto de Lei ainda não for votado, resta aplicar os elementos da responsabilidade civil na reparação de danos decorrentes da manipulação do meio digital pelo *deepfake*.

2.2 RESPONSABILIDADE CIVIL PELO USO NÃO CONSENTIDO DO *DEEPFAKE*

Conforme visto, na ausência de lei específica que regule o *deepfake*, incumbe à responsabilidade civil o dever de trazer a reparação nas hipóteses em que restarem preenchidos os seus elementos. Com efeito, a doutrina leciona que:

> Só se cogita, destarte, de responsabilidade civil onde houver violação de um dever jurídico e dano. Em outras palavras, responsável é a pessoa que deve ressarcir o prejuízo decorrente da violação de um precedente dever jurídico. E assim é porque a responsabilidade pressupõe um dever jurídico preexistente, uma obrigação descumprida. Daí ser possível dizer que toda conduta humana que, violando dever jurídico originário, causa prejuízo a outrem é fonte geradora de responsabilidade civil. (CAVALIERI FILHO, 2012, p. 02).

A análise prática da incidência de responsabilidade civil em casos de *deepfake* depende da verificação de seus elementos na hipótese fática. Nesse sentido, cumpre salientar certa divergência doutrinária para estabelecer a quantidade de aspectos que compreendem os chamados elementos ou pressupostos da responsabilidade civil. Dessa forma, há que se adentrar previamente nessa discussão para balizar a incidência da responsabilidade civil nas situações de *deepfake*.

Parte da doutrina entende que, da compreensão do artigo 186 do Código Civil de 2002, constata-se que são 04 (quatro) os elementos essenciais da responsabilidade civil, dentre eles: ação ou omissão, culpa ou dolo do agente, relação de causalidade e o dano experimentado pela vítima. (GONÇALVES, 2019).

Já para outra corrente doutrinária, contemporaneamente, a divisão dos pressupostos da responsabilidade é realizada sob 03 (três) facetas, quais sejam: a conduta (entendida como o ato culposo ou atividade objetivamente considerada), o dano e o nexo de causalidade. (TEPEDINO; TERRA; GUEDES, 2023).

Nessa última linha de pensamento, entende-se que:

> Embora mencionada no referido dispositivo de lei por meio das expressões “ação ou omissão voluntária, negligência ou imprudência”, a culpa (em sentido lato, abrangente do dolo) não é, em nosso entendimento, pressuposto geral da responsabilidade civil, sobretudo no novo Código, considerando a

> existência de outra espécie de responsabilidade, que prescinde desse elemento subjetivo para a sua configuração (a responsabilidade objetiva). (GAGLIANO; PAMPLONA FILHO, 2012, p. 24-26).

Em que pese a divergência doutrinária acerca do quantitativo dos pressupostos da responsabilidade civil, é certo que tal fato não prejudica o olhar sobre como esses elementos se comportam nos casos de *deepfake*.

2.2.1 Conduta

O elemento da conduta, em um primeiro plano, se refere a um ato ilícito positivo ou negativo cometido por um indivíduo, isso porque a responsabilidade pode decorrer de ações que o agente tenha efetuado ou de omissões nas quais tenha incorrido.

Desde já, é importante destacar que a responsabilidade pode se originar não apenas de atos diretamente cometidos pelo próprio agente, mas também de ações realizadas por terceiros que estejam sob sua guarda ou responsabilidade – a exemplo dos filhos menores e empregados –, ou então, de danos causados por objetos e animais que pertençam ao agente.

Com efeito, nos termos do artigo 186 do Código Civil de 2002, "*aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito*" (BRASIL, 2002).

Assim, nota-se que o ato ilícito, para o ordenamento jurídico pátrio, presume uma ação ou omissão voluntária do agente, vinculada a uma culpa em *lato sensu*, isto é, que pode ocorrer tanto na modalidade de dolo – quando há a intenção de provocar o prejuízo –, como na de culpa em *stricto sensu* – consubstanciada pela falta de observância de um dever jurídico. (SCHREIBER; RIBAS; MANSUR, 2020).

Nessa toada, afigura-se relevante diferenciar a responsabilidade civil objetiva da subjetiva. Na primeira, o aspecto da culpa é dispensado, razão pela qual o agente será responsabilizado independentemente se agiu com dolo ou culpa em sentido estrito. Já em relação à segunda, a culpa desempenha um papel fundamental, e o agente só pode ser responsabilizado se for comprovada sua negligência, imprudência ou dolo no ato que causou o dano.

Mesmo que se admitam hipóteses de responsabilidade civil objetiva em casos de *deepfake* – notadamente, as estipuladas em lei, tal como em situações de relação de consumo[11-12] –, todas as demais hipóteses versarão sobre responsabilidade civil subjetiva, o que exige a comprovação da culpa em sentido amplo.

Desse modo, verifica-se o elemento da conduta humana nas situações de manipulação do meio digital pelo *deepfake*, na medida em que a criação do conteúdo que violou direito ou gerou dano é ato positivo, demandando-se, inclusive, técnicas avançadas de processamento de imagem e áudio, bem como a utilização de algoritmos de aprendizado profundo. Em se tratando de hipótese em que se aplica a responsabilidade civil objetiva, tão somente essa caracterização já seria suficiente para se reconhecer o elemento conduta.

Por outro lado, nos casos de responsabilidade civil subjetiva, é necessário comprovar a culpa em *lato sensu*. Assim, há dolo quando o agente produz o *deepfake* com a intenção de difamar, difundir informações falsas – a exemplo das *deepfake news* –, obter vantagens ilegítimas ou prejudicar a reputação de uma pessoa ou algo que ela represente, por exemplo.

Já a culpa em sentido estrito pode ser observada, nas situações de manipulação do meio digital pelo *deepfake*, quando o autor cria ou dissemina o conteúdo falso sem devida diligência na verificação da sua autenticidade, sem considerar as consequências prejudiciais, ou ainda, sem deixar claro que se trata de uma mídia manipulada.

2.2.2 Dano

Outrossim, é imperioso analisar o elemento do dano no contexto da responsabilidade civil. O dano se desdobra no âmbito material e/ou moral, não sendo necessário, desse modo, que sua caracterização esteja vinculada apenas ao plano patrimonial. Ressalte-se que a

[11] "Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos". (BRASIL, 1990).

[12] "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos". (BRASIL, 1990).

inexistência de dano ou a ausência da prova de que ele tenha ocorrido, implica, mandatoriamente, na impossibilidade de responsabilização na esfera civil, não havendo que se falar em obrigação de se indenizar, porquanto se pressupõe a existência da violação de direito e do dano, concomitantemente. (GONÇALVES, 2019).

No contexto do *deepfake*, o dano pode abranger tanto o aspecto material quanto o moral. Sob essa perspectiva, o dano material pode se manifestar quando a divulgação de conteúdos falsos cause prejuízos financeiros diretos, como perda de oportunidades profissionais ou comerciais.

A despeito desse último exemplo, aplica-se a Teoria da Perda de Uma Chance, considerando-se que a repercussão da mídia manipulada deu causa a perda de uma chance legítima que a vítima tinha de obter um benefício, uma vantagem econômica, um direito, uma posição, ou qualquer outro ganho.

Em paralelo, é relevante considerar o dano moral, pois está intrinsecamente ligado à violação dos direitos da personalidade, posto que os desdobramentos da manipulação do meio digital pelo *deepfake* podem causar sofrimento emocional, angústia e constrangimento à pessoa retratada de maneira enganosa ou difamatória. Logo, não há dúvidas quanto à constatação do dano moral nesses casos de *deepfake*, tendo em vista que o bem-estar psicológico dessas pessoas é colocado em xeque.

Com efeito, deve ser registrada a concepção do dano por ricochete no âmbito do *deepfake*. Isso porque, esse conceito se refere a um tipo de dano que se origina indiretamente a partir de um evento ou ação inicial, mas que afeta terceiros que não estavam diretamente envolvidos na situação. É exatamente o caso do dano que atinge familiares decorrente da divulgação de *deepfake* que difama parente já falecido.

Torna-se mister mencionar que a doutrina vem admitindo uma certa flexibilização desse elemento da responsabilidade civil, o que está sendo chamado de “novos danos”:

> Neste contexto, os pressupostos da responsabilidade civil relacionados à imputação do dever de indenizar (culpa e nexo causal) perdem relevância em face de uma certa ascensão daquele elemento que consiste, a um só tempo, no objeto e na *ratio* da reparação: o dano. Por décadas relegado a um patamar

> secundário, advindo da sua fácil verificação sob a ótica materialista, este pressuposto – então, efetivamente pré-suposto – o dano vem, pouco a pouco, conquistando local de destaque na análise jurisprudencial, como elemento apto, por si só, a atrair a atuação das cortes em amparo às vítimas dos infortúnios mais diversos. (SCHREIBER, 2009, p. 81)

A aplicabilidade dessa tese vai ao encontro daquilo que se pode esperar em relação aos desdobramentos do *deepfake*. Essa afirmativa fica mais evidente, sabendo-se que o *deepfake* pode causar dano moral coletivo, caso afete interesses metaindividuais, como é o caso do seu uso para manipular informações durante as eleições.

Nesse sentido, é importante destacar a possibilidade de uma concepção de dano, relacionado ao *deepfake*, que não está abarcado pelos aspectos clássicos desse instituto jurídico, a exemplo do dano oriundo do abalo de confiança nas fontes de notícias jornalísticas com a disseminação generalizada de *deepfake news*.

2.2.3 Nexo de causalidade

O pressuposto do nexo de causalidade é definido como os vínculos de causa e efeito que unem a ação do agente ao dano sofrido pela vítima. Essa relação é crucial para se identificar se, no caso concreto, o agente tem o dever de indenizar a vítima considerando o impacto da sua conduta no dano experimentado.

Ao asseverar que “ainda que a inexecução resulte de dolo do devedor, as perdas e danos só incluem os prejuízos efetivos e os lucros cessantes por efeito dela direto e imediato, sem prejuízo do disposto na lei processual” (BRASIL, 2002), o legislador pátrio adotou a teoria do dano direto e imediato, por meio da qual se compreende que o dano deve ser uma consequência direta e imediata da ação do agente, sem a ocorrência de outros eventos ou condições intermediárias que desempenhem um papel significativo na produção do dano.

Não obstante, o instituto do nexo causal possui certa peculiaridade nos casos de *deepfake*, o que transcende a relação da conduta culposa do agente criador do conteúdo manipulado e do dano. Isso se deve ao fato de, em muitas ocasiões, o dano estar inexoravelmente ligado ao vultuoso compartilhamento do conteúdo manipulado. É dizer, nessa hipótese, que o dano pressupõe a divulgação em massa do *deepfake*, para além de sua criação pelo agente.

É preciso ter especial atenção quanto a esse ponto, uma vez que o ato de compartilhar o *deepfake* não configura causa superveniente de rompimento do nexo de causalidade entre o fato inicial e o dano. Isso ocorre porque, para que uma causa subsequente seja imputada o dano, é fundamental que ela não tenha relação com a causa anterior, de forma a permitir que seja atribuída a responsabilidade pelo dano de maneira exclusiva. (GUEDES, 2005).

Assim, é notório que o compartilhamento do conteúdo manipulado está relacionado ao *deepfake*, primeiramente, por uma questão lógica, já que aquele não seria possível sem a existência deste; e, em segundo, pois se supõe que uma mídia criada com a finalidade de causar repercussão no meio social será amplamente divulgada.

A despeito da possibilidade de o ato de compartilhar conteúdo nas redes sociais servir como motivo de interrupção do nexo de causalidade entre o material criado e o respectivo dano por ele causado, a doutrina esclarece que:

> O que se verifica nos danos causados por compartilhamento de conteúdo nas redes sociais, como regra, é justamente o oposto, sendo notório o vínculo de necessariedade entre a elaboração e o compartilhamento por terceiros, na medida em que esses materiais já são elaborados no intuito de "viralizar", sendo esse objetivo antecipado e almejado pelo criador. Embora não se possa desconsiderar a liberdade de decisão de cada pessoa que recebe o material em compartilhá-lo novamente ou não, o fenômeno assume um viés essencialmente coletivo, já sendo possível antever, com auxílio de aportes de ciência comportamental, que determinados conteúdos tendem a ser replicados, o que possibilita afirmar a continuidade (e não interrupção) da cadeia causal, sendo ambas as condutas – criação e compartilhamento – necessárias à produção do resultado danoso. (SCHREIBER; RIBAS; MANSUR, 2020, p. 621).

Ainda quanto à verificação do nexo causal nos casos de *deepfake*, torna-se eminente as diferentes perspectivas que a manipulação do meio digital pode conceber. Nesse sentido, é imperioso refletir se se configuraria nexo causal na hipótese de um *deepfake*, que difamasse determinado candidato político durante o período eleitoral, ocasionasse a diminuição do seu eleitorado e, por consequência, a eleição de seu concorrente.

Com base na teoria do dano direto e imediato, o nexo de causalidade restaria configurado, tão somente, na relação entre a conduta do agente criador do *deepfake* e o dano

oriundo da difamação suportada pelo candidato político, desde que comprovados os elementos da responsabilidade civil.

No mais, ainda que se argumente que a diminuição do eleitorado e a derrota na eleição foram ocasionados em alguma medida pelo *deepfake*, é certo que esse entendimento abrangeria circunstâncias indetermináveis, o que é vedado no ordenamento pátrio para fins de verificação do nexo causal.

2.2.4 Responsabilidade pelo compartilhamento do *deepfake*

Conforme já antecipado, para atribuir-se o dano a uma causa superveniente, é necessário que ela não esteja relacionada com a causa anterior, de modo que o dano seja imputado de maneira exclusiva. Por essa razão, compreende-se que o ato de compartilhar o *deepfake* não é capaz de romper o nexo de causalidade entre a elaboração do material manipulado (conduta culposa) e o dano, na medida em que "cada compartilhamento constitui uma causa concorrente ou complementar ao dano causado". (LEAL; SIQUEIRA, 2020, p. 121).

Por outro lado, não há como se afastar a possibilidade de se vincular o elemento da culpa ao ato de compartilhamento do *deepfake*, já que, a depender do caso, a conduta do agente reclama um padrão comportamental esperado no meio social.

Esse panorama se torna claro ao se observar o compartilhamento de *deepfake news* cuja falsidade já tenha sido reconhecida em veículos de grande circulação ou na mídia segmentada, em que pese a ausência de obrigação ética de averiguar a fonte daquele conteúdo manipulado, nos demais casos – diferentemente dos jornalistas, por exemplo. De igual forma, ao compartilhar *deepfake* de teor pornográfico, o agente está agindo com culpa, considerando o caráter sensível daquele conteúdo.

Para esses casos, em que se constata a existência de uma concorrência de agentes, admite-se a hipótese da responsabilidade solidária. À luz da inteligência do artigo 942, *caput*, do Código Civil de 2002, "os bens do responsável pela ofensa ou violação do direito de outrem ficam sujeitos à reparação do dano causado; e, se a ofensa tiver mais de um autor, todos responderão solidariamente pela reparação". (BRASIL, 2002).

Cumpre salientar que, na prática, a responsabilização pelo compartilhamento do *deepfake*, mesmo que com culpa, não é tão comum de se constatar. Isso ocorre porque a tecnologia é disseminada de forma ampla e anônima, tornando desafiador identificar individualmente as pessoas que efetivamente compartilharam o conteúdo manipulado e, até mesmo, o próprio criador daquele *deepfake*.

2.2.5 Responsabilidade dos provedores de aplicações pela remoção do conteúdo de terceiros

Tratando-se de responsabilidade civil dos provedores de aplicações sobre os conteúdos produzidos por terceiros em suas plataformas virtuais, é de extrema relevância analisar o tema sob dois cenários: em um primeiro plano, o período de consolidação jurisprudencial anterior à elaboração do Marco Civil da Internet (Lei n.º 12.965/2014) e, posteriormente, as alterações promovidas pelo marco regulatório e suas repercussões no ordenamento jurídico.

Em relação ao período anterior à Lei n.º 12.965/2014, ressalta-se que coube à jurisprudência erigir óbices que freassem o incentivo à liberdade no meio digital. Assim, entendeu-se que em casos de danos provocados por terceiros na internet, seria observado o prevalecimento da responsabilidade subjetiva tanto do agente causador do dano, quanto do provedor de aplicação – este último, na ocasião de não haver retirada do conteúdo danoso, após a notificação prestada pelo interessado.

Com o advento do Marco Civil da Internet, por meio de seu artigo 19, restou assentado que:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal. § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet,

> poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação. (BRASIL, 2014).

Diferentemente de como a jurisprudência se orientava, quando da míngua do Marco Civil da Internet, o artigo 19 da referida lei estipulou que a responsabilidade civil dos provedores precederia do não cumprimento de ordem judicial específica para tornar indisponível o conteúdo apontado como infringente.

Em que pese a mudança trazida pelo dispositivo legal em questão parecer ser ínfima, posto que passou a condicionar a retirada da mídia do ar à superveniência de ordem judicial específica, e não mais apenas na hipótese de notificação prestada pelo interessado, aponta a doutrina especializada que a positivação desse artigo foi de encontro aos preceitos constituídos no texto constitucional.

Nesse sentido, confira-se:

> Trata-se de matéria extremamente controvertida, mas o melhor entendimento é o de que o artigo 19 contrasta com o tecido constitucional por diversas razões: (a) ao condicionar a reparação de danos decorrentes da violação a direitos fundamentais ao descumprimento de uma ordem judicial específica, o dispositivo legal viola, em primeiro lugar, o artigo 5º, X, da Constituição brasileira, que não se limita a consagrar os direitos fundamentais à intimidade, privacidade, honra e imagem, mas também determina seja "[…] assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"; (b) ao impor o recurso ao Poder Judiciário como condição imprescindível para que o dano sofrido gere, mesmo em abstrato, responsabilidade civil, o artigo afronta a garantia de acesso à Justiça em sua dimensão substancial (CR, art. 5º, XXXV); (c) viola, ainda, o chamado princípio da vedação de retrocesso, na medida em que, ao condicionar a tutela de direitos fundamentais ao recebimento de "ordem judicial específica", promove o retrocesso em relação ao grau de proteção que já era assegurado aos direitos fundamentais pela jurisprudência brasileira, pois, antes da edição do Marco Civil da Internet, nossas cortes vinham considerando os réus responsáveis por tais violações se deixassem de agir após comunicação de qualquer espécie (incluindo, a notificação extrajudicial física ou até eletrônica; (d) ao fornecer proteção mais intensa, célere e efetiva aos direitos autorais conexos (incluindo, portanto, aqueles de conteúdo exclusivamente patrimonial) que a proteção reservada aos direitos fundamentais do ser humano, aos quais a Constituição brasileira atribuiu maior importância valorativa (CR, art. 1º, III), o dispositivo opera verdadeira inversão axiológica, incompatível com a hierarquia de valores

> constitucionais; (e) o condicionamento da responsabilidade civil dos chamados provedores de aplicações ao descumprimento de ordem judicial específica se afigura desproporcional, na medida em que exige imenso esforço da vítima para que obtenha a tutela de seus direitos da personalidade, ao mesmo tempo em que nenhuma concessão exige à liberdade econômica das sociedades proprietárias de redes sociais e outros ambientes virtuais. (SCHREIBER; RIBAS; MANSUR, 2020, p. 623-624).

Sem embargo, é relevante mencionar que o artigo 21 do Marco Civil da Internet, por sua vez, excepciona o conteúdo do artigo 19, na medida em que afasta a hipótese de responsabilidade civil subjetiva mediante ordem judicial específica, para passar a adotar o regime do *notice and takedown*[13]. (QUEIROZ, 2018).

Isso se deve ao fato de o artigo 21 do Marco Civil da Internet prever a responsabilização subsidiária do provedor de aplicações "pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado" (BRASIL, 2014), quando deixar de promover a indisponibilização do conteúdo, após o recebimento de notificação do interessado ou de seu representante legal.

Sob esse prisma, verifica-se que a referida norma legal nada diz quanto a necessidade de o conteúdo divulgado ser, mandatoriamente, um material naturalmente capturado. Dessa forma, é perfeitamente viável que a sanção prevista nesse artigo seja cabível nas hipóteses em que a mídia contendo nudez ou ato sexuais de caráter privado, tenha sido manipulado por meio do uso do *deepfake*.

Constata-se, portanto, que o legislador ofereceu uma base sólida para a responsabilização dos provedores de aplicações de internet quando se tratar de divulgação não autorizada de conteúdo íntimo, independentemente de ter sido criado ou modificado por meio de técnicas de *deepfake*.

[13] O instituto do *notice and takedown* refere-se a um procedimento legal utilizado em plataformas *online* e provedores de serviços na internet para lidar com conteúdos considerados infratores de direitos autorais, difamatórios, ofensivos, ou de outra forma em violação aos termos de serviço da plataforma. Após receber uma notificação de violação, o provedor de serviço realiza uma análise criteriosa para validar a alegação, comparando o conteúdo à luz dos termos da plataforma. Se a alegação é confirmada, o provedor remove ou restringe o acesso ao conteúdo. Esse sistema, embora eficaz, suscita debates sobre possíveis abusos e a necessidade de equilibrar a remoção de conteúdo prejudicial com a preservação da liberdade de expressão *online*.

Essa abordagem abrangente do Marco Civil da Internet é essencial para enfrentar os desafios decorrentes do uso crescente de tecnologias de manipulação de mídia digital, como o *deepfake*, que podem ser utilizadas para prejudicar a privacidade e a reputação das pessoas. No entanto, a aplicação precisa dessas disposições legais em casos específicos ainda requer análise jurídica aprofundada, levando em consideração a jurisprudência e as circunstâncias individuais de cada caso.

2.3 REPARAÇÃO PELOS DANOS DECORRENTES DE *DEEPFAKE*

À luz da abordagem exauriente realizada nos tópicos anteriores, foi possível se observar a configuração dos elementos da responsabilidade civil em diversos exemplos – sejam eles verídicos ou hipotéticos – de manipulação do meio digital pelo uso do *deepfake*. Logo, há que se falar numa devida reparação, por meio da indenização.

A despeito desse instituto, insta fazer referência à pertinente ponderação doutrinária: "se a responsabilidade é a necessidade de reparar um dano, como já analisado, a indenização é o ressarcimento do prejuízo, recompondo o patrimônio do lesado, tornando-o indene da situação lesiva por ele experimentada". (AZEVEDO, 2019, p. 378).

É claro que nem todos os casos de *deepfake* admitem uma reparação, até mesmo porque, não há diploma legal no ordenamento jurídico brasileiro – até o momento – que preveja a criação do *deepfake*, propriamente dita, como um ato antijurídico. Com efeito, a reparação será cabível, na prática, quando a divulgação do *deepfake* provocar dano a algum direito da personalidade, de modo a preencher os pressupostos da responsabilidade civil.

Não obstante, em se tratando de reparação pelos danos decorrentes de *deepfake*, é necessário pontuar que a sua satisfação pode ser uma tarefa árdua e nem sempre eficaz. Isso se deve, sobretudo, às características intrínsecas ao ambiente digital e à própria natureza do *deepfake*.

2.3.1 Limitações da reparação no cenário prático

Uma das principais dificuldades inerentes à reparação pelos danos decorrentes de *deepfake* reside na capacidade de identificar e responsabilizar os criadores daquele conteúdo

manipulado. A anonimização é comum nesse contexto, e os agentes da conduta culposa muitas vezes conseguem ocultar sua identidade com facilidade, tornando a responsabilização um desafio significativo.

Ademais, o uso de servidores e plataformas *online* que transcendem fronteiras torna a jurisdição complexa e, em muitos casos, ineficaz. Dessa forma, a dinâmica da internet e das redes sociais torna o rastreamento e controle do conteúdo de *deepfake* um desafio constante, uma vez que a criação e disseminação dessas mídias são muitas vezes descentralizadas e altamente flexíveis.

Além disso, um fator relevante que limita a reparação é a velocidade de propagação do conteúdo de *deepfake*. Uma vez que um *deepfake* é compartilhado, ele pode se espalhar rapidamente por várias plataformas e comunidades *online*. Mesmo que o conteúdo seja removido de uma fonte, ele pode já ter sido amplamente distribuído e replicado, o que torna a remoção da mídia manipulada incompleta e muitas vezes insuficiente.

Outra limitação a ser considerada é que a retirada do conteúdo do ar não impede a possibilidade de disseminação *offline*. Uma vez que o conteúdo de *deepfake* tenha sido criado e compartilhado *online*, ele pode ser salvo, baixado e redistribuído de outras formas, tornando difícil controlar completamente sua disseminação.

Somado a isso, ainda que fosse possível remover completamente determinado *deepfake* do ambiente digital, é necessário considerar que a complexidade da reparação é ainda mais acentuada pelo fato de que o *deepfake* pode causar danos à reputação e à privacidade das vítimas de maneira duradoura. Nesse sentido, mesmo que o conteúdo fosse apagado e não mais oferecesse qualquer tipo de dano, os impactos psicológico e emocional das vítimas poderão perdurar por um longo e indeterminado período.

2.3.2 Liquidação do dano

Considerando que a indenização predispõe a finalidade de restaurar – na medida do possível – a vítima ao seu estado anterior, sua liquidação deve incluir a totalidade do dano realmente sofrido, bem como os lucros que deixaram de ser auferidos, isto é, os lucros cessantes. O grau de culpa do agente não afetará a determinação do valor dos danos. Mesmo

que a sua culpa seja mínima, ele será responsável pelo dano causado à vítima em toda a sua extensão. (GONÇALVES, 2019).

Na visão da doutrina clássica:

> A maior ou menor gravidade da falta não influi sobre a indenização, a qual só se medirá pela extensão do dano causado. A lei não olha para o causador do prejuízo, a fim de medir-lhe o grau de culpa, e sim para o dano, a fim de avaliar-lhe a extensão. A classificação da infração pode influir no sentido de atribuir-se ou não responsabilidade ao autor do dano, o que é diferente. (ALVIM, 1980, p. 197).

Com efeito, o Código Civil de 2002, por meio do seu artigo 944, caput e parágrafo único, conservou a interpretação doutrinária no que tange ao grau de culpa não interferir na liquidação do dano, veja-se, respectivamente: “a indenização mede-se pela extensão do dano. […] se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização”. (BRASIL, 2002).

Dessa forma, destaca-se a possibilidade de a reparação do dano se aperfeiçoar sob duas modalidades: a reparação específica, na qual se pretende restabelecer o *statu quo ante*; e a reparação por equivalente em dinheiro, geralmente verificada na impossibilidade de devolver a vítima ao estado em que se encontrava.

Quanto à primeira modalidade, a ideia por trás da restauração da situação anterior à ocorrência do dano, implica na tomada de medidas, pelo agente causador do dano, que visem à restituição à vítima daquilo que fora perdido. Já em relação a segunda, a inviabilidade prática ou suficiente da primeira, lhe dá causa. Por seu turno, o valor da compensação financeira é calculado com base nos danos efetivamente sofridos pela vítima, incluindo prejuízos materiais e, em alguns casos, danos morais.

No caso de reparação de prejuízos derivados de *deepfake*, é importante salientar que o dano pode estar vinculado ao aspecto material, mas, necessariamente está, em relação ao aspecto moral, considerando a hipótese de dano ao direito à imagem provocado pelo uso não autorizado dessa.

É certo que em casos de dano material derivado do *deepfake* a indenização por reparação específica não seria a modalidade mais adequada, tendo em vista que os prejuízos materiais ocasionados pelo *deepfake* geralmente estão relacionados à teoria da perda de uma chance. Sob esse aspecto, a aplicação da reparação específica provavelmente seria inviável, pois demandaria que o agente gerasse um cenário em que a chance perdida se tornasse uma nova oportunidade à vítima.

Por essa razão, seria mais comum a aplicação da reparação por equivalente em dinheiro, posto que, nos casos de dano material decorrente de *deepfake*, que geralmente estão associados à teoria da perda de uma chance, a indenização poderia ser calculada com base na probabilidade de sucesso da chance e nos danos efetivos causados pela perda.

Já nas situações em que a utilização do *deepfake* implicou em dano moral, a reparação específica encontra vez de maneira excepcional. Isso porque, mesmo que não se alcançasse a reconstituição natural anterior, ainda seria possível que o agente do dano promovesse uma atitude de retratação da conduta culposa, esclarecendo publicamente, por exemplo, que o conteúdo divulgado se tratava de mídia manipulada, tal como quando um jornal publica um desagravo. (DINIZ, 2019). Desse modo, atingir-se-ia uma “situação material correspondente”. (CUPIS, 1979, p. 305).

Conquanto exista essa exceção, cumpre salientar que nos demais casos de dano moral derivado da manipulação do meio digital pelo *deepfake*, torna-se mais habitual a utilização da reparação por equivalente em dinheiro. Afinal, a depender das peculiaridades do caso concreto, o impacto na esfera psicológica da vítima pode provocar traumas severos e, por consequência, uma maior dificuldade para se retornar ao *statu quo ante*.

2.3.3 Técnicas de detecção

As técnicas de detecção de *deepfake* representam uma parte significativa da resposta à ameaça potencial que esses conteúdos manipulados podem ocasionar. Nesse sentido, a adoção de medidas no âmbito subjetivo é necessária para prevenir as pessoas de se tornarem vítimas da manipulação do meio do digital.

Uma das estratégias de detecção de *deepfake* envolve a análise atenta aos elementos digitais daquela mídia, haja vista que, até o momento, nem todo trabalho de *deepfake* é completamente verossímil. Com um olhar meticuloso, é possível identificar imperfeições visuais, como distorções, sobreposições irregulares, reflexo irregular da luz no rosto criado digitalmente, além de outras discrepâncias que apontam que aquele conteúdo de imagem ou vídeo não foi capturado naturalmente.

A despeito desse ponto, torna-se relevante a abordagem do fenômeno do "*Uncanny Valley*" – ou, Vale da Estranheza, na tradução livre. Essa concepção destaca a importância de atenção aos detalhes quando se trata da autenticidade de uma representação humana, seja em um *deepfake* ou em qualquer outra forma de simulação.

A ideia principal por trás desse conceito é que, à medida que uma representação de um ser humano se torna mais realista, nosso grau de empatia e aceitação tende a aumentar, até que algo no realismo falha, e a aceitação despenca abruptamente, criando um "vale" na curva de aceitação.

É isso o que explica a sensação de desconforto ao se identificar algo que está fora da normalidade em uma representação digital do ser humano, a exemplo de robôs interativos e assistentes virtuais que acabam se tornando perturbadores ao buscarem a máxima semelhança ao comportamento humano.

Assim, a conscientização das potenciais vítimas sobre o "*Uncanny Valley*" pode ser uma ferramenta valiosa para a prevenção e identificação de *deepfakes* enganosos, notadamente, em razão de sua compreensão oferecer às pessoas um olhar mais crítico ao se estar diante de imagens, áudios e vídeos que possam parecer suspeitos, tornando-as mais vigilantes e críticas em relação ao conteúdo que consomem *online*.

Ademais, também deve ser destacada a técnica de verificação das fontes como uma estratégia fundamental para a detecção de *deepfake*. Essa abordagem se baseia no princípio de que a autenticidade de uma informação ou mídia pode ser confirmada por meio da validação de sua origem, promovendo, em última análise, a integridade da informação e a prevenção da propagação de conteúdo falso.

Conforme anteriormente visto, os *deepfakes* frequentemente exploram situações sensíveis ou polêmicas, como discursos políticos, notícias de última hora, ou declarações provocativas. Logo, a verificação da fonte atua como um filtro crítico na identificação de conteúdo manipulado, contribuindo para a proteção da integridade da informação, o combate à desinformação e a preservação da confiança do público em um ambiente digital repleto de desafios relacionados à autenticidade e à veracidade das informações.

De igual modo, as assinaturas digitais desempenham um papel crucial na detecção de *deepfakes* e na verificação da autenticidade de conteúdo digital. Embora não sejam uma técnica de detecção por si só, as assinaturas digitais podem servir como uma camada adicional de segurança e validação para ajudar a confirmar a autenticidade de mídias digitais, o que é especialmente relevante na era dos *deepfakes*.

Uma assinatura digital é uma forma de autenticação que garante a integridade e a origem de um documento ou arquivo digital. Ela envolve a aplicação de algoritmos de criptografia para criar um selo digital exclusivo que está vinculado ao conteúdo e ao criador. Quando uma assinatura digital é anexada a um arquivo, ela atua como um selo de autenticidade, garantindo que o conteúdo não tenha sido alterado desde a sua assinatura e que o criador seja quem ele alega ser.

As técnicas apresentadas estão inexoravelmente vinculadas a uma educação digital, o que, ao fim e ao cabo, representa o meio eficaz para capacitar o grande público a desenvolver habilidades críticas de avaliação e identificação do conteúdo digital manipulado. Em um ambiente digital repleto de desafios relacionados à autenticidade e à veracidade das informações, a educação é uma técnica vital para combater a disseminação de *deepfakes* prejudiciais e fortalecer a resiliência contra essa forma de desinformação.

Promover a alfabetização digital e a conscientização sobre os riscos associados ao uso de *deepfakes* é fundamental, pois permite que as pessoas possam discernir entre o real e o fabricado, no contexto de mundo digital em constante transformação. Nesse sentido, a colaboração entre instituições educacionais, governos e organizações da sociedade civil desempenha um papel crucial na promoção da educação e na construção de uma sociedade mais capaz de enfrentar os desafios da era digital.

CONCLUSÃO

A crescente manipulação do meio digital pelo uso de *deepfake* representa um enorme desafio para a proteção dos direitos da personalidade no cenário cibernético. Nesse sentido, a presente monografia teve como proposta analisar os impactos do fenômeno nos direitos personalíssimos bem como o entendimento da doutrina acerca do enfrentamento jurídico da questão, seja por meio do projeto de lei que vise à regulamentação do *deepfake*, seja por meio do estudo acerca da incidência da responsabilidade civil nos casos concretos.

Desse modo, em que pese se admitir situações de uso consentido do *deepfake*, as hipóteses de uso não consentido do *deepfake*, que acabam sendo a grande maioria dos casos, estão mais propensas a se perdurarem no meio social e ensejarem consequências nocivas aos indivíduos, sobretudo mediante a facilidade e acessibilidade das ferramentas de manipulação do meio digital.

Diante desse cenário, os resultados da pesquisa apontam para a imprescindibilidade de uma regulamentação da utilização do *deepfake* pelo Poder Legislativo federal. Ainda que incipiente o Projeto de Lei de regulamentação do uso do *deepfake*, no contexto brasileiro, é relevante compreender que a incrementação a esse projeto precederá de um diálogo em conjunto com a sociedade, para fins de dar notoriedade à sociedade – sobretudo às classes mais vulneráveis às novas tecnologias como um todo – a respeito do uso do *deepfake* e dos riscos envolvidos.

Com efeito, o diálogo popular além de dar ciência sobre os impactos do *deepfake*, também balizará os objetivos de sua regulamentação, de modo que serão trazidos os pontos controvertidos do ordenamento jurídico para debate democrático.

Outrossim, verificou-se que a responsabilidade civil vem se apresentando de maneira muito sólida nos casos de *deepfake*. Dessa forma, a observação do preenchimento dos pressupostos da responsabilidade civil não tem suscitado quaisquer dúvidas por parte da doutrina, sendo que as hipóteses de responsabilização dos provedores de aplicação e dos usuários que compartilham o *deepfake*, de igual forma, também restam muito bem delimitadas.

Por último, há que se considerar a existência de limitações para reparação dos danos decorrentes de *deepfake*, as quais são verificadas na prática, muito em razão da falta de regulamentação das relações sociais no meio digital, sobretudo em hipóteses de *deepfake*.

Diante de todo o exposto, conclui-se que ainda persistem muitos desafios relativos aos casos de violação dos direitos da personalidade pela manipulação do meio digital com o uso de *deepfake*. Contudo, tais dificuldades podem ser amenizadas por meio de políticas de educação digital, uma regulamentação sólida e eficaz, bem como por uma reparação compatível aos danos experimentados pela vítima; os quais, em última análise, propiciarão um uso mais consciente dessa ferramenta tecnológica e coibirão as finalidades abusivas que afrontam os direitos personalíssimos e, em última análise, o próprio Estado de Direito.

Afinal, são inúmeras as possibilidades de uso do *deepfake* que proporcionam efeitos positivos à sociedade, de modo que não se afigura razoável sobrepor a conotação negativa dessa tecnologia em detrimento dessas potencialidades benéficas. Assim, é crucial que se estimule uma criatividade ética e responsável, o que viabilizará o avanço dessa tecnologia em consonância com princípios que resguardem os direitos individuais e, inclusive, os coletivos.

REFERÊNCIAS

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

ALECRIM, Emerson. Bruce willis pode voltar a atuar graças a uma tecnologia de deepfake. *In:* **Tecnoblog**, 30 set. 2022. Disponível em: <https://tecnoblog.net/noticias/2022/09/30/bruce-willis-pode-voltar-a-atuar-gracas-a-uma-tecnologia-de-deepfake/>. Data de acesso: 22 nov. 2023.

ALVIM, Agostinho Neves de Arruda. **Da inexecução das obrigações e suas conseqüências**. 5. ed. São Paulo: Saraiva, 1980. p. 197.

AZEVEDO, Álvaro Villaça. **Curso de direito civil: teoria geral das obrigações e responsabilidade civil**. 13. ed. São Paulo: Saraiva Educação, 2019. p. 378.

BESCHIZZA, Rob. Rowan atkinson deepfaked into the j'adore ad. *In:* **Boing Boing**, 12 dez. 2019. Disponível em: < https://boingboing.net/2019/12/12/rowan-atkinson-deepfaked-into.html>. Data de acesso: 20 nov. 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 11 dez. 2022.

BRASIL. **Lei nº 8.078, de 23 de abril de 2014**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 12 dez. 2022.

BRASIL. **Lei nº 9.610, de 20 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l9610.htm>. Acesso em: 14 set. 2023.

BRASIL, **Lei nº 10.406**, de 10 de janeiro de 2022. Institui o Código Civil. Brasília, DF: Senado, 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 04. dez. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 04 dez. 2022.

BRASIL, **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 03 fev. 2023.

BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Especial 86.109/SP**. Responsabilidade civil. Uso indevido da imagem. Divulgação, em revista de expressiva circulação, de propaganda comercial contendo as fotos do conhecido casal 'lampião' e 'maria bonita'. Falta de autorização finalidade comercial. Reparação devida.- A utilização da imagem da pessoa, com fins econômicos, sem a sua autorização ou do sucessor, constitui locupletamento indevido, a ensejar a devida reparação. - Não demonstração pelo recorrente de que a foto caiu no domínio público, de acordo com as regras insertas no art. 42 e seus parágrafos da Lei nº 5.988, de 14.12.73. - Improcedência da denunciação da lide à falta do direito de regresso contra a litisdenunciada. Recurso especial não conhecido. Recorrente: Lloyds Bank PLC. Recorrida: Expedita Ferreira Nunes. Relator: Ministro Barros Monteiro, 28 de junho de 2001. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=MON&sequencial=226879&tipo_documento=documento&num_registro=199600033889&data=20020222&formato=PDF>. Acesso em: 20 dez. 2022.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 10. ed. São Paulo: Atlas, 2012. p. 02.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Violação dos direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros. **Civilistica.com**. Rio de Janeiro, a. 8, n. 1, p. 10, 2019. Disponível em: <http://civilistica.com/violacao-dos-direitos-de-personalidade/>. Data de acesso: 30 nov. 2022.

CUNHA, Rodrigo Santos. Projeto de lei do Senado nº 3.592, de 2023. Estabelece diretrizes para o uso de imagens e áudios de pessoas falecidas por meio de inteligência artificial (IA), com o intuito de preservar a dignidade, a privacidade e os direitos dos indivíduos mesmo após sua morte. Brasília, DF: Senado Federal, 2023. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9412197&ts=1698248946824&disposition=inline&_gl=1*4dru8c*_ga*MTkzMzU2MTI5OS4xNjk4MDM5NjMw*_ga_CW3ZH25XMK*MTcwMDYzNDg2MS43LjAuMTcwMDYzNDg2MS4wLjAuMA..>. Acesso em: 20 nov. 2023.

CUPIS, Adriano de. **Os direitos da personalidade**. Tradução de Adriano Vera Jardim e Antonio Miguel Caeiro. Lisboa: Livraria Morais, 1961. p. 135

CUPIS, Adriano de. **Il dano – teoria general della responsabilità civile**. 3. ed. Milão: Giuffre, 1979. p. 305.

DOFFMAN, Zak. Aplicativo chinês que coloca rosto em vídeos deixa milhões em risco. *In:* **Forbes**, 03 set. 2019. Disponível em: <https://forbes.com.br/colunas/2019/09/aplicativo-chines-de-que-coloca-rosto-em-videos-poe-milhoes-em-risco/>. Data de acesso: 21 mai. 2022.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. 29. ed. São Paulo: Saraiva, 2019. v. 1: Teoria geral do direito civil, p. 132-133.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. 25. ed. São Paulo: Saraiva, 2011. v. 7: Responsabilidade civil, p. 126.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de direito civil**. 14. ed. Salvador: JusPodvim, 2016. v. 1: Parte geral e LINDB, p. 210.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**. 17. ed. São Paulo: Saraiva Educação, 2019. v. 3: Responsabilidade civil, p. 24-26.

GOMES, Orlando. **Introdução ao direito civil**. 21. ed. rev. e atual. Rio de Janeiro: Forense, 2016. p 118-119.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro: responsabilidade civil**. 7. ed. São Paulo: Saraiva Educação, 2019. v. 4: Responsabilidade civil.

GUEDES, Gisela Sampaio da Cruz. **O problema do nexo causal na responsabilidade civil**. 1. ed. Rio de Janeiro: Renovar, 2005. p. 159.

GUERRA, Sidney Cesar Silva. O direito à privacidade e a internet. *In*: SILVA JÚNIOR, Roberto Roland Rodrigues da (coord.). **Internet e Direito Reflexões Doutrinárias**. 1 ed. Rio de Janeiro: Lumen Juris, 2001. p. 115-132.

HESSEL, Marcelo. The irishman | robert de niro vai rejuvenescer 40 anos no filme de martin scorsese. *In:* **Omelete**, [São Paulo], 20 dez. 2016. Disponível em: < https://www.omelete.com.br/filmes/the-irishman-robert-de-niro-vai-rejuvenescer-40-anos-no-filme-de-martin-scorsese>. Data de acesso: 22 nov. 2023.

ITFORUM. **2019: o ano do avanço do deepfake; relembre episódios que marcaram**. 31 dez. 2019. Disponível em: <https://itforum.com.br/noticias/2019-o-ano-do-avanco-do-deepfake-relembre-episodios-que-marcaram/>. Acesso em: 17 dez. 2022.

KONDER, Carlos Nelson de Paula. O alcance do direito à identidade pessoal no direito civil brasileiro. **Pensar**. Fortaleza, v. 23, n. 1, p. 1-11, jan./mar. 2018. Disponível em: <https://ojs.unifor.br/rpen/article/view/7497/>. Data de acesso: 03 dez. 2022.

LEAL, Livia Teixeira; SIQUEIRA, Mariana Ribeiro. Responsabilidade civil pelo compartilhamento de mensagens pelo whatsapp. *In*: SCHREIBER, Anderson; MORAES, Bruno Terra de; TEFFÉ, Chiara Spadaccini de (coords.). **Direito e mídia: tecnologia e liberdade de expressão**. Indaiatuba: Foco, 2020. p. 121.

LEE, Dami. Deepfake salvador dalí takes selfies with museum visitors. *In:* **The Verge**, 10 mai. 2019. Disponível em: <https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum>. Data de acesso: 22 nov. 2023.

LONGHI, João Victor Rozatti. **Responsabilidade civil por danos à pessoa humana oriundos do uso de perfis falsos em sites de redes sociais**. Orientador: Guilherme Calmon Nogueira da Gama. 2011. Dissertação (Mestrado em Transformações do direito privado, estado e sociedade) – Programa de Pós-graduação em Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2011.

LOUBAK, Ana Letícia. Aplicativo zao usa deepfake para criar vídeos e viraliza na china. *In:* **Techtudo**, 03 nov. 2019. Disponível em:

<https://www.techtudo.com.br/noticias/2019/09/aplicativo-zao-usa-deepfake-para-criar-videos-e-viraliza-na-china.ghtml>. Data de acesso: 21 mai. 2022.

LOUREIRO, Henrique Vergueiro. **Direito à imagem**. Dissertação (Mestrado) – Pontifícia Universidade Católica de São Paulo – PUC/SP, São Paulo, 2005. p. 80.

METZ, Rachel. Deepfakes estão tentando mudar o curso da guerra na Ucrânia. *In:* **CNN**, 25 mar. 2022. Disponível em: < https://www.cnnbrasil.com.br/tecnologia/deepfakes-estao-tentando-mudar-o-curso-da-guerra-na-ucrania/>. Acesso em: 02 dez. 2022.

MORAES, Maria Celina Bodin de. **Danos à pessoa humana**. Uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara Antonia Spadaccini de. Redes sociais virtuais: privacidade e responsabilidade civil análise a partir do Marco Civil da Internet. **Pensar**. Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017. Disponível em: <https://ojs.unifor.br/rpen/article/view/6272/>. Data de acesso: 03 dez. 2022.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil**. 26. ed. Rio de Janeiro: Forense, 2018. v. 4: Direitos reais, p 202.

PIMENTEL, Alexandre Freire. Clone virtual: uso da imagem de pessoa falecida por algoritmos de ia. *In:* **Consultor Jurídico**. Disponível em: <https://www.conjur.com.br/2023-ago-01/alexandre-pimentel-uso-imagem-falecido-ia/>. Acesso em: 22 set. 2023.

PLACIDO, Dani di. James dean and the rise of 'deep fake' hollywood. *In:* **Forbes**, 08 nov. 2019. Disponível em: <https://www.forbes.com/sites/danidiplacido/2019/11/08/james-dean-and-the-rise-of-deep-fake-hollywood/?sh=404ceaf46953>. Data de acesso: 22 nov. 2023.

QUEIROZ, João Quinelato de. **A responsabilidade civil dos provedores de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros: estudo na perspectiva civil-constitucional**. Orientadora: Maria Celina Bodin de Moraes. 2018. Dissertação (Mestrado em Pensamento jurídico e relações sociais) – Programa de Pós-graduação em Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

RIBEIRO, Iara Pereira. Imagem e julgamento de frinéia: a compreensão do conceito jurídico de imagem por meio da análise de um poema. **Rev. de Direito, Arte e Literatura**. Salvador, v. 4, n. 1, p. 1-8, jan./jun. 2018. Disponível em: <https://www.indexlaw.org/index.php/revistadireitoarteliteratura/article/view/4201/>. Data de acesso: 27 nov. 2022.

RODRIGUES JÚNIOR, Otávio Luiz. Responsabilidade civil e Internet: problemas de qualificação e classificação de conflitos nas redes sociais. *In*: ANDRIGHI, F. Nancy (coord.). **Responsabilidade civil e inadimplemento no direito brasileiro**. São Paulo: Atlas, 2014.

SCHREIBER, Anderson. **Direito da personalidade**. 3. ed. São Paulo: Atlas, 2014. p. 137-214.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil: a erosão dos filtros da reparação à diluição dos danos**. 2. ed. São Paulo: Atlas, 2009. p. 81.

SCHREIBER, Anderson; RIBAS, Felipe; MANSUR, Rafael. Deepfakes: regulação e responsabilidade civil. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org.). **O direito civil na era da inteligência artificial**. 1 ed. São Paulo: Thomson Reuters, 2020. p. 609-626.

SPLASH. **Por que comercial da Volks com Elis levantou debate sobre a ditadura**. São Paulo, 04 jul. 2023. Disponível em: <https://www.uol.com.br/splash/noticias/2023/07/04/musica-em-comercial-com-elis-foi-composta-na-ditadura-apoiada-pela-volks.htm>. Acesso em: 13 nov. 2023.

TARTUCE, Flávio. **Direito civil: lei de introdução e parte geral**. 15. ed. Rio de Janeiro: Forense, 2019. v. 1. p. 264-315.

TEFFÉ, Chiara Antonia Spadaccini de. Considerações sobre a proteção do direito à imagem na internet. **Revista de Informação Legislativa**: RIL, v. 54, n. 213, p. 173-198, jan./mar. 2017. Disponível em: <http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p173>. Data de acesso: 02 dez. 2022.

TELLES JÚNIOR, Goffredo da Silva. Direito subjetivo. *In*: FRANÇA, Rubens Limongi (coord.). **Enciclopédia saraiva do direito**. São Paulo: Saraiva, 1977. v. 28. p. 315-316.

TEPEDINO, Gustavo; OLIVA, Milena Donato. **Fundamentos do direito civil**. 4. ed. Rio de Janeiro: Forense, 2023. v. 1: Teoria geral do direito civil. p. 165-180.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil**. 4. ed. Rio de Janeiro: Forense, 2023. v. 4: Responsabilidade civil. p. 04-08.

TI INSIDE. **Mrbeast, maior youtuber do mundo é usado em golpes com deep fake**. 05 out. 2023. Disponível em: < https://tiinside.com.br/05/10/2023/mrbeast-maior-youtuber-do-mundo-e-usado-em-golpes-com-deep-fake/>. Acesso em: 13 nov. 2023.

TORRES, Bolíviar; BARROS, Luisa. Vídeo da mona lisa 'falante' esconde uma nova ameaça: as 'deepfakes'. *In:* **O Globo**, 01 jun. 2019. Disponível em: <https://oglobo.globo.com/cultura/video-da-mona-lisa-falante-esconde-uma-nova-ameaca-as-deepfakes-23710483>. Data de acesso: 22 nov. 2023.

VAINZOF, Rony. Da responsabilidade por danos decorrentes de conteúdos gerados por terceiros. *In* MASSO, F. del; ABRUSIO, J.; FLORÊNCIO FILHO, Marco A. (Coord.). **Marco Civil da Internet**: Lei 12.965/2014. São Paulo: RT, 2014. p. 177-205.

VENDRUSCOLO, Stephanie. Volkswagen assina acordo milionário de reparação por colaborar com ditadura e abre precedente histórico. *In:* **El país**, 24 set. 2020. Disponível em: <https://brasil.elpais.com/brasil/2020-09-24/volkswagen-assina-acordo-milionario-de-reparacao-por-colaborar-com-ditadura-e-abre-precedente-historico.html>. Data de acesso: 14 nov. 2023.

VOLK, Pete. Tom hanks is getting de-aged with deepfake ai for new movie. *In:* **Polygon**, 31 jan. 2023. Disponível em: < https://www.polygon.com/23579566/tom-hanks-ai-movie-de-aged-robert-zemeckis>. Data de acesso: 22 nov. 2023.