ISSN 1809-1628
REVISTA MULTIDISCIPLINAR
HUMANIDADES E TECNOLOGIAS (FINOM)
FACULDADE DO NOROESTE DE MINAS

O uso do Deep Fake e a violação às garantias do estado democrático de direito

The use of Deep Fake and the violation of guarantees of the democratic state of law

Anna Beatriz Hashioka*
Ana Beatriz da Silva**
Patrícia Borba Marchetto***

Resumo: Com a expansão da nova Era Digital, inúmeras questões sociais emergiram e, com elas, a necessidade de proteção do Estado democrático de direito. Dentro desse contexto, os *deep fakes* ganharam destaque, pois, além de se enquadrarem como uma forma de evolução das *fake news*, são um mecanismo de inteligência artificial capaz de manipular imagens e outros recursos. Diante disso, faz-se necessário levantar questionamentos sobre quais os possíveis impactos dessa tecnologia no Estado democrático, bem como entender como essa questão se encontra sendo tutelada pelo direito. Partindo dessas premissas, através do método dedutivo, realizou-se uma pesquisa exploratória, com a revisão bibliográfica de artigos científicos e livros pertinentes à temática. Ao final, conclui-se que essa prática pode colocar em risco os ideais estabelecidos pelo Estado democrático, de modo que, a regulamentação do *deep fake* é algo de interesse público e também privado.

Palavras-chave*: Deepfake*. Estado Democrático de Direito. Inteligência Artificial.

Abstract: As the new Digital Age expands, countless social issues have emerged and, with them, the need to protect the democratic rule of law. Within this context, deep fakes have become more prominent because, in addition to being a form of evolution of fake news, it is an

* Graduanda em Direito pela Universidade Estadual Paulista (UNESP), Faculdade de Ciências Humanas e Sociais (FCHS) e bolsista pelo Programa Institucional de Bolsas de Iniciação Científica da UNESP/CNPQ, ORCID: https://orcid.org/0009-0002-4362-588X, e-mail: beatriz.hashioka@unesp.br

** Graduanda em Direito pela Universidade Estadual Paulista (UNESP), Faculdade de Ciências Humanas e Sociais (FCHS) e bolsista pelo Programa Institucional de Bolsas de Iniciação Científica da UNESP/REITORIA, ORCID: https://orcid.org/0009-0004-0925-9278, e-mail: aanabeatrizdasilva1@gmail.com

*** Realizou estágio pós-doutoral em Genética Forense na Faculdade de Ciências Farmacêuticas de Araraquara (FCF/UNESP). Doutora em Direito pela Universidad de Barcelona (2001), com título reconhecido pela Faculdade de Direito da USP. Professora na graduação e pós-graduação da UNESP, ORCID: https://orcid.org/0000-0002-7507-961X, e-mail: patricia.marchetto@unesp.br

Recebido em 14//04/2025
Aprovado em: 03/09/2025

Sistema de Avaliação: *Double Blind Review*

OPEN ACCESS

artificial intelligence mechanism capable of manipulating images and other resources. Given this, it is necessary to raise questions about the possible impacts of this technology on the democratic state, as well as to understand how this issue is being protected by the law. Based on these premises, using the deductive method, exploratory research was carried out, with a bibliographical review of scientific articles and books pertinent to the subject. In the end, it was concluded that this practice could jeopardize the ideals established by the democratic state, so the regulation of deep fakes is something of both public and private interest.

Keywords: Artificial intelligence. Deepfake. Democratic Rule of Law.

1 Introdução

O surgimento de novas tecnologias tem sido acompanhado de novos dilemas éticos, morais e legais, os quais abrem margem para inúmeras discussões, principalmente, em relação ao avanço da inteligência artificial (IA). Nesse sentido, um dos aspectos que ganha destaque se refere ao impacto que a IA, em específico o *deep fake*, pode ter no Estado Democrático de Direito, bem como as formas com que o direito pode tutelar essa prática.

Sob esse prisma, para melhor compreender essa problemática, é necessário antes reconhecer que a comunicação e o discurso exercem um papel fundamental nesse cenário. Isso ocorre pois estes são elementos essenciais para o funcionamento de uma democracia. Contudo, com a disseminação do uso da *internet*, houve uma alteração em relação aos modelos tradicionais de comunicação, de modo que, as redes sociais passaram a ser destaque para a comunicação interpessoal.

Esse novo ambiente, o qual é composto por algoritmos que fornecem aos usuários as informações que atendem a seu perfil, se tornou também ideal para a disseminação de notícias falsas, ou *fake news*. De uma maneira similar, foi o desenvolvimento da IA que tornou possível o surgimento dos *deep fakes*, ou falsidades profundas que podem ser vistas como uma evolução das *fake news*, às quais utilizam elementos imagéticos para transmitir informações inverídicas e muitas vezes colocar pessoas em situações que nunca estiveram.

Em ambos os casos, restou evidente que esse desenvolvimento mudou as formas de comunicação entre indivíduos e, consequentemente trazem o alerta sobre como a sociedade pode ser influenciada. Aprofundando ainda mais, não apenas pessoas podem ser atingidas por esse efeito, mas o cenário democrático e o próprio Estado democrático de direito. Como efeito disso, tem-se observado a criação de um cenário de desconfiança geral nas instituições, nos atores democráticos e na organização estatal.

Diante disso, abarcando especificamente as *deep fakes*, elas chamam ainda mais atenção por permitirem um leque de possibilidade quanto a manipulação da imagem, muitas vezes de

forma negativa e prejudicial, de indivíduos que se encontram em posição importante no cenário político. Ainda, esse uso da IA pode afetar até mesmo no cenário eleitoral ao induzirem eleitores a votarem em determinado candidato em decorrência de conteúdos inverídicos que receberam virtualmente de outros concorrentes.

Como consequência desse contexto, resta evidente o interesse do poder público em regulamentar esse uso da IA, principalmente como uma maneira de assegurar as boas práticas democráticas. Da mesma forma, esse interesse, além de ser público, também pode ser privado, ao buscar-se proteger a honra e a imagem das pessoas particulares atingidas por essa nova tecnologia.

À vista disso, o presente artigo visa apontar quais são os riscos do *deep fake* para o Estado democrático de direito e como essa prática está tutelada pelo direito. Nesse sentido, foi estruturado metodologicamente com base em uma pesquisa exploratória, mediante a qual foi feita a revisão bibliográfica com a leitura de artigos e revistas sobre o tema. Assim, com a utilização do método dedutivo, partiu-se da ideia geral sobre o funcionamento da democracia e aprofundou-se em quais impactos o Estado Democrático de Direito pode ter em decorrência do *deep fake*. Por fim, passou-se a análise o quadro legislativo atual em relação ao tema e como ocorreria eventuais responsabilizações quanto ao uso dessa tecnologia.

2 Democracia, Estado Democrático De Direito E As Novas Formas De Comunicação

De início, Bobbio (*apud* Piovesan e Hernandes, 2023) aponta que a democracia se trata de um conjunto de regras e princípios que determinam quem está autorizado a tomar decisões e através de quais procedimentos isso se daria. Nesse sentido, relacionado com a definição apresentada por Bobbio, Piovesan e Hernandes (2023) indicam que, para que se tenha o funcionamento da democracia, é importante que haja o respeito por estas normas postas, de modo a permitir um melhor desenvolvimento do sistema democrático. Dessa forma:

> Essas são condições sem as quais o jogo democrático não se desenrola. Tais regras são as liberdades públicas (direitos de liberdade, de opinião, de expressão das próprias opiniões, de reunião, de associação, etc.) previstas em normas constitucionais que conformam a base do Estado liberal e do Estado de Direito. Mas o que distingue um regime democrático de um regime não democrático é a previsão e o respeito às regras constitutivas do jogo (Piovesan; Hernandes, 2023, p. 06).

Relacionando a isso, é possível afirmar que a democracia é a base para o Estado Democrático de Direito, composto, em sua essência, pela soberania popular, o respeito às

normas e aos princípios de direitos humanos. Em outras palavras, essa forma de Estado une o modelo democrático com o Estado de Direito – na qual prevalece o império das normas. Logo, "o 'democrático' qualifica o Estado, o que irradia os valores da democracia sobre todos os seus elementos constitutivos e, pois, também, sobre a ordem jurídica." (Silva, 1988, p. 21).

Tendo isso em vista, é evidente que esse modelo de organização política visa estabelecer regras básicas, de modo que se encontra alinhado com os direitos fundamentais, em especial à dignidade da pessoa humana e à liberdade de expressão. Estes elementos são imprescindíveis para o funcionamento do Estado Democrático de Direito, principalmente, por permitirem a livre manifestação de ideias. Portanto, para o bom funcionamento do regime democrático, é necessário a existência de um alinhamento das práticas com as regras.

Sob esse prisma, passando a analisar quanto à perspectiva da comunicação em um sistema de normas postas, a diversidade de meios e formas de comunicação, quando usadas positivamente, podem ser tidas como instrumentos para a disseminação de conhecimento e informação.

Nessa linha, com o avanço das novas tecnologias, bem como a expansão da *internet* e das redes sociais, é possível se verificar uma democratização do acesso à informação e, consequentemente, dos discursos. Esse novo modelo de estruturação da comunicação surge em oposição àquele tradicionalmente estabelecido, no qual apenas um transmissor definia qual seria o conteúdo transmitido ao receptor (Wolkoff, 2021). Diante disso, atualmente, um usuário pode decidir como deseja se informar ao possuir acesso a diversas fontes, com inúmeros pontos de vista.

Contudo, diante da imensidade de opções, os usuários da *internet* tendem a se informar através das plataformas digitais e, muitas vezes, com indivíduos ou perfis que busquem confirmar seu ponto de vista. Nesse contexto, a algoritmização da vida das pessoas exerce um papel de destaque no estabelecimento de impedimentos ao fornecimento de discursos plurais aos indivíduos. Isso porque os algoritmos das plataformas são programados para selecionar conteúdos similares àqueles engajados pelas pessoas.

Assim, quanto mais um usuário consome determinado assunto ou tema, mais ele receberá posts semelhantes, criando uma bolha de viés de confirmação ideológico. Ademais, é importante destacar que esse fenômeno pode ser prejudicial à democracia, tendo em vista que a pluralidade de discursos é um elemento essencial para o funcionamento desse sistema.

À vista disso, essas bolhas são o cenário propício para a disseminação das famosas *fake news*, ou em uma tradução livre, notícias falsas. A razão disso é que essas informações

enganosas geralmente são disseminadas através das redes sociais e impulsionadas pelas bolhas, tendo como objetivo serem "propagadas com a intenção de enganar ou com total desrespeito e desprezo com a verdade (falta de veracidade)." (Piovesan *et al.*, 2023, p. 13). Diante da ausência de respeito pela credibilidade da informação, essas notícias oferecem um grande risco ao Estado Democrático de Direito e às liberdades individuais.

Nesse sentido, a propagação das *fake news* forma um cenário que pode ser catastrófico para o sistema democrático como um todo. Tal constatação ocorre em razão de que, uma vez recebida uma informação, a maioria dos indivíduos tendem a incorporá-las, de modo que é muito difícil reparar o dano. Em outras palavras, as pessoas têm sua percepção de realidade distorcida e a verdade se torna uma questão de opinião, gerando um fenômeno generalizado de desconfiança. Esse cenário abre margem para a ampliação da descrença nas instituições, prejudicando o sistema democrático como um todo.

Além disso, se tratando de um impacto mais profundo no Estado Democrático de Direito, não se pode deixar de ressaltar que a propagação de notícias falsas pode impactar no processo eleitoral. Através da disseminação direcionada de mensagens enganosas sobre determinado candidato, essas notícias podem ser capazes de induzir eleitores a votarem em outra pessoa em razão das informações que receberam.

Na verdade, esse já se mostra como um cenário real. Atento a isso, o Tribunal Superior Eleitoral (TSE) criou o *site* "Fato ou Boato"[1] e, segundo informações divulgadas pelo próprio órgão, no ano de 2022, foram realizados 193 textos com a checagem de publicações falsas. Nessa linha, o Tribunal ainda ressaltou que boa parte dos registros de circulação de notícias falsas se deu por meio de redes sociais. Diante disso, conclui-se que a realidade das *fake news* já se assentou no contexto brasileiro, cabendo ao Estado e à sociedade civil adotarem medidas de combate à desinformação, como a plataforma disponibilizada pelo TSE.

Ademais, é importante ressaltar que no debate quanto aos riscos das *fake news*, muitos indicam a correlação delas com o direito à liberdade de expressão. Contudo, não se pode deixar de apontar que este é um direito fundamental que não é intransponível, de maneira que, ao entrar em conflito com outros ou ainda colocar em risco a ordem democrática, pode ser relativizado. Dessa forma, muitas vezes, essas notícias falsas são propagandas com o intuito de

[1] Essa informação se encontra disponível em: Tribunal Superior Eleitoral. FATO ou Boato publicou quase 200 esclarecimentos contra fake news em 2022. [S. l.], 18 nov. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Novembro/fato-ou-boato-publicou-193-esclarecimentos-contra-fake-news-em-2022. Acesso em: 1 abr. 2025.

Doi 10.5281/zenodo.17068521

disseminar discursos de ódio e não podem ser consideradas como uma manifestação da liberdade de expressão.

Logo, diante desse cenário, a ampliação da disseminação das *fake news*, com o intuito de obter algum tipo de vantagem ou prejudicar alguém, se mostra impulsionado pela nova era digital. Como consequência, é de suma importância o debate quanto aos possíveis efeitos disso, de modo a se buscar preservar o Estado Democrático de Direito.

2.1 O *Deep Fake* e o Estado Democrático De Direito

Diante da nova era tecnológica, o combate a disseminação de informações inverídicas ganha uma nova dimensão ao se depararem com uma versão mais perigosa das *fake news*, o *deep fake*. Esse termo, em uma tradução livre, se refere a "falsidades profundas" e é um mecanismo que se utiliza de inteligência artificial generativa para manipular uma imagem, ou criar um vídeo com base em um conteúdo já existente. Nesse sentido, são, "portanto, ferramentas de engano mais modernas e mais perigosas, capazes de imitar pessoas e simular acontecimentos reais, criando falsidades difíceis de serem detectadas". (Brasil, 2024, p. 06).

Com isso, assim como as *fake news*, os *deep fake* se mostram como um instrumento poderoso, que pode gerar danos ao Estado Democrático de Direito, principalmente, ao também reforçar o descrédito nas instituições em um cenário de desconfiança geral. Entretanto, essa nova tecnologia ganha maior destaque, pois é capaz de gerar um outro tipo de risco: pode ser usado na manipulação da imagem de atores democráticos. Sejam candidatos em época de eleições, sejam ministros do Supremo Tribunal Federal, quaisquer figuras públicas passaram a ser suscetíveis a serem vítimas do emprego do *deep fake* com o intuito de distorcer a realidade. Nesse sentido, ressalta-se que:

> As deepfakes, as quais são utilizadas de forma deliberada para enganar os demais indivíduos com conteúdos falsos com aparência de veracidade, e as ações coordenadas inautênticas são claros elementos desinformação e obviamente não estão protegidos pelo âmbito de proteção da liberdade de expressão, já que não são corolários do livre desenvolvimento da personalidade dos seres humanos, assim como não auxiliam, e sim corroem a liberdade de ideias na esfera pública (Robl Filho, *et al*., 2022, p. 41).

Ademais, esse tipo de mecanismo se tornou possível a partir do desenvolvimento da inteligência artificial (IA); para melhor compreender seus os impactos, é necessário antes analisar os conceitos relacionados a ele. Assim, o termo inteligência artificial pode ser compreendido como a capacidade, atribuída às máquinas, em realizar atividades inerentes aos seres humanos, como o estabelecimento de raciocínio lógico. Apesar dessa definição empírica,

a ideia é se tratar de uma tecnologia que, através do processamento de dados, consegue integrar modelos capazes de realizar tarefas cognitivas, gerando previsões e tomadas de decisões (Russell; Norvig, 2022).

Dentro dessa área se encontra o *machine learning* (ML), um modelo de IA no qual o computador é capaz de aprender e melhorar seu processamento de dados sem ser especificamente programado. Assim, um modelo nestes formatos consegue chegar a resultados e realizar previsões inimagináveis a seus programadores (Russell e Norvig, 2022). Por sua vez, dentro do ML, se encontra o *deep learning* (DPL) – utilizado nos programas de produção de *deep fakes* – que é composto por diversas camadas as quais buscam simular as redes neurais humanas.

Diante da formulação complexa desse sistema, ele permitiu a criação de modelo generativo de IA, o qual utiliza programas capazes de processar grande quantidade de dados, sejam eles categorizados ou não. Nesse sentido, a IA generativa tenta "capturar as características estatísticas subjacentes dos dados para gerar novos exemplos que se assemelham aos dados reais." (ANPD, 2024, p. 11). Logo, é por meio do uso dessa categoria de inteligência artificial que os *deep fakes* são formulados.

Ressalta-se ainda que, o objetivo central desses modelos é o aperfeiçoamento, de forma que utilizam os dados gerados para a comparação com os dados reais, no intuito de cada vez mais se tornar difícil identificar a distinção entre ambos. Em razão disso, muito em breve, não será possível constatar se determinada imagem/produção é verídica ou oriunda de *deep fake*. Ante esta constatação, surge o debate quanto aos impactos que essa tecnologia pode gerar ao Estado Democrático de Direito, bem como ao direito à imagem de figuras públicas atuantes no "jogo da democracia".

A exemplo disso, é possível mencionar o caso apontado em uma reportagem da BBC News Brasil [2], em que, ao longo do primeiro ano da invasão russa à Ucrânia, circularam diversos vídeos usando *deep fake*. Os vídeos falsos apresentavam imagens dos presidentes da Rússia Vladimir Putin e da Ucrânia Volodymyr Zelensky, dizendo coisas que nunca disseram. Apesar disso, a reportagem menciona que era evidente que os vídeos se tratavam de montagens. Contudo, a disseminação de tal conteúdo ressalta o alerta do quanto a IA pode ser utilizada para influenciar o cenário político global.

[2] Essa informação se encontra disponível em: WAKEFIELD, Jane. Guerra na Ucrânia: os 'presidentes deepfake 'usados na propaganda do conflito. BBC NEWS BRASIL, [S. l.], 18 mar. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60791955. Acesso em: 1 abr. 2025.

Doi 10.5281/zenodo.17068521

Trazendo para o cenário brasileiro, já ocorreram casos de terceiros espalhando vídeos do Presidente Luiz Inácio Lula da Silva[3], divulgado informações inverídicas e ainda induzindo pessoas a apresentarem dados pessoais. Em ambos os casos, é evidente a possibilidade que essa nova tecnologia tem de afetar não apenas o interesse público, mas também a imagem dos envolvidos e, como consequência disso, seus direitos pessoais. Da mesma forma, o modo com que a sociedade civil, como um todo, se encontra exposta e em risco por essas produções é algo que chama atenção negativamente.

Sob esse prisma, ao retomar os conceitos de democracia e Estado Democrático de Direito anteriormente expostos, é possível constatar que aqueles que utilizam dos *deep fakes* como meio de obter vantagem, seja política ou econômica, estão claramente desrespeitando as "regras do jogo". Assim, levando em consideração o modelo de organização do Estado brasileiro, é papel deste assegurar os direitos e garantias de todos os indivíduos. Desse modo, tendo em vista os riscos que as *fake news* e, em específico, o *deep fake* podem oferecer à sociedade, é de interesse estatal sua regulação e responsabilização daqueles que o empregam com má-fé.

2. 2 A Tutela do Direito na Prática de *Deep Fake*

A fim de preservar as garantias tidas no Estado Democrático de Direito, recai-se em um ponto crucial, qual seja a responsabilização no cenário de *deep fakes*. Nesse sentido, analisar como se dá a sua regularização é um dos passos para tanto. Inicialmente, tem-se como uma das primeiras convenções a de Budapeste, firmada em 2001. Trata-se de uma norma internacional que visa reprimir crimes cibernéticos em escala global, a qual foi promulgada pelo Brasil com um atraso superior a 20 anos por meio do Decreto nº 11.491, de 2023 (Santos, 2025).

Já em 2013, as Leis 12.737/2012 (Lei Carolina Dieckmann) e 12.735/2012 (Lei Azeredo) passaram a vigorar. Em especial atenção, ao estabelecer o art. 154-A no Código Penal Brasileiro, a Lei Carolina Dieckmann tipificou como crime a conduta de invadir dispositivo informático, mesmo não estando conectado à *internet*, com o fim de obter, adulterar ou destruir dados ou informações sem autorização do usuário do dispositivo ou de instalar vulnerabilidades para obtenção de vantagem ilícita (Brasil, 2012).

[3] Essa informação se encontra disponível em: Secretária de Comunicação Social. ESTELIONATÁRIOS usam imagem do presidente da República em deep fake. [S. l.], 11 dez. 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/estelionatarios-usam-imagem-do-presidente-da-republica-em-deep-fake. Acesso em: 1 abr. 2025.

Outrossim, ela acrescentou dois parágrafos no art. 266 do Código Penal; o primeiro parágrafo prevê que incorrerá na mesma pena do crime do *caput* do art. 266 quem interromper serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar o restabelecimento; e o segundo altera a dosimetria da pena ao prever a pena em dobro caso cometido o crime em calamidade pública (Brasil, 1940).

Posteriormente, adveio o Marco Civil da *Internet* (Lei 12.965/2014). Para Oliveira e Ávila (2024), a referida Lei é tida como o maior marco na regulamentação de crimes digitais, vez que ela regula o uso da *internet* no país ao estabelecer princípios, garantias, direitos e deveres em seu uso. E, por derradeiro, o mesmo autor cita a Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais), a qual tem como escopo a proteção e tratamento de dados pessoais no ambiente digital por parte das empresas.

Ante o panorama legislativo ora exposto, depreende-se que não há uma tipificação legal específica para a conduta de *deep fakes*, mesmo que presente uma certa regulação temática escassa; há, portanto, uma maior complexidade devido a esta certa lacuna legislativa. Ainda, a conjuntura presente é ainda mais delicada. Se *deep fakes* são uma espécie de "evolução tecnológica" das *fake news*, esta conduta também não está positivada especificamente como crime.

Destarte, para alguns, este cenário pode impactar na responsabilização daqueles que causam desinformações e atentam contra os direitos fundamentais dos ofendidos. Tendo em vista tal complexidade, uma das tentativas para abordar as particularidades deste Direito Digital em detrimento da ausência de leis próprias regulatórias do mundo digital seria o uso de analogias (Pinheiro, 2021, *apud* Alves *et al.*, 2024).

Contudo, orientando-se pela regularização na seara penal, a analogia não se adequa como solução. Nesse sentido, explica-se: partindo do pressuposto de que há uma brecha legislativa como já exposto, não há um tipo penal específico para a prática da *deep fake.* E, em consequência da inexistência desta tipificação penal própria, não é possível aplicar o critério da analogia, pois o Direito Penal não admite *analogia in malam partem*, como defendido por Alves *et al.* (2024).

Recai-se, assim, na seguinte problemática: é necessário criar um tipo penal para criminalizar a conduta de *deep fakes?* A título de exemplo na área dos crimes cibernéticos, a Lei Carolina Dieckmann seguiu no entendimento de instituir um novo tipo penal: a invasão de dispositivo informático é crime de forma expressa. Inclusive, o caso da atriz Carolina

Dieckmann expôs como o meio digital serve como forma de vitimização feminina. No caso, Carolina teve suas fotos íntimas divulgadas na *internet* diante da invasão de seu computador.

Persistindo um pouco neste escopo dos crimes contra dignidade sexual, é corriqueira a prática de *deep fakes* de conteúdo pornográfico principalmente contra mulheres. Essa conduta possui grande potencial lesivo às vítimas indo em direção contrária aos direitos garantidos no Estado democrático, quais sejam os direitos à imagem, à honra e à dignidade sexual das ofendidas. Como exemplo, figuras femininas como Michelle Obama tornaram-se vítimas do *deep fake* pornográfico, o que mostra uma tentativa de se interferir no contexto eleitoral, violando a ideia central do Estado Democrático de Direito:

> A geração de vídeos não consensuais é uma aplicação perturbadora de deepfakes e GANs (Rede Adversária Generativa). Tudo começou com atrizes como Natalie Portman e Gal Gadot, além de outras figuras públicas femininas como Michelle Obama, Ivanka Trump e Kate Middleton, que se tornaram vítimas de inserção de deepfakes não consensuais em cenas de filmes adultos. Até o momento, as mulheres continuam sendo as principais vítimas de deepfakes (Whittaker *et al*., 2020, p. 95, tradução nossa)[4].

Mesmo diante de tamanha violação, a responsabilização dos criadores dos vídeos ou imagens pornográficas adulteradas não é eficiente. De acordo com Faria, Silva e Cardoso (2024), tendo em vista que a maioria das vítimas são do sexo feminino como mencionado, a conduta de *deep fake* pornográfico no contexto brasileiro se enquadraria no art. 147-B do Código Penal (violência psicológica contra a mulher). Em outras palavras, não há um tipo normativo específico para punição do ato, o que pode ser visto como uma forma de dificultar a responsabilização do autor.

E, novamente, retoma-se a questão inicial: a criação de um tipo penal específico seria suficiente ou até mesmo eficiente? De um lado, o Direito Penal necessita estar atento à prática de *deep fake* no cenário atual, pois "o que a *deepfake* oferece, e isso justifica o olhar cuidadoso do Direito Penal, é a credibilidade da montagem, ou seja, sua potencialidade em induzir a percepção alheia no sentido da autenticidade da cena fabricada" (Rodrigues, 2023, p. 13).

Ou seja, o que gera a tipicidade é, justamente, a credibilidade da imagem/vídeo. Se antes as tecnologias não eram desenvolvidas a ponto de causar dúvidas se a imagem era real ou não, agora, a evolução das inteligências artificiais tornou as mídias cada vez mais verdadeiras,

[4] "The generation of nonconsensual videos is a disturbing application of deepfakes and GANs. It all started with actresses such as Natalie Portman and Gal Gadot in addition to other female public figures such as Michelle Obama, Ivanka Trump, and Kate Middleton who became victims of nonconsensual deepfake insertion into adult film scenes. To date, women remain the main victims of deepfakes."

Doi 10.5281/zenodo.17068521

permitindo que se coloque em risco a imagem e a honra das vítimas, isto é, os bens jurídicos tutelados.

Desta forma, para responder a pergunta exposta, existem dois posicionamentos. De um lado, Oliveira e Ávila (2024) entendem que o fato de não ter um tipo penal específico para *deep fakes* gera impactos na punição dos responsáveis. De outro, Alves *et al.* (2024) explica que criminalizar o procedimento da criação de *deep fakes* não seria suficiente, em observância à rapidez das mudanças tecnológicas em oposição à legislativa.

Para tanto, o último autor acima mencionado assevera que a conduta acertada é analisar quais crimes já previstos podem utilizar um *deep fake* para cometê-los. Ou seja, o uso de *deep fake* (no sentido do emprego da inteligência artificial) seria o meio para consumação do outro delito expressamente tipificado no ordenamento legal adequado à conduta.

Alves *et al.* (2024, p. 26) ilustra os seguintes exemplos:

> Caso alguém edite um vídeo de modo a fazer parecer que determinada pessoa está praticando um crime, o editor do conteúdo terá praticado o crime de calúnia (art. 138, CP). Se, por outro lado, no vídeo falsificado, o indivíduo não estiver praticando um crime, mas estiver praticando um ato desabonador de sua conduta, será o criador do "deep fake" responsabilizado pelo crime de difamação (art. 139, CP). Na hipótese de injuriar alguém através dessa tecnologia, terá praticado o crime de injúria (art. 140, CP).

Nesse sentido, o que caberia seria a criação de qualificadoras ou causas de aumento de pena para aqueles que seguem o entendimento desse autor, o que poderia ser aplicado também no caso das *fake news*, já que inexiste crime específico. Tal raciocínio é adotado nos crimes contra honra, nos quais incide a causa de aumento de pena em triplo do §2º do art. 141 do Código Penal, caso cometidos ou divulgados nas redes sociais da rede mundial de computadores.

Em síntese, não há pacificação quanto à temática. A dificuldade na responsabilização é uma questão que põe em destaque a violação dos direitos fundamentais garantidos neste Estado Democrático e como as tecnologias e seu uso precisam estar alinhados a seus avanços. Mas, de toda forma, não se pode olvidar que a tutela do Direito Penal se faz imprescindível no controle e na fiscalização do manejo da inteligência artificial a fim de que os bens jurídicos por ele observados não sejam lesados.

E, por fim, terminando em uma perspectiva de responsabilidade civil, retoma-se ao denominado Marco Civil da *Internet*, explorado anteriormente neste artigo; isso porque os seus artigos 19 e 21 merecem destaque. Por meio do art. 19, a responsabilização civil do provedor

de aplicações de *internet* por dano resultante de conteúdo gerado por terceiro só se dará mediante a inércia dele na indisponibilização do conteúdo, após ordem judicial específica. Destarte, ao prever esta ordem judicial como requisito imprescindível cria-se um maior empecilho, qual seja, a necessidade de movimentar o Poder Judiciário causando maior morosidade, ao passo que a divulgação do conteúdo visual gerado por *deep fake* segue na velocidade máxima em razão da rapidez de sua propagação no meio digital.

Em contrapartida, a mesma Lei trouxe um avanço no art. 21: em caso de disponibilização de conteúdo com violação da intimidade contendo cenas de nudez ou ato sexual sem autorização dos participantes, haverá responsabilização do provedor da aplicação de *internet* se não deixar de disponibilizar o conteúdo mediante notificação dos participantes. Nesse sentido, Rodrigues (2023) aponta a relevância desta disposição legal ao compreender que se confere autonomia à vítima por poder ela iniciar as tratativas para exclusão do material sem ter que recorrer ao Judiciário, o que, por consequência, proporciona agilidade ao processo e, assim, retoma a ideia de rapidez na transmissibilidade de informações na *internet* já aqui explanada.

Por todo o discutido, estabelecer uma responsabilização civil e penal no cenário do emprego de *deep fakes* é uma tarefa árdua. O conjunto legislativo atual, ainda que esteja atento às novidades tecnológicas, não possui a mesma rapidez de avanço destas. Desta forma, advém inúmeros questionamentos, principalmente quando colocados na ótica das garantias do Estado Democrático de Direito, vez que a qualidade dos conteúdos falsamente criados pelas IAs vem se aprimorando, causando maior credibilidade às mídias manipuladas, as quais maculam direitos fundamentais das vítimas.

3 Conclusão

A democracia pode ser afetada pela evolução das tecnologias. O desenvolvimento das IAs e seu aperfeiçoamento – termo este que pode inclusive ser questionado – traz à tona diversas questões. Nesse sentido, uma delas é como o uso de *deep fakes* se encontra no cenário de violação das garantias do Estado Democrático.

Como detalhado neste artigo, a credibilidade das mídias adulteradas põe em jogo o que o Estado Democrático de Direito tanto pretende tutelar. A partir do momento em que não se é mais possível diferenciar o real do irreal, os direitos à dignidade, à honra, à informação, à liberdade sexual são afetados com a manipulação indevida das imagens das pessoas.

Práticas como o *deep fake* pornográfico ou aquele inserido em contexto eleitoral impactam tanto o campo individual quanto o coletivo. Individualmente, a vítima sofrerá abalos, vez que afetados seus bens jurídicos em sua esfera particular, como sua honra. No contexto coletivo, o interesse público se sobressai quando o manejo do conteúdo cria discursos e realidades políticas falsas, culminando na desinformação dos eleitores, o que gera efeitos graves para a democracia.

Destarte, pensa-se na responsabilização desta prática. Tal qual explicado neste texto, no âmbito criminal, inexiste um tipo penal específico para prática de *deep fake*; pior ainda, partindo do pressuposto de que *deep fake* é uma "espécie de evolução" das *fake news*, não há previsão expressa sequer para a conduta das *fake news*.

Nesta conjuntura, há quem defenda que seria ineficiente a criação de um tipo normativo específico e há quem defenda que sua ausência interfere na responsabilização. De toda forma, é imprescindível que alguma medida se inicie a fim de preservar os direitos deste Estado Democrático. A solução ainda não é clara, seja o estabelecimento de um tipo penal para tanto ou seja a alteração na dosimetria da pena de crime já existente, a questão central é que, de fato, a rapidez do avanço na qualidade das mídias falsas está em descompasso com o amparo legislativo.

O mesmo cenário se dá na responsabilização civil. Há presença tanto de avanços quanto de dispositivos legais questionáveis como o art. 19 e 21 do Marco Civil da *Internet*, como analisado anteriormente. De toda forma, nota-se uma legislação, ainda que presente, tímida e carente de melhorias.

Ante todo o exposto, infere-se que balizar as garantias do Estado Democrático de Direito e a evolução das tecnológicas, no sentido do uso das IAs no aspecto da prática de *deep fake*, não é uma tarefa fácil, mas é uma temática que precisa ser abordada e debatida para que não se transforme seu uso em um jogo de interesses, no qual os direitos individuais dos ofendidos e da coletividade são atingidos, o que não se coaduna com um sistema democrático.

REFERÊNCIAS

ALVES, B. M., *et al.*. Análise da responsabilização criminal dos criadores e propagadores de "deep fakes" no ordenamento jurídico brasileiro. **Caderno Pedagógico**, *[S. l.]*, v. 21, n. 6, p. e4348 , 2024. DOI: 10.54033/cadpedv21n6-075. Disponível em: https://ojs.studiespublicacoes.com.br/ojs/index.php/cadped/article/view/4348. Acesso em: 30 mar. 2025.

Autoridade Nacional de Proteção de Dados (ANPD). **Radar Tecnológico: Inteligência artificial generativa.** 1ª Ed. V.l. 3, - Brasília: Distrito Federal. NOV, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf. Acesso em: 9 de março de 2025.

BRASIL. **Decreto -Lei n. 2.848**, de 7 de dezembro de 1940 . Código Penal. Diário Oficial da União. Seção 1. 31/12/1940. p. 23911. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 27 de mar de 2025.

BRASIL. **Lei n. 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto - Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União. Seção 1. 03/12/2012. p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.Acesso em: 27 de mar de 2025.

Brasil. Guia Ilustrado Contra as Deepfakes. Supremo Tribunal Federal; Data Privacy Brasil. Brasília: STF, Coordenadoria de Combate à Desinformação, 2024.

FARIA, Lucas Ribeiro de; SILVA, Lucas Gonçalves da; CARDOSO, Henrique Ribeiro. DEEPFAKE PORNOGRÁFICO NA SOCIEDADE DE RISCO CONTEMPORÂNEA: OS DESAFIOS DE REGULAMENTAÇÃO E CONTROLE DA INTELIGÊNCIA ARTIFICIAL. **Interfaces Científicas - Direito**, *[S. l.]*, v. 9, n. 3, p. 343–355, 2024. DOI: 10.17564/2316-381X.2024v9n3p343-355. Disponível em: https://periodicos.grupotiradentes.com/direito/article/view/12399. Acesso em: 30 mar. 2025.

FILHO, I.N.R.; MARRAFON, M.A.; MEDÓN, F. A Inteligência Artificial a Serviço da Desinformação: como as Deepfakes e as Redes Automatizadas Abalam a Liberdade de Ideias no Debate Público e a Democracia Constitucional e Deliberativa. **Economic Analysis of Law Review**, Brasilia, v. 13, n. 3, p. 32-47, Out 2022. Disponível em: https://www.proquest.com/docview/2841146127/fulltextPDF/8C87EDA36C504E3APQ/1?accountid=8112&sourcetype=Scholarly%20Journals. Acesso em: 02 abr. 2025

OLIVEIRA, G. A. G.; ÁVILA, G. N. de. Deep fake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital. **Revista Eletrônica do Curso de Direito da UFSM**, *[S. l.]*, v. 19, p. e85239, 2024. DOI: 10.5902/1981369485239. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/85239. Acesso em: 29 mar. 2025.

PIOVESAN, Flávia; HERNANDES, Luiz Eduardo Camargo O. **Democracia: proteção constitucional e internacional**. São Paulo: Expressa, 2023. E-book. p.2. ISBN 9786553628137. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553628137/. Acesso em: 02 abr. 2025.

RODRIGUES, M. P. G. Deepfakes pornográficas não-consensuais: a busca por um modelo de criminalização. **Revista Brasileira de Ciências Criminais** , *[S. l.]*, v. 199, n. 199, p. 277–311, 2023. DOI: 10.5281/zenodo.8380977. Disponível em: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/267. Acesso em: 30 mar. 2025.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial: Uma Abordagem Moderna.** Tradução Daniel Vieira; Flávio Soares Corrêa da Silva. - 4. ed. - Rio de Janeiro: Grupo Editorial Nacional S.A, 2022.

SANTOS, Ivanilson Antônio dos. **A cadeia de custódia das provas a partir das alterações da lei 13.964 de 2019**. 57 f. Monografia (Graduação) - Curso de Bacharelado em Direito, Universidade Federal do Tocantins, Arraias, 2025.

Secretária de Comunicação Social. ESTELIONATÁRIOS usam imagem do presidente da República em deep fake. [S. l.], 11 dez. 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/estelionatarios-usam-imagem-do-presidente-da-republica-em-deep-fake. Acesso em: 1 abr. 2025.

SILVA, José Afonso da. O Estado Democrático de Direito. **Revista de Direito Administrativo**. Rio de Janeiro, vl. 173, pág. 15-34, jul./set. 1988. Disponível em: https://periodicos.fgv.br/rda/article/download/45920/44126/91434. Acesso em: 02 abr. 2025

Tribunal Superior Eleitoral. FATO ou Boato publicou quase 200 esclarecimentos contra fake news em 2022. [S. l.], 18 nov. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Novembro/fato-ou-boato-publicou-193-esclarecimentos-contra-fake-news-em-2022. Acesso em: 1 abr. 2025.

WAKEFIELD, Jane. Guerra na Ucrânia: os ‘presidentes deepfake’ usados na propaganda do conflito. **BBC NEWS BRASIL**, [S. l.], 18 mar. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60791955. Acesso em: 1 abr. 2025.

WHITTAKER, Lucas; KIETZMANN, Tim C.; KIETZMANN, Jan; DABIRIAN, Amir. All Around Me Are Synthetic Faces: The Mad World of AI- Generated Media. **IT Professional**, v. 22, n.5, p. 90-99, 2020. DOI: 10.1109/MITP.2020.2985492. Disponível em: https://ieeexplore.ieee.org/abstract/document/9194439/authors#authors. Acesso em 30 mar. 2025.

WOLKOFF, Tania Giandoni. **A era da comunicação digital: a necessidade de uma política nacional de inteligência artificial**. Tese (Doutorado em Direito) - Programa de Estudos Pós-Graduados em Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2021. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/24656. Acesso em: 21 jan. 2025.