DIREITO & POLÍTICA

Direito e Política, vol. 18, n. 2, 2023

NÃO ACREDITE EM TUDO QUE VÊ: *DEEPFAKE PORNOGRAPHY* E RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

Felipe Chiarello de Souza Pinto

Gabriela Franklin de Oliveira

Contextualização: O fenômeno da desinformação vem sendo alvo de preocupação na esfera mundial, especialmente quando se trata de eleições e ameaças à democracia. Em 2018, nos Estados Unidos, a *Deepfake* começou a ganhar destaque por ser ainda mais manipuladora do que as *Fake News*, já que, enquanto a primeira utiliza imagens, vídeos e áudios modificados por inteligência artificial, a segunda é produzida por pessoas e de forma escrita. No entanto, o que pouco se fala é que as *Deepfakes* de cunho pornográfico são as que mais circulam na internet, tendo como vítimas as mulheres cujas imagens são utilizadas sem consentimento. Assim, inicia-se um debate acerca de como responsabilizar civilmente os causadores do dano de acordo com as normas do ordenamento jurídico brasileiro.

Objetivo: Identificar os problemas, impactos e preocupações relacionado a prática de *Deepfakes*.

Metodologia: Análise de casos e de isntrumentos legislatiovos internacionais aliados a análise da legislação nacional pertinente ao caso das *Deepfakes*.

Resultados: Como resultado da presente pesquisa, foi proposto a autorregulação das plataformas como solução rápida e eficaz no combate à propagação de *Deepfakes*.

Palavras-chave: *Deepfake Pornography*; Direitos da personalidade; Responsabilidade Civil.

DO NOT BELIEVE EVERYTHING YOU SEE: DEEPFAKE PORNOGRAPHY AND CIVIL LIABILITY IN THE BRAZILIAN LEGAL SYSTEM

Contextualization: The phenomenon of misinformation has been a concern on a global scale, especially when it comes to elections and threats to democracy. In 2018, in the United States, Deepfake began to gain prominence for being even more manipulative than Fake News, as the former uses images, videos, and audio modified by artificial intelligence, while the latter is produced by individuals and in written form. However, what is rarely discussed is that pornographic Deepfakes are the most widely circulated on the internet, with women being the victims whose images are used without consent. This initiates a debate about how to hold those responsible for the harm civilly accountable according to the norms of the Brazilian legal system.

Objectives: Identifying the problems, impacts, and concerns related to the practice of Deepfakes.

Methodology: Analysis of cases and international legislative instruments, along with an examination of relevant national legislation in the case of Deepfakes.

Results: As a result of the present research, self-regulation of platforms was proposed as a swift and effective solution in combating the spread of Deepfakes.

Keywords: Deepfake Pornography; Personality Rights; Civil Liability.

NO CREAS TODO LO QUE VES: PORNOGRAFÍA DEEPFAKE Y RESPONSABILIDAD CIVIL EN EL SISTEMA LEGAL BRASILEÑO

Contextualización del tema: El fenómeno de la desinformación ha sido motivo de preocupación a nivel global, especialmente en lo que respecta a elecciones y amenazas a la democracia. En 2018, en Estados Unidos, los Deepfakes empezaron a ganar prominencia por ser aún más manipuladores que las Fake News, ya que los primeros utilizan imágenes, videos y audio modificados por inteligencia artificial, mientras que las segundas son producidas por individuos y en forma escrita. Sin embargo, lo que rara vez se discute es que los Deepfakes pornográficos son los más ampliamente difundidos en internet, con mujeres siendo las víctimas cuyas imágenes se utilizan sin su consentimiento. Esto inicia un debate sobre cómo responsabilizar civilmente a aquellos que causan el daño de acuerdo con las normas del sistema legal brasileño.

Objetivos: Identificar los problemas, impactos y preocupaciones relacionados con la práctica de los Deepfakes.

Metodología: Análisis de casos e instrumentos legislativos internacionales, junto con un examen de la legislación nacional relevante en el caso de los Deepfakes.

Resultados: Como resultado de la presente investigación, se propuso la autorregulación de las plataformas como una solución rápida y efectiva para combatir la propagación de los Deepfakes.

Palabras clave: Deepfake Pornografía; Derechos de personalidad; Responsabilidad civil.

INTRODUÇÃO

Não se sabe ao certo a origem do ditado "uma imagem vale mais do que mil palavras", mas há muitos anos ele vem sendo utilizado para dizer que uma imagem pode ser muito mais explicativa do que palavras. No meio publicitário, por exemplo, entende-se que imagens e vídeos são mais apelativos do que textos escritos, além de facilitarem a compreensão rápida do que se pretende divulgar.

Foi com finalidade publicitária, em 2017, que as *Deepfakes* começaram a ser empregadas. Tratam-se de imagens, vídeos e áudios modificados e produzidos por inteligência artificial para parecerem reais, propagando desinformação para manipular a população[1]. Apesar do "*fake*", que significa "falso", ter uma conotação negativa, as *Deepfakes* podem ter impactos positivos não apenas na indústria cinematográfica e de entretenimento,[2] como em outros setores.

Vários são os exemplos de *Deepfakes* utilizadas em produções midiáticas. Recentemente, com as especulações de que o ator Henry Cavill poderia ser o novo James Bond da franquia de 007, um canal na plataforma *YouTube* empregou tecnologia avançada para simular a atuação do ator como o personagem.[3] Em outra oportunidade, a *Deepfake* foi utilizada pela *Womanity Foundation* – instituição que atua em âmbito internacional para proteger mulheres promovendo a igualdade de gênero – no lançamento da campanha *The Noble Speech* que simulou como seria se cientistas mulheres tivessem sido reconhecidas pelo Prêmio Nobel.[4]

Entretanto, apesar de as *Deepfakes* terem potencial para criar projetos positivos e inovadores, não é o caso da maioria que circula no meio digital e as que são desenvolvidas para causar danos têm impactos avassaladores.

Em razão do próprio nome, as *Deepfakes* são muitas vezes relacionadas às *Fake News*, que protagonizam o fenômeno da desinformação e que vêm ganhando destaque nos últimos anos. Assim como as *Fake News*, as *Deepfakes* não passam de um conteúdo fraudulento que aparenta ser real. Entretanto, enquanto as *Fake News* fazem uso de palavras e textos escritos para disseminar a desinformação, as *Deepfakes* manipulam

1 RAIS, Diogo; SALES, Stela Rocha. Fake News, Deepfakes e Eleições. In: RAIS, Diogo (coord.). **Fake News**: a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. p. 29.

2 PACETE, L. Bom uso de Deepfake amplia horizontes para o marketing, saúde e entretenimento. **Forbes**, 03 dez. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/12/bom-uso-da-deepfake-amplia-horizontes-para-o-marketing-e-os-negocios/. Acesso em: 29 maio 2023.

3 ALIAGA, V. Henry Cavill é o James Bond perfeito em vídeo deepfake. **IGN**, 02 nov. 2021. Disponível em: https://br.ign.com/henry-cavill/94131/news/henry-cavill-james-bond-perfeito-video-deepfake. Acesso em: 29 maio 2023.

4 THE making of 'The Noble Speech'. Direção e produção: The Womanity Foundation. Grand-Lancy: The Womanity Foundation, 2022. 1 vídeo. Disponível em: https://www.youtube.com/watch?v=f7DhJ9dhGmY. Acesso em: 29 maio 2023.

recursos audiovisuais.

Não se trata de mero *photoshop*, pois o uso da inteligência artificial faz com que as imagens e os vídeos pareçam ser reais, de modo que quem as vê não consegue, em regra, fazer distinção entre o conteúdo falso e o verdadeiro. Um exemplo relevante foi a imagem do Papa Francisco, líder da igreja católica, usando um casaco branco que, por fugir do vestuário típico e ser considerado uma roupa *fashion*, viralizou nas redes sociais ao redor do mundo e enganou diversos usuários. Posteriormente, descobriu-se que a imagem foi criada por inteligência artificial da ferramenta *Midjourney*.[5]

O que torna as *Deepfakes* ainda mais perigosas é a forma como elas são utilizadas. Infelizmente, como será demonstrado no presente artigo, a maior parte delas são de cunho pornográfico e tem como principal alvo as mulheres. Através de aplicativos e *softwares* de inteligência artificial, é possível criar a chamada *Deepfake Pornography*, manipulando imagens de mulheres sem consentimento.

O Brasil ainda não possui leis especificas para regulamentar o uso de inteligência artificial ou que criminalizem a criação de pornográfica através de *Deepfakes*, porém existem dispositivos no ordenamento jurídico capazes de amparar as vítimas desse tipo de prática. Constatando-se violados os direitos da personalidade, surge o dever de indenizar, mas, em contrapartida, a velocidade com que o conteúdo se propaga no meio virtual somada com a anonimização dos usuários, a responsabilidade civil se torna um desafio.

É pensando em soluções rápidas para combater a *Deepfake Ponography* que a possibilidade de autorregulação das plataformas passa a se tornar um atrativo, sendo que o principal modelo é a lei alemã chamada *NetzDG*, que, por um lado, atribuiu aos provedores de aplicação a responsabilidade de remoção de conteúdo ilícito e, por outro lado, abriu margem para *overblocking* de publicações e notificações em massa de conteúdos não necessariamente infringentes.

O presente artigo foi escrito com base na análise de dados e estudos de casos de *Deepfake Ponography*, a fim de que fosse possível identificar quais os problemas, impactos e preocupações dessa prática. Em segundo momento, foi realizada análise do ordenamento jurídico brasileiro e da lei que regulamenta o uso de internet no Brasil, para que fossem identificadas as formas de amparar as vítimas e meios para responsabilização dos envolvidos. Por fim, foi considerada a autorregulação das plataformas como solução rápida e eficaz no combate à propagação de *Deepfakes*, tendo sido realizada análise crítica da *NetzDG*.

[5] LEAH, D. O que diz o casaco de Inteligência Artificial do Papa Francisco sobre o futuro da moda. *CNN Portugal*, Lisboa, 02 abril 2023. Disponível em: https://cnnportugal.iol.pt/inteligencia-artificial/papa-francisco/o-que-diz-o-casaco-de-inteligencia-artificial-do-papa-francisco-sobre-o-futuro-da-moda/20230402/642412160cf2c84d7fcedfe5. Acesso em: 29 maio 2023.

1. AS NOVAS TECNOLOGIAS E O CRESCIMENTO DA *DEEPFAKE PORNOGRAPHY*

As *Deepfakes* são um fenômeno que surgiu a partir de 2017, mas para compreender o que são, é necessário mergulhar em alguns conceitos.

Nos últimos anos, a inteligência artificial (IA), tecnologia mais sofisticada do que os robôs, vem tomando espaço no cotidiano da população. As empresas e órgãos governamentais perceberam ser viável o investimento dessa tecnologia para cortar gastos e otimizar o tempo de trabalho dos funcionários. A exemplo, o Supremo Tribunal Federal, maior órgão do poder judiciário, celebrou uma parceria com a Universidade de Brasília (UnB) e, com um investimento de R$1,6 milhões, implementou o Victor, nome em homenagem ao Victor Nunes Leal, ex-ministro que atuou na corte entre 1960 e 1969. De acordo com Dias Toffoli, ministro do STF, Victor é uma inteligência artificial com capacidade de identificar recursos com precisão de 85%, executando tarefas que demorariam 40 minutos em cinco[6]. Na prática, Victor atua na triagem de recursos recebidos pelo STF e facilita na análise de temas de repercussão geral.[7] Além disso, a suprema corte vem trabalhando no desenvolvimento de outra ferramenta conhecida como VitórIA, inteligência artificial que fará triagem de recursos e, a partir do acervo de processos do tribunal, identificará quais tratam do mesmo assunto para que recebam o mesmo tratamento, garantindo agilidade e segurança jurídica.[8]

Embora contemporaneamente muito se fale sobre inteligência artificial, não é possível dizer que se trata de uma "nova" tecnologia, já que os primeiros estudos sobre a matéria começaram na primeira metade do século XX. De acordo com as informações do acervo da enciclopédia *Britannica*, Alan Turing, pioneiro em computação, começou a desenvolver, em 1935, seus estudos em programação para desenvolvimento de máquinas com sistema e capacidade de memória e de escrita automática. Anos depois, em 1948, desenvolveu um estudo chamado *Intelligent Machinery* e, embora não tivesse usado o termo Inteligência Artificial, estabeleceu conceitos iniciais sobre essa nova tecnologia, porém o artigo nunca foi publicado e a pesquisa acabou sendo reinventada por outros cientistas posteriormente[9].

---

6 MONTENEGRO, M. C. Inteligência Artificial: Trabalho judicial de 40 minutos pode ser feito em 5 segundos. **Agência CNJ de Notícias**, Brasília, 23 outubro 2018. Disponível em: https://www.cnj.jus.br/inteligencia-artificial-trabalho-judicial-de-40-minutos-pode-ser-feito-em-5-segundos/. Acesso em: 29 maio 2023.

7 ESTRUTURA orgânica do STF passa a contar com setor voltado a inteligência artificial. **STF Notícias**, Brasília, 27 dezembro 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalh e.asp?idConteudo=499690&ori=. Acesso em: 29 maio 2023.

8 STF finaliza testes de nova ferramenta de Inteligência Artificial. **STF Notícias**, Brasília, 11 maio 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=507120&ori=1. Acesso em: 24 maio 2023.

9 COPELAND, B. J. Alan Turning and the beginning of AI. **Britannica**. Disponível em: https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI. Acesso em: 29 maio 2023.

Poucos anos depois, em 1956, foi desenvolvido o primeiro projeto de inteligência artificial, durante o *Dartmouth Summer Research Project on Artificial Intelligence* (Projeto de Pesquisa de Verão sobre a Inteligência Artificial de *Dartmouth* – tradução livre), cujo objetivo era o aprofundamento dos estudos quanto ao funcionamento da mente humana para então reproduzi-la em máquinas. Embora pioneiro, os cientistas conseguiram estabelecer os pilares para o desenvolvimento dessa nova tecnologia, quais sejam: capacidade de aprendizagem, processamento e criatividade do cérebro humano.[10]

O Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial (GPAN IA), formado pela Comissão Europeia, define a inteligência artificial como um sistema desenvolvido por humanos que, em sua complexidade, atua no meio físico e digital, tendo a capacidade de perceber e interpretar o ambiente, coletando informações e desenvolvendo estruturas de dados e, com base nisso, conseguindo tomar decisões, fundamentando-se em parâmetros pré-definidos. A inteligência artificial também pode ser desenvolvida para aprender a se adaptar e se aprimorar com base nos resultados das ações anteriores no ambiente[11].

Para funcionamento, a inteligência artificial faz uso de algoritmos que são, de forma bem simplificada, fórmulas matemáticas e operações estatísticas que programam e executam tarefas em curto espaço de tempo e com alto grau de precisão[12]. Para tanto, a IA faz uso de algumas técnicas de aprendizagem.

Algumas inteligências artificiais possuem tecnologia *machine learning*, frequentemente traduzido para o português como aprendizado da máquina, que corresponde a um método por meio do qual o computador busca padrões nos dados, através de estatísticas, para tomar decisões[13]. Ou seja, a máquina, por tentativa e erro, gera um catálogo de resultados que tornam os algoritmos mais preparados para a solução de problemas e para obtenção de melhores resultados. Essa tecnologia é utilizada, por exemplo para reconhecimento facial e decodificação de linguagem.

---

10 ARTIFICIAL Intelligence Coined at Dartmouth. Dartmouth College, Hanover. Disponível em: https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth. Acesso em: 29 maio 2023.

11 "Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions." (A DEFINITION of AI: Main Capabilities and Scientific Disciplines. The European Commission's High-Level Expert Group on Artificial Intelligence, Brussels, 2018. Disponível em: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines. Acesso em: 30 maio 2023.

12 SOARES, Flaviana Rampazzo. Levando Algoritmos a Sério. In: BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 45

13 FALEIROS JÚNIOR, José Luiz de Moura. A evolução da Inteligência Artificial em breve retrospectiva. In: BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 20

A inteligência artificial com *machine learning* já está sendo utilizada pela polícia federal brasileira desde julho de 2021, ano em que foi implementada a Solução Automatizada de Identificação Biométrica (ABIS), tecnologia que possibilita coleta, armazenamento e cruzamento de dados de impressão digital e reconhecimento facial.[14] A polícia federal realizou a transferência dos dados do sistema de armazenamento anterior para abastecer a ABIS, ou seja, já na implementação, foi abastecida com 22,2 milhões de digitais de pessoas cadastradas.[15]

Dentro das tecnologias que utilizam *machine learning* existe um segmento de inteligência artificial que utiliza uma técnica ainda mais aprimorada, conhecida como *deep learning* e frequentemente traduzida para o português como aprendizado profundo. Esse método utiliza *neural networks*, isto é, assim como o cérebro humano, possui um complexo de neurônios que são pequenas unidades de computadores simples que se conectam. Essas redes neurais permitem que a máquina tome decisões precisas baseadas em dados[16].

O *deep learning* é a tecnologia da inteligência artificial utilizada para criação das *Deepfakes* (combinação de *deep learning* com *fake*)[17]. Através das redes neurais, a inteligência artificial analisa imagens, vídeos e áudios e aprende a criar conteúdo imitando expressões faciais, voz e jeito. Em razão do *deep learning*, quanto mais a inteligência artificial é exposta ao material visual e auditivo, mais ela se aprimora para produzir conteúdo que pareça cada vez mais real[18]. Por isso, a *Deepfake* não é mero uso de Photoshop, afinal a inteligência artificial manipula o conteúdo audiovisual de forma tão precisa que quem o consome pode ser facilmente enganado.

A tecnologia *Deepfake* pode ter impactos positivos em vários segmentos, como cinematográfico, educacional, telecomunicações, entre outros. A *Deepfake* permite recriar o passado, como no áudio criado pela *CereProc*, em que a voz de John F. Kennedy, ex-presidente dos Estados Unidos, foi utilizada para recriar o discurso que seria feito em

14 POLÍCIA Federal implementa nova Solução Automatizada de Identificação Biométrica. Gov.br, Brasília, 30 jun. 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica. Acesso em: 30 maio 2023.

15 LIMA, E. K. Sistema de reconhecimento facial da PF é "preocupante e ilícito", afirmam especialistas. **Olhar Digital**, 13 jul. 2021. Disponível em: https://olhardigital.com.br/2021/07/13/seguranca/sistema-de-reconhecimento-facial-da-pf-e-preocupante-e-ilicito-afirmam-especialistas/. Acesso em: 30 maio 2023.

16 FALEIROS JÚNIOR, José Luiz de Moura. A evolução da Inteligência Artificial em breve retrospectiva. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. Direito Digital e Inteligência artificial: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 21.

17 RAIS, Diogo; SALES, Stela Rocha. Fake News, Deepfakes e Eleições. In: RAIS, Diogo (coord.). **Fake News**: a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. p. 28.

18 FALEIROS JÚNIOR, José Luiz de Moura. A evolução da Inteligência Artificial em breve retrospectiva. In: BARBOSA, M. M.; BRAGA NETTO, F.; SILVA, M.C.; FALEIROS JÚNIOR, J. L. M. **Direito Digital e Inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 21.

Dallas na data de seu assassinato em 22 de novembro de 1963.[19] Em outro campo, a inteligência artificial já está sendo empregada para auxiliar pessoas com necessidades especiais, a exemplo da empresa *VOCALiD*, que criou um sistema que permite a criação de voz personalizada para pessoas com deficiência ou cuja habilidade de fala está comprometida.[20]

Entretanto, as *Deepfakes*, a depender de como forem usadas, podem ter um impacto avassalador e as principais vítimas são mulheres, que se tornaram alvo de conteúdo pornográfico, como visto no estudo publicado em 2019 pela empresa de cyber-segurança *Deeptrace* (hoje chamada *Sensity*). Neste, identificou-se que, entre dezembro de 2018 e setembro de 2019, foram publicadas cerca de 14.678 *Deepfakes*, destas, 96% são *Deepfake Pornography* e todas elas envolvem mulheres.[21]

Um novo estudo realizado pela *Sensity* identificou que, em junho de 2020, existiam 49.081 vídeos *Deepfakes* circulando na internet, demonstrando um crescimento de 330% entre os meses de julho de 2019 e junho de 2020. Ainda em análise dos dados deste novo relatório, foi identificado que a *Deepfake Pornography* segue sendo a principal e majoritária, sendo que 99% das mulheres, cujas imagens são criadas de forma não consensual, são atrizes e celebridades do setor de entretenimento. O 1% restante corresponde às mulheres do setor de notícias e midiático. O crescimento anual das *Deepfakes* pode ser visto no gráfico abaixo:[22]

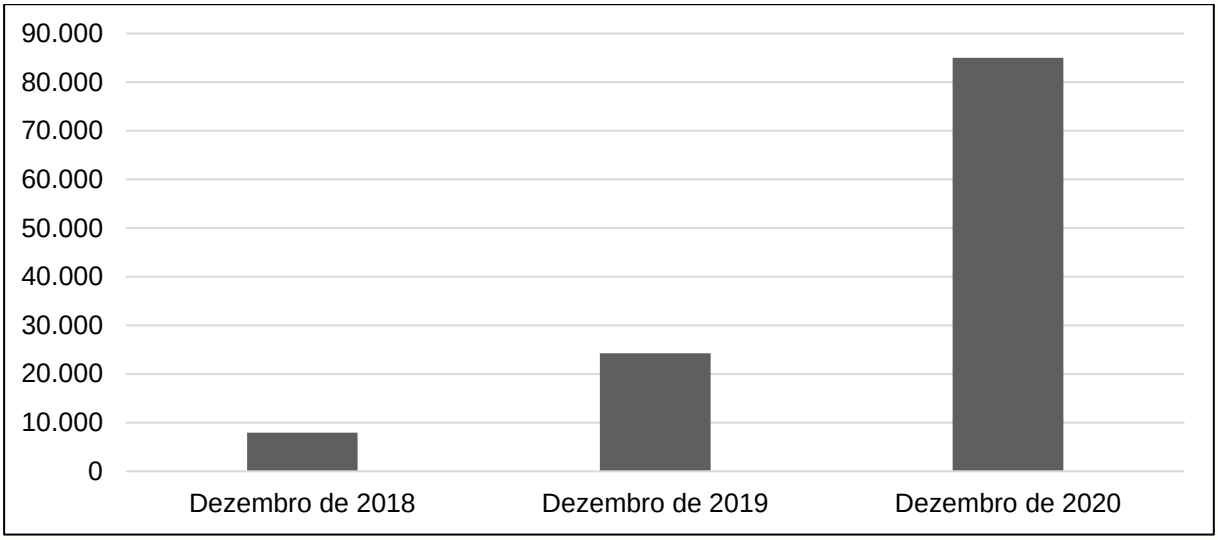
19 JFK Unsilenced Project. Direção: Chris Pidcock. Produção: CereProc. Edinburgh, 2018. Disponível em: https://www.cereproc.com/en/jfkunsilenced. Acesso em: 28 maio 2023.

20 VOCALID a Veritone company. Disponível em: https://vocalid.ai/. Acesso em: 28 maio 2023.

21 DEEPTRACE. The State of Deepfakes: Landscape, Threats, and Impact. Amsterdã: Deeptrace, 2019. Disponível em: https://sensity.ai/reports/. Acesso em: 14 maio 2023.

22 DEEPTRACE. The State of Deepfakes: Landscape, Threats, and Impact. Amsterdã: Deeptrace, 2019. Disponível em: https://sensity.ai/reports/. Acesso em: 14 maio 2023, p. 3.

Figura 1 - Crescimento anual das Deepfakes



Um caso emblemático de *Deepfake Pornography* foi o aplicativo *DeepNude*, lançado em junho de 2019. [23]Tratava-se de um aplicativo de computador por meio do qual os algoritmos removem as roupas das mulheres e geram partes do corpo nuas. No caso desse aplicativo, não era possível obter resultados com corpos masculinos, pois a inteligência artificial foi treinada e desenvolvida apenas para assimilar o corpo feminino. Assim que ficou disponível para *download*, os criadores perderam o controle. Em um mês, o aplicativo teve 545.162 visitas e 95.464 usuários ativos, de modo que os criadores optaram por exclui-lo e não lançar novas versões, pois, segundo eles, "o mundo não está pronto para *DeepNude*". Apesar da desativação do aplicativo, novos sistemas semelhantes continuaram a ser criados. Uma vez reconhecido o potencial do *DeepNude* original, os criadores lançaram para venda no mercado por 30.000 dólares.[24]

No ano seguinte, em 2020, outro caso envolvendo *Deepfake Pornography* ocorreu na plataforma do aplicativo de mensagens *Telegram*. Trata-se de um bot que, de forma simplificada, opera dentro da plataforma *Telegram* por meio do qual os usuários podem interagir e customizar a aplicação.[25] Por meio da interação com os *bots*, usuários do *Telegram* conseguiram criar conteúdo pornográfico de mulheres a partir das imagens utilizadas em redes sociais. De acordo com a apuração da empresa *Sensity*, mais de 100.000 imagens foram criadas e propagadas pelo *Telegram* durante o mês de julho de 2020 (esses valores não incluem as *Deepfakes* que foram criadas, porém não

23 DEEPTRACE. **The State of Deepfakes**: Landscape, Threats, and Impact. Amsterdã: Deeptrace, 2019. Disponível em: https://sensity.ai/reports/. Acesso em: 14 maio 2023, p. 8.

24 DEEPTRACE. **The State of Deepfakes**: Landscape, Threats, and Impact. Amsterdã: Deeptrace, 2019. Disponível em: https://sensity.ai/reports/. Acesso em: 14 maio 2023. p. 8.

25 TELEGRAM. Disponível em: https://core.telegram.org/bots. Acesso em: 20 de maio de 2022.

compartilhadas). As vítimas são mulheres de todas as idades, inclusive crianças e adolescentes.[26]

O crescimento da *Deepfake Pornography*, de forma desgovernada e sem regulamentação, está sendo utilizada como uma ferramenta de opressão das mulheres. As imagens, sons e vídeos são manipulados para criar um conteúdo pornográfico, sem consentimento, de mulheres falando e agindo da forma desejada pelos criadores da *Deepfake*, como um conteúdo personalizado.

Segundo um estudo desenvolvido pelo *European Parliamentary Research Service* no painel sobre futuro da ciência e da tecnologia e destinado aos membros do Parlamento Europeu, inicialmente, os vídeos de pornografia tinham como principais alvos mulheres celebridades, porém a grande oferta de dados para a tecnologia *Deepfake* tornou mais fácil para criar conteúdo de mulheres não famosas. A preocupação é que a *Deepfake* possa ser usada para criar pornografia de vingança ou outros tipos de abuso especialmente para descredibilizar mulheres, como as que atuam na política e jornalistas.[27]

A jornalista investigativa Rana Ayyub foi uma das vítimas de uma *Deepfake Pornography*. Ela havia sido convidada para comentar uma matéria sobre abuso sexual infantil na Índia e, no dia seguinte, vídeos pornográficos com o seu rosto e que pareciam verdadeiros começaram a circular pelos aplicativos de mensagem. Embora o caso tenha tomado notoriedade e um dos vídeos tenha sido compartilhado mais de 40.000 vezes, o governo indiano e as redes sociais tomaram providências apenas após a intervenção do Reino Unido[28].

O relatório escrito pelo *European Parliamentary Research Service* destaca que a *Deepfake Pornography*, do ponto de vista jurídico, em se tratando de uso de imagem não consensual, não há que se falar em legalidade do conteúdo. Embora ainda não exista, no ordenamento jurídico europeu, a criminalização da pornografia gerada por *Deepfake*, já existem leis que podem servir de amparo para as vítimas.[29]

Nesse mesmo sentido, no ordenamento jurídico brasileiro, ainda não existem leis

---

26 DUFFY, Ryan. Pornographic "Deepfake Ecosystem" on Telegram Uncovered by Sensity. **Tech Brew**, 02 nov. 2020. Disponível em: https://www.emergingtechbrew.com/stories/2020/11/02/pornographic-deepfake-ecosystem-telegram-uncovered-sensity. Acesso em: 30 maio 2023.

27 SERVICE, European Parliamentary Research. Tackling deepfakes in European policy. In: Panel for the future of science and technology. Estrasburgo: European Parliament, julho 2021. p. 24. Disponível em: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690039. Acesso em 30 maio 2023.

28 AYYUB, Rana. "I was the victim of a deepfake porn intended to silence me" by Rana Ayyub. Huffpost, 21 novembro 2018. Disponível em: https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316. Acesso em: 12 dezembro 2021.

29 SERVICE, European Parliamentary Research. Tackling deepfakes in European policy. In: Panel for the future of science and technology, 2021, Estrasburgo, Relatório [...]. Estrasburgo: European Parliament, jul. 2021. p. 1-95. Disponível em: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690039. Acesso em: 30 maio 2023. p. 50.

que criminalizam a *Deepfake Ponography*, mas já é possível pensar em garantias que podem amparar as vítimas desse tipo de prática, bem como quais os desafios que podem ser enfrentados.

2. VIOLAÇÃO AOS DIREITOS DA PERSONALIDADE E OS DESAFIOS NA RESPONSABILIZAÇÃO CIVIL DAS *DEEPFAKES*

Os direitos da personalidade são, em uma concepção naturalista, atributos inerentes à condição humana e são exercidos normalmente por qualquer pessoa. São direitos naturais e inatos, cabendo ao Estado unicamente trazê-los ao plano positivo através de sanções.[30]

Isso significa dizer que toda pessoa humana tem direitos da personalidade que devem ser zelados e respeitados. Dentro dessa categoria, existe o direito à imagem, que corresponde ao direito que toda pessoa tem sobre sua forma física com todos os componentes distintos que a individualizam (como boca, nariz, olhos e entre outras características físicas). Trata-se de um direito autônomo cuja disponibilidade depende inteiramente da vontade e autorização do titular[31]. Nesse sentido, antes do advento do Código Civil de 2002, o Superior Tribunal de Justiça julgou o Recurso Especial 46.420/SP, sob relatoria de Ruy Rosado de Aguiar Júnior, ex-ministro da corte, e definiu direito a imagem como "direito autônomo, incidente sobre um objeto específico, cuja disponibilidade é inteira do seu titular e cuja violação se concretiza com o simples uso não consentido ou autorizado"[32]

O direito à imagem é frequentemente confundido com o direito à honra. Embora ambos sejam direitos da personalidade, um independe do outro. Enquanto o primeiro está dentro da classificação de direitos físicos da personalidade e diz respeito a representação audiovisual, o segundo está dentro dos direitos psíquicos e tem como objeto a reputação.[33]

O direito à honra é um elemento de cunho moral que acompanha a pessoa humana desde o nascimento até pós-morte. Tal direito abrange tanto a reputação da pessoa (honra objetiva) quanto o sentimento pessoal de estima e consciência da própria dignidade (honra subjetiva). A violação desse direito causa impactos na posição do indivíduo na

30 BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. São Paulo: Saraiva, 2015. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502208292/. Acesso em: 10 maio 2022. p. 38.

31 SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Editora Atlas, 2014. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493449/. Acesso em: 10 maio 2022. p. 108.

32 BRASIL. Superior Tribunal de Justiça (4. Turma) **Recurso Especial 46420-0/SP**. Diário de Justiça Eletrônico Brasília, DF, 331.565. 05 de dezembro de 1994. p. 7-8.

33 SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Editora Atlas, 2014. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493449/. Acesso em: 10 maio 2022, p. 74.

sociedade.[34]

Tanto o direito à imagem, quanto o direito à honra, estão dentre os direitos fundamentais assegurados no art. 5º, X, da Constituição Federal de 1988 (CF/88), assim como na Declaração Universal dos Direitos Humanos, no artigo 12 que prevê que nenhuma pessoa será sujeita a ataques a sua honra e reputação.

O Código Civil estabelece, no art. 20, a proibição da publicação, exposição ou utilização da imagem de uma pessoa sem a sua autorização, prevendo ainda a possibilidade de indenização no caso desta violação.

Nesse sentido, o ordenamento brasileiro é muito semelhante ao português, que em seu art. 79 dispõe sobre o direito à imagem de forma clara ao determinar que "1. O retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela [...]". Ou seja, no caso das redes sociais, embora o usuário titular da conta tenha publicado retrato contendo imagem própria, esta não pode ser utilizada para outros fins sem que haja prévio consentimento.

O Código Civil, no artigo 11, estabelece, ainda, que os direitos da personalidade são intransmissíveis e irrenunciáveis, ou seja, o direito à imagem sempre será do titular, que pode autorizar para que esta seja utilizada para outros fins. A autorização é, portanto, um negócio jurídico que requer consentimento[35].

No caso dos aplicativos que criam as *Deepfakes* ou até as *Deepfakes Pornographies*, a imagem das mulheres é utilizada sem consentimento e sem que muitas sequer saibam, ou seja, as vítimas claramente têm seu direito à imagem violado. Ainda, para a mulher, o constrangimento e a humilhação decorrentes da exposição e uso não consentido da imagem para produção de conteúdo pornográfico configuram grave ofensa ao direito à honra. Isso pois, há clara violação à reputação da mulher, podendo causar impactos não apenas sociais, como também patrimoniais (como por exemplo o abalo ou descrédito da pessoa no emprego).

Assim, nos termos do art. 5º, X, da Constituição Federal, a violação do direito à honra e imagem gera o dever de indenizar material e moralmente pelos danos decorrentes de tal violação.

Na esfera cível, ao se tratar de responsabilidade, uma vez reconhecida a prática de

34 SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Editora Atlas, 2014. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493449/. Acesso em: 10 maio 2022, p. 75.

35 SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Editora Atlas, 2014. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493449/. Acesso em: 10 maio 2022.

ato ilícito, há o dever de indenizar (art. 927 do Código Civil).[36] No Brasil, a responsabilidade civil requer a presença de quatro elementos: fato, culpa, dano e nexo causal.[37] Dessa forma, é necessário que a vítima do ato danoso demonstre: (i) o nexo de causalidade (conexão) entre a conduta culposa e o dano causado e (ii) a culpa do ofensor a ser responsabilizado.[38]

Em alguns casos, no entanto, não é necessária a comprovação da culpa para que o agente tenha o dever de indenizar, conforme estabelece o Código Civil, no art. 927, parágrafo único,[39] que dispõe a obrigação de reparar o dano independente de culpa nos casos específicos previstos em lei ou quando a atividade normalmente desenvolvida pelo autor implicar risco aos direitos de outrem.

Quando se trata de responsabilização no ambiente digital, surgem alguns desafios quanto à tutela dos direitos fundamentais. O primeiro é a velocidade extraordinária que o conteúdo se propaga, de modo que o dano pode ser compartilhado em esfera mundial dentro de minutos. O segundo desafio está relacionado à eternização do conteúdo compartilhado nas redes que, mesmo depois de removido, não interrompe integralmente a ocorrência do dano. O terceiro desafio é o anonimato.

No caso do aplicativo *DeepNude*, por exemplo, conforme já demonstrado no tópico anterior, os dados são alarmantes. Em um mês de uso, o aplicativo teve 545.162 visitas e 95.464 usuários ativos, o que demonstra a velocidade com que o conteúdo se propagou no meio virtual. Após a criação, outros aplicativos da mesma natureza surgiram com modificações e melhorias, o que demonstra que a simples remoção do *DeepNude* não surtiu o efeito desejado. [40]

Por sua vez, o anonimato na internet prejudica a responsabilização dos usuários que compartilham o conteúdo pornográfico no meio virtual. Isso pois, muitas vezes o usuário é identificado com um mero apelido ou nome "fantasia", não dispondo de endereço físico ou eletrônico ou de qualquer outro meio para identificação.[41]

---

36 "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo". (BRASIL. **Código Civil**. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF, Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 set. 2023.)

37 PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 20 maio 2022. Capítulo 9.

38 GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 20. ed. São Paulo: Saraiva Educação, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 20 maio 2022.

39 "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. [...] Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".

40 DEEPTRACE. **The State of Deepfakes**: Landscape, Threats, and Impact. Amsterdã: Deeptrace, 2019. Disponível em: https://sensity.ai/reports/. Acesso em: 14 maio 2023. p. 8

41 PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 20 maio 2022. Capítulo 9.

A solução para identificar os usuários e solicitar a remoção do conteúdo é recorrer aos provedores de aplicação, categoria que integra provedores de correio eletrônico, hospedagem e conteúdo que ocupam grande espaço no meio virtual,[42] a exemplo do *Google, Meta, Yahoo* e *Telegram*.

Seguindo a lei 12.965 de 2014, conhecida como Marco Civil da Internet (MCI), criada para estabelecer diretrizes, direitos e deveres para o uso da internet no Brasil, estabeleceu-se, no artigo 19, *caput*, parágrafo 1°, como regra, a necessidade de ordem judicial específica para a remoção de conteúdo publicado no site hospedado por um provedor de aplicação. Isso obriga o interessado na remoção a, necessariamente, acionar o poder judiciário.

É importante destacar a relevância do artigo 19 do MCI que, como a própria redação sugere, foi criado com objetivo de "assegurar a liberdade de expressão e impedir censura", de modo que o "provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para (...) tornar indisponível o conteúdo apontado como infringente".[43]

Nas palavras de André Zonaro Giacchetta:

> A adoção dessa medida visa combater a indústria das notificações para remoção de conteúdo. O Marco Civil assume posição de defesa da liberdade de expressão e garante aos provedores a necessária imunidade que minimiza o temor que poderia existir no sentido de que a não remoção do conteúdo, depois de notificação, geraria responsabilização.[44]

Ou seja, na redação do artigo 19 do MCI, a intenção do legislador é evitar a retirada indevida de conteúdo de forma unilateral pelos provedores, garantindo a liberdade de expressão prevista nos artigos 2 e 3, I, da referida lei. Entretanto, a vítima de violações à personalidade passou a ter que buscar o Poder Judiciário para ter resguardados seu direito à imagem e honra.[45]

Quando se trata de liberdade de expressão no ambiente digital, é importante deixar claro que, nas palavras de Marco Aurélio Florêncio Filho, "nenhum princípio tem caráter absoluto, a própria liberdade de expressão não possui esse caráter", de modo que, havendo excessos ou abusos no exercício desse direito, a liberdade de expressão não deve

---

[42] TEIXEIRA, Tarcisio. **Direito Digital e Processo Eleitoral**. 5. ed. São Paulo: Saraiva Educação, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596946/. Acessado em 19 de maio de 2022.

[43] BRASIL. **Marco Civil da Internet**. Brasília, DF: Presidência da República, 2014 Redação do artigo 19, caput, do Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 09 maio 2023.

44 GIACCHETTA, André Zonaro. Atuação e responsabilidade dos provedores diante das fake news. In: RAIS, D. (coord). **Fake News**: a conexão entre a desinformação e o direito. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 289.

45 LONGHI, João Victor Rozatti. **#ódio**: responsabilidade civil nas redes sociais e a questão do *hate speech*. In: MARTINS, G. M.; ROSENVALD, N. (coord.). 1. ed. Indaiatuba: Editora Foco, 2020. p. 304.

prevalecer "sob pena de violar ainda a dignidade da pessoa humana".[46]

Nesse mesmo sentido, conforme explica Juliana Abrusio, a liberdade de expressão, além de respeitar a honra alheia, deve estar ausente de informações manipuladas, afinal, o acesso às informações verdadeiras garante que a Internet seja um "instrumento democrático para o exercício da cidadania".[47] Ainda, Felipe Chiarello afirma que a liberdade de expressão marca a consolidação do regime democrático de direito e que nenhum governo tem o direito de impedir que os indivíduos se expressem, contanto que as informações sejam verdadeiras de modo que as considerações feitas ao acaso ou sem comprovações prejudiquem outrem. Afirma, ainda, que nesses casos devem ser punidas na forma da lei.[48]

No caso do uso de imagens por *Deepfakes* para criar pornografia, além da ausência de consentimento que caracteriza violação dos direitos à personalidade, o conteúdo é manipulado e propositalmente fraudulento, fato que por si só já é suficiente para que haja remoção das redes.

Soma-se a isso o art. 21[49] do MCI traz previsão que possibilita a remoção de publicação sem que haja ordem judicial específica, qual seja: em caso de divulgação de imagens, vídeos e outros materiais contendo cenas de nudez e outros atos sexuais de caráter privado. Nesses casos, é possível que a vítima encaminhe notificação diretamente ao provedor, contendo a URL específica a que se pretende a remoção. Caso não haja remoção após o envio da notificação, o provedor de aplicação poderá ser responsabilizado subsidiariamente pela violação.

No que se refere à identificação dos usuários, os provedores de aplicação podem fornecer dados para esse fim mediante ordem judicial, conforme previsto nos. artigos 7º, II e III e 10º, ambos do MCI. Apenas assim, poderá ser quebrado o sigilo e fornecidos os dados de registro de acesso à aplicação, que contém endereço de IP, data e horário relativos à atividade.

Uma vez obtidas essas informações, surge um terceiro personagem: os provedores

46 FLORÊNCIO FILHO, Marco Aurélio. Apontamentos sobre a liberdade de expressão e a violação da privacidade no Marco Civil da Internet. In: MASSO, F. D.; ABRUSIO, J.; FILHO, M. A. F. (coord.). **Marco Civil da Internet**: lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais Ltda., 2014. p. 32.

47 ABRUSIO, Juliana. As fragilidades da estrutura informacional da rede. In: MASSO, F. D.; ABRUSIO, J.; FILHO, M. A. F. (coord.). **Marco Civil da Internet**: lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais Ltda., 2014. p. 89 e 90.

48 ARANHA FILHO, R. C.; PINTO, F. C.; RAMOS, T. A Liberdade de Expressão Política e o Discurso de Ódio (Hate Speech) em Período Eleitoral: estudos de casos da Corte Interamericana de Direitos Humanos. In: MARQUES, C. L.; MARTINI, S. R.; FINCO, M. (org). **Diálogos entre direitos humanos, direito do consumidor, compliance e combate à corrupção**. 1. ed. São Paulo: YK Editora, 2021. p. 155 a 159.

49 "Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente 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 quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo."

de conexão. O que se busca, neste momento, é o registro de conexão à internet para que se certifique de que aquele endereço de IP se conectou à internet a partir da estrutura daquele provedor. Uma vez identificado, o provedor de conexão pode dizer qual cliente realizou acesso[50].

Ou seja, restou demonstrado que não se trata de um processo simples e muito menos célere. Se por um lado um conteúdo, mesmo que danoso, pode atingir a escala mundial dentro de minutos, a justiça brasileira é lenta, podendo, em alguns casos, demorar mais de um ano para que um processo destes seja concluído.[51]

Vale destacar, ainda, que o MCI estabelece a guarda dos registros de conexão por apenas um ano e a guarda do registro de aplicação por seis meses, no caso de provedores que sejam pessoas jurídicas. No caso de provedor pessoa física, a remoção é facultativa.[52]

Para contornar processos judiciais e na tentativa de tornar a navegação virtual mais segura para os usuários, as plataformas estabelecem Termos de Uso e Políticas de Privacidade, que nada mais são do que diretrizes e regras que devem ser respeitadas por todos os usuários, sob pena de remoção do conteúdo ou até mesmo a exclusão do perfil. Isso demonstra que o artigo 19 do MCI, embora exerça um papel fundamental para garantir a liberdade de expressão, não é absoluto, na medida em que é possível a remoção de conteúdo em caso de violação das políticas internas da plataforma.[53]

Quando se fala em combater a pornografia, o anonimato e a propagação de conteúdo fraudulento, os provedores de aplicação podem ser grandes aliados. A plataforma *Facebook*, por exemplo, implementou inteligência artificial para detectar conteúdo violador dos Termos de Uso, possibilitando que seja removido em menor tempo e com maior precisão.[54] A possibilidade de autorregulação das plataformas permite maior velocidade e efetividade, fator que é grande aliado no combate à *Deepfake Pornography*.

50 CRUZ, Francisco Brito; SILVEIRA, Hélio Freitas de Carvalho da; ABREU, Jacqueline de Souza; ANDRADE, Marcelo Santiago de Paduá; VIEIRA, Rafael Sonda; OLIVA, Thiago Dias. **Direito Eleitoral na Era Digital**. Belo Horizonte: Casa do Direito, 2018. p. 104.

51 Segundo os dados divulgados no relatório "Justiça em números 2021" do Conselho Nacional de Justiça, o tempo médio de um processo em 1° grau na Justiça Estadual é de 2 anos e 5 meses até a sentença e de 3 anos e 4 meses até a baixa. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/09/relatorio-justica-em-numeros2021-12.pdf. Acessado em 09 de maio de 2023.

52 CRUZ, Francisco Brito; SILVEIRA, Hélio Freitas de Carvalho da; ABREU, Jacqueline de Souza; ANDRADE, Marcelo Santiago de Paduá; VIEIRA, Rafael Sonda; OLIVA, Thiago Dias. **Direito Eleitoral na Era Digital**. Belo Horizonte: Casa do Direito, 2018. p. 106.

53 GIACCHETTA, André Zonaro. Atuação e responsabilidade dos provedores diante das fake news. In: RAIS, D. (coord). **Fake News**: a conexão entre a desinformação e o direito. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 278.

54 META AI. Community Standards. Disponível em: https://ai.facebook.com/blog/community-standards-report/. Acesso em: 15 maio 2023.

3. A POSSIBILIDADE DE AUTORREGULAÇÃO DAS PLATAFORMAS PARA O COMBATE DE *DEEPFAKES*

Como se verá abaixo, as plataformas digitais podem ser grandes aliadas no combate de *Deepfakes* no ambiente digital, posto que, através da autorregulação, é possível a remoção de conteúdo de forma rápida e eficaz.

Como mencionado anteriormente, o artigo 19 do MCI prevê como regra a necessidade ordem judicial específica para remoção de conteúdo publicado nas plataformas digitais. Visando contornar a necessidade de provocar o poder judiciário e garantir soluções mais rápidas no combate de conteúdo ilícito, as plataformas digitais podem remover publicações que violem as diretrizes da comunidade por elas estabelecidas.

Na Europa, já está sendo adotado o modelo de autorregulação, que atribui o dever de remover conteúdo ilícito aos provedores de aplicação. Segundo a Comissão Europeia, conteúdos ilícitos, como discurso de ódio nas redes sociais, têm um potencial destrutivo e devem ser confiados à autorregulação.[55] Inclusive, em 2016, as empresas *Facebook, Twitter, Microsoft* e *Google* se comprometeram a lutar contra a propagação desse tipo de conteúdo através da adoção do Código de Conduta, da Comissão Europeia.

Dentre o que estabelece o Código de Conduta, destaca-se a adoção de procedimentos para examinar as notificações relativas aos discursos ilegais de incitação ao ódio em prazo de 24 horas.[56] Como resultado, até janeiro de 2018, as empresas de tecnologia de informação conseguiram suprimir, em média, 70% dos discursos de ódio ilegais que lhes foram notificados e mais de 80% das notificações foram analisadas no prazo de 24 horas.[57]

Nesse mesmo sentido, em 2018, a lei alemã conhecida como *NetzDG* ganhou destaque no ordenamento jurídico europeu, pois estabeleceu a autorregulação das plataformas para remoção de conteúdos ilícitos nas redes sociais com mais de 2 milhões de usuários e que não prestem comunicações individuais, como o aplicativo de mensagens *WhatsApp* e *Telegram*. Desse modo, foi estipulado prazo máximo de 24 horas para remoção de conteúdo ilícito (ou em até sete dias, a depender da complexidade do caso),

55 CUEVA, Ricardo Villas Boas. Alternativas para a remoção de fake news nas redes sociais. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 274.

56 EUROPEIA, Comissão. Código de Conduta para a luta contra os discursos ilegais de incitação ao ódio em linha. Disponível em: https://commission.europa.eu/document/551c44da-baae-4692-9e7d-52d20c04e0e2_pt. Acesso em: 09 maio 2023.

57 WIGAND. C. Luta contra discursos ilegais de incitação ao ódio em linha – Iniciativa da Comissão regista progressos constantes, adesão de novas plataformas. Comissão Europeia, Bruxelas, 19 jan. 2018. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_261. Acesso em: 09 maio 2023.

sob pena de multa de 50 milhões de euros.[58] Em 2021, foi criada a Lei de Combate ao Extremismo de Direita e Discurso de Ódio[59], que ampliou o rol de crimes listados na lei alemã, incluindo, por exemplo, o crime de perturbação da paz pública e ameaças de cometer crimes.

Ou seja, a lei alemã atribui a responsabilidade jurídica de remover conteúdos ilícitos, concentrados em delitos penais, aos provedores de aplicação. Dessa forma, o conteúdo que viole a lei penal alemã, bem como direitos de personalidade de indivíduos ou que tenha potencial de causar perturbação da ordem pública deve ser removido. O objetivo da lei é garantir que os provedores tenham um procedimento efetivo e transparente para remoção de conteúdo ilícito dentro do prazo determinando e, consequentemente, atingindo melhores resultados na garantia dos direitos individuais.[60]

Apesar de a lei dar destaque para pontos centrais de regulação das plataformas, surgiram muitas críticas, pois, logo após a entrada em vigor, postagens que eram lícitas foram deletadas, fato que levantou preocupações para um possível *overblocking* (bloqueio excessivo) de publicações. Para combater esse tipo de situação, defende-se que as plataformas devem adotar um sistema de transparência e de procedimento auditáveis.[61]

Em cumprimento à legislação alemã, a *Google* vem emitindo relatórios de transparência a cada 6 meses explicando o procedimento para remoção de conteúdo na plataforma. Uma vez recebida a denúncia com base na *NetzDG*, o provedor realiza análise e, se constatada que há violação, o conteúdo é bloqueado. Segundo o relatório de transparência, entre o período de julho a dezembro de 2022, foram recebidas 233.440 denúncias no *YouTube*, sendo que 32.150 foram removidos com base na lei alemã. Ou seja, 97,79% dos itens denunciados com base na lei alemã não foram identificados como ilegais.[62]

Vale destacar, ainda, que o *YouTube* adotou medidas para facilitar a denúncia de conteúdos pela plataforma, de modo que deixou de exigir que o usuário identifique o tipo penal violado. Em contrapartida, o *Facebook* optou por direcionar o usuário para a página de suporte para que seja realizada a denúncia, devendo ser indicado o tipo penal e o *link* da publicação. De todo modo, as duas plataformas adotaram um regime de verificação do

58 CUEVA, Ricardo Villas Boas. Alternativas para a remoção de fake news nas redes sociais. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 275.

59 ALEMANHA. Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, Vom 30. März 2021.

60 EIFERT, Martin. A Lei Alemã para a Melhoria da Aplicação da Lei nas Redes Sociais (NetzDG) e regulação da plataforma. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 168 e 169.

61 CUEVA, Ricardo Villas Boas. A lei alemã para a melhoria da aplicação da lei nas redes sociais (NetzDG). In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 275.

62 GOOGLE. Remoções de acordo com a Lei aplicável a redes. Disponível em https://transparencyreport.google.com/netzdg/youtube?hl=pt_BR. Acesso em 30 maio 2023.

conteúdo com base nas diretrizes internas e, posteriormente, com a lei alemã, a fim de que fosse evitado bloqueio de publicações sem caráter violador.[63]

Apesar da transparência nos relatórios e as medidas adotadas pelas plataformas para evitar *overblocking* de publicações não violadoras, assim que a lei alemã entrou em vigor, ocorreram bloqueios de publicações que estavam em conformidade com as diretrizes.[64] Ainda, o modelo alemão é alvo de críticas na medida em que atribui às redes sociais a responsabilidade de remoção de conteúdo com base em tipos penais, tendo poder para interpretar o que é ilegal ou não.[65] Segundo o *Facebook*, denúncias relacionadas à difamação começaram a ser feitas com base na lei, de modo que a rede social passou a ter que analisar quais publicações eram mero insulto e quais seriam criminosas.[66] Esse fato motivou a *Meta* a criar do *Oversight Board*, um órgão independente e com orçamento próprio que analisa reclamações de usuários que discordam das decisões tomadas em relação aos conteúdos do *Facebook* e *Instagram*.[67]

Sem desconsiderar as críticas à lei alemã, o modelo de autorregulação tem se tornado cada vez mais um atrativo, pois tende a ser mais ágil na identificação e remoção de conteúdos ilícitos sem depender de qualquer tipo de ordem judicial.[68]

CONSIDERAÇÕES FINAIS

A *Deepfake Ponography* se tornou uma preocupação em escala mundial. O aperfeiçoamento da inteligência artificial, através da manipulação de recursos audiovisuais, possibilitou a criação de conteúdo que, aos olhos humanos, não é possível distinguir se o conteúdo é ou não verdadeiro. O fácil acesso às ferramentas que produzem a pornografia usando imagem de mulheres sem consentimento ocasionou na perda de controle da inteligência artificial pelos criadores e se tornou uma ferramenta de opressão

63 BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileita. **Revista Direito FGV**. v. 19, publicado em 14/03/2023. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/89111. Acesso em: 30 maio 2023. p. 20.

64 EIFERT, Martin. A Lei Alemã para a Melhoria da Aplicação da Lei nas Redes Sociais (NetzDG) e regulação da plataforma. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 162.

65 BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileita. **Revista Direito FGV**, v. 19, publicado em 14/03/2023. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/89111. Acesso em: 30 maio 2023. p. 21.

66 "You may be surprised but the most commonly reported issues on the NetzDG pages are in fact defamation of a person or insult. The law aimed to fight hate and violence, but you mostly get complaints, for example, of someone reported for commenting about dirty towels in a gym club. The owner would define that as defamation of his fitness club" (FISS, Joelle; MCHANGAMA, Jacob. The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship. Disponível em: https://globalfreedomofexpression.columbia.edu/publications/the-digital-berlin-wall-how-germany-accidentally-created-a-prototype-for-global-online-censorship/. p. 4.)

67 META, Oversight Board. Disponível em: https://about.fb.com/news/tag/oversight-board/. Acesso em: 30 maio 2023.

68 CUEVA, Ricardo Villas Boas. Alternativas para a remoção de fake news nas redes sociais. In: ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 279.

às vítimas.

O ordenamento jurídico brasileiro, assim como outros países, não tem leis específicas que regulamentam o uso da inteligência artificial ou que criminalizam as *Deepfakes* que geram conteúdo pornográfico, mas existem dispositivos norteadores para amparar as vítimas dessa prática.

Primeiro, o uso indevido de imagem de mulheres sem consentimento caracteriza violação do direito de imagem e honra, fato que por si só já gera o dever de indenizar. Em segundo plano, o Marco Civil da Internet, lei que serve para regulamentar o uso da Internet no Brasil, estabelece que o meio virtual não é espaço para informações manipuladas, sob pena de comprometer o ambiente democrático e o exercício da cidadania. O conteúdo que ofende à honra alheia pode ser, portanto, removido.

Pelo que dispõe o MCI, no artigo 19, em regra, é necessária ordem judicial específica para remover conteúdo que ofenda à honra, fato que obriga a vítima a provocar o poder judiciário para obter a tutela de seus direitos. Se por um lado o tramite de um processo pode levar mais de ano, o conteúdo publicado nas redes sociais pode tomar proporções globais em minutos e sair do controle dos seus criadores, causando danos imensuráveis para a honra e dignidade da vítima. A exceção à regra é o artigo 21 do MCI, que possibilita a remoção de conteúdo pornográfico através de envio de notificação.

É visando contornar a necessidade de interferência do poder judiciário, bem como promover maior rapidez na remoção de conteúdo, que as plataformas digitais estipularam diretrizes e políticas da privacidade que servem de regras para regulação dos conteúdos postados, ou seja, a publicação que não estiver em conformidade com as políticas será bloqueada.

Ainda nesse sentido, a Alemanha se tornou referência mundial com a entrada em vigor da lei *NetzDG*, que possibilita a autorregulação das plataformas digitais e estabelece prazo de 24 horas para remoção de conteúdo após simples notificação, sob pena de multa, além da obrigatoriedade de divulgação de relatórios de transparência. Com isso, a Alemanha encontrou uma solução para remoção e bloqueio de conteúdo ilícito em curto prazo e sem necessidade de atuação das vias judiciais. O objetivo era maior celeridade e transparência e isso foi atingido.

A *NetzDG*, entretanto, foi alvo de uma série de críticas. O que se temia, é que a lei alemã pudesse dar margem para *overblocking* de publicações que estivessem em conformidade com a legislação e, logo após a entrada em vigor da lei, isso realmente aconteceu. Ainda, foi identificado grande número de denúncias sobre conteúdos que não infringiam a legislação, cabendo aos provedores a responsabilidade de interpretar quais publicações se enquadrariam em qual tipo penal, fato que gera margem para interpretações equivocadas.

Por fim, vale destacar que a possibilidade de autorregulação não anula ou exclui a importância do poder judiciário, que exerce papel fundamental de garantidor dos direitos individuais, como direito à imagem. No mais, para fins de responsabilização cível e reparação dos danos causados pelas *Deepfakes*, a necessidade de provocação do judiciário é essencial. Em se tratando de internet, o poder público precisa atuar em conjunto com as plataformas digitais para combater conteúdos manipulados, especialmente *Deepfake Ponography*, visando minimizar danos causados às vítimas e remover o conteúdo de forma rápida e efetiva.

REFERÊNCIAS DAS FONTES CITADAS

ABBOUD, Georges; NERY JÚNIOR, Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2. ed. São Paulo: Thomson Reuters, 2020.

ALIAGA, V. Henry Cavill é o James Bond perfeito em vídeo deepfake. **IGN Brasil**, 02 nov. 2021. Disponível em: https://br.ign.com/henry-cavill/94131/news/henry-cavill-james-bond-perfeito-video-deepfake. Acesso em 29 maio 2023

ARTIFICIAL Intelligence Coined at Dartmouth. **Dartmouth College**, Hanover. Disponível em: https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth. Acesso em: 29 maio 2023.

BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021.

BITTAR, Carlos Alberto. **Os direitos da Personalidade**. 6. ed., rev., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileita. **Revista Direito FGV**. v. 19, publicado em 14/03/2023. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/89111. Acesso em: 30 maio 2023.

COPELAND, B. J. Alan Turning and the beginning of AI. *Britannica*. Disponível em: https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI. Acesso em: 29 maio 2023.

CRUZ, Francisco Brito; SILVEIRA, Hélio Freitas de Carvalho da; ABREU, Jacqueline de Souza; ANDRADE, Marcelo Santiago de Paduá; VIEIRA, Rafael Sonda; OLIVA, Thiago Dias. **Direito Eleitoral na Era Digital**. Belo Horizonte: Casa do Direito, 2018.

DEEPTRACE. **The State of Deepfakes**: Landscape, Threats, and Impact. Amsterdã: Deeptrace, 2019. Disponível em: https://sensity.ai/reports/. Acesso em: 14 maio 2023

DUFFY, Ryan. Pornographic "Deepfake Ecosystem" on Telegram Uncovered by Sensity. **Tech Brew**, 02 nov. 2020. Disponível em: https://www.emergingtechbrew.com/stories/2020/11/02/pornographic-deepfake-ecosystem-telegram-uncovered-sensity. Acesso em: 30 maio 2023.

ESTRUTURA orgânica do STF passa a contar com setor voltado a inteligência artificial. **STF Notícias**, Brasília, 27 dez. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalh e.asp?idConteudo=499690&ori=. Acesso em: 29 maio 2023.

EUROPEIA, Comissão. *Código de Conduta para a luta contra os discursos ilegais de incitação ao ódio em linha.* Disponível em: https://commission.europa.eu/document/551c44da-baae-4692-9e7d-52d20c04e0e2_pt. Acesso em: 09 maio 2023.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**, volume 1: parte geral. 16. ed. São Paulo: Saraiva Educação, 2018.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital***:* transformação digital: desafios para o direito. 2. ed. Rio de Janeiro: Forense, 2022.

HOW TO DETECT A DEEPFAKE ONLINE: Image Forensics and Analysis of Deepfake Videos. Disponível em: https://sensity.ai/blog/deepfake-detection/how-to-detect-a-deepfake/. Acesso em: 08 mar. 2022.

LEAH, D. O que diz o casaco de Inteligência Artificial do Papa Francisco sobre o futuro da moda. **CNN Portugal**, Lisboa, 02 abr. 2023. Disponível em: https://cnnportugal.iol.pt/inteligencia-artificial/papa-francisco/o-que-diz-o-casaco-de-inteligencia-artificial-do-papa-francisco-sobre-o-futuro-da-moda/20230402/642412160cf2c84d7fcedfe5. Acesso em: 29 maio 2023.

LIMA, E. K. Sistema de reconhecimento facial da PF é "preocupante e ilícito", afirmam especialistas. **Olhar Digital**, 13 jul. 2021. Disponível em: https://olhardigital.com.br/2021/07/13/seguranca/sistema-de-reconhecimento-facial-da-pf-e-preocupante-e-ilicito-afirmam-especialistas/. Acesso em: 30 maio 2023.

MARQUES, C. L.; MARTINI, S. R.; FINCO, M. (org). **Diálogos entre direitos humanos, direito do consumidor, compliance e combate à corrupção**. 1. ed. São Paulo: YK Editora, 2021.

MASSO, F. D.; ABRUSIO, J.; FLORÊNCIO FILHO, M. A. (coord.). **Marco Civil da Internet**: lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais Ltda., 2014.

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

MORAES, Alexandre de. **Direito constitucional***:* atualizado até a EC 115, de 10.02.2022. 38. ed. Barueri: Editora Atlas, 2022.

MONTENEGRO, M. C. Inteligência Artificial: Trabalho judicial de 40 minutos pode ser feito em 5 segundos. **Agência CNJ de Notícias**, Brasília, 23 out. 2018. Disponível em:

https://www.cnj.jus.br/inteligencia-artificial-trabalho-judicial-de-40-minutos-pode-ser-feito-em-5-segundos/. Acesso em: 29 maio 2023.

MUELLER, John Paul; MASSARON, Lucas. **Aprendizado profundo para leigos**. Rio de Janeiro: Alta Books, 2020.

PACETE, L. Bom uso de Deepfake amplia horizontes para o marketing, saúde e entretenimento. **Forbes**, 03 dez. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/12/bom-uso-da-deepfake-amplia-horizontes-para-o-marketing-e-os-negocios/. Acesso em 29 maio 2023

PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 20 maio 2022.

PINTO, Felipe Chiarello de Souza; SOUZA JÚNIOR, Arthur Bezerra de. Limites da Liberdade de Expressão no Espaço Virtual: a questão Fake News. *In:* LÓSSIO, C. J. B.; NASCIMENTO, L.; TREMEL, R. (org.). **Cibernética Jurídica***:* Estudos sobre Direito Digital. Campina Grande: EDUEPB, 2020. p. 142-154.

RAIS, Diogo; FALCÃO, Daniel; GIACCHETTA, André Zonaro; MENEGUETTI, Pamela. **Direito Eleitoral Digital**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

RAIS, Diogo. **Fake News**: a conexão entre a desinformação e o direito. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 25-52.

SERVICE, European Parliamentary Research. Tackling deepfakes in European policy. *In:* PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY, 2021, Estrasburgo, *Relatório* [...]. Estrasburgo: European Parliament, jul. 2021. p. 1-95. Disponível em: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690039. Acesso em 30 maio 2023.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Editora Atlas, 2014. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493449/. Acesso em: 10 maio 2022.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil***:* da erosão dos filtros da reparação à diluição dos danos. 5. ed. São Paulo: Editora Atlas, 2013.

SCHREIBER, Anderson; MORAES, Bruno Terra de; TEFFÉ, Chiara Spadaccini de. (coord.) **Direito e Mídia**: tecnologia e liberdade de expressão. 2. ed. Indaiatuba: Editora Foco, 2022.

SOARES, Flaviana Rampazzo. Levando Algoritmos a Sério. *In:* BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

THE making of 'The Noble Speech'. **Direção e produção**: The Womanity Foundation. Grand-Lancy: The Womanity Foundation, 2022. 1 vídeo. Disponível em: https://www.youtube.com/watch?v=f7DhJ9dhGmY. Acesso em 29 maio 2023

COMO CITAR:

PINTO, Felipe Chiarello de Souza; OLIVEIRA, Gabriela Franklin de. Não acredite em tudo que vê: *Deepfake Pornography* e responsabilidade civil no ordenamento jurídico brasileiro. **Revista Direito e Política**. Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, vº 18, nº 2, 2º quadrimestre de 2023. Disponível em: https://periodicos.univali.br/index.php/rdp - ISSN 1980-7791. DOI: https://doi.org/10.14210/rdp.v18n2.p404-426

INFORMAÇÕES DOS AUTORES:

Felipe Chiarello de Souza Pinto
Mestre e Doutor em Direito pela PUC/SP. Professor Titular da Faculdade de Direito e do PPGD da Universidade Presbiteriana Mackenzie, onde foi Diretor e atualmente é Pró-Reitor de Pesquisa e Pós-Graduação. Professor Colaborador do PPGD/UPF e Bolsista de Produtividade e Pesquisa do CNPq.

Gabriela Franklin de Oliveira
Pós-graduanda em Processo Civil pela Fundação Getúlio Vargas/SP. Bacharel em direito pela Universidade Presbiteriana Mackenzie. Advogada.

Received: 30/04/2022
Approved: 10/04/2023

Recebido em: 30/04/2022
Aprovado em: 10/04/2023