III ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

DANIELLE JACON AYRES PINTO

HENRIQUE RIBEIRO CARDOSO

AIRES JOSE ROVER

D597

Direito, governança e novas tecnologias III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Henrique Ribeiro Cardoso – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-321-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: segurança humana para a democracia

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Governança. 3. Novas tecnologias. III Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

III ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

No III Encontro Virtual do CONPEDI, realizado de 23 a 28 Junho de 2021, o grupo de trabalho "Direito, Governança e Novas Tecnologias III", que teve lugar na tarde de 25 de junho de 2020, foi o promotor de debates profundos e estruturantes sobre esse tema tão instigante e contemporâneo. Ao longo de GT foram apresentados trabalhos de alta qualidade produzidos por doutores, pós-graduandos e graduandos. Vale ressaltar nesse GT a potencialidade e alegria de ver a diversidade de gênero sendo efetivada entre os participantes, homens e mulheres elevaram de forma significativa a qualidade dos estudos jurídicos que versam sobre as novas tecnologias e os processos de governança, num esforço efetivo para promover de práticas justas e democráticas frente às novas tecnologias e à sua influência no mundo do direito.

Ao total foram apresentados 16 artigos que tiveram comentários dos coordenadores e do público presente como assistência na sala virtual do GT.

Esse rico debate demonstra a inquietude que os temas estudados despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em Direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõem a enfrentar os desafios que as novas tecnologias impõem ao Direito e a toda a sociedade. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em três blocos, quais sejam: a) inteligência artificial e os perigos do uso das novas tecnologias; b) Desinformação, internet e privacidade; e c) governo eletrônico e seus processos de governança impulsionados pela pandemia de COVID-19.

O bloco inicial dedicou-se a pensar a inteligência artificial e os perigos do uso das novas tecnologias. Nesse espaço foram debatidos os seguintes temas: "Risco e internet"; "Os limites éticos do uso da IA no Judiciário"; "Avanço da IA na atividade jurisdicional"; "Gestão de Departamentos Jurídicos e data drive"; "Governança algorítmica" .

No segundo bloco os temas ligados a desinformação, internet e privacidade foram os principais em debate, com temas como: "A proteção dos direitos da personalidade nos negócios jurídicos das lawtechs"; "O capitalismo de vigilância e a necessidade de uma ética para os avanços tecnológicos"; "Deepfake e a desinformação"; "A exploração da autonomia na sociedade da informação"; "A governança e o registro de dados em LGPD sob a ótica da

tomada de decisão estratégica"; "O direito fundamental à privacidade no governo digital"; "A lei geral de proteção de dados pessoais – nível de adequação nas operadoras de plano de saúde".

No terceiro e derradeiro bloco, os trabalhos tiveram o intuito de debater o governo eletrônico e seus processos de governança impulsionados pela pandemia de COVID-19 com os temas: "Responsabilidade social, governança corporativa e compliance"; "O governo digital e a nova roupagem da administração pública: o empurrão dado pela crise atual da pandemia de covid-19"; "Direito à informação correta e a covid-19"; "Legal design como mecanismo de acesso à justiça"; "Mundo V.U.C.A. e saúde global".

Todos os artigos apresentados nesse GT tiveram como função fomentar a pesquisa de qualidade e fortalecer o diálogo interdisciplinar em torno dos temas do direito, novas tecnologias e processos de governança. Tais produções são resultados claros do aumento de importância desses temas para os programas de pós-graduação na área jurídica, motivados pela cada vez maior inserção do mundo virtual na vida cotidiana dos cidadãos e da necessidade de buscar transformações e adequações legais efetivas para satisfazer as demandas da sociedade nesse mundo em transformação.

Os Coordenadores

Prof. Dr. Aires José Rover

Profa. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Henrique Ribeiro Cardoso

DEEPFAKE E A DESINFORMAÇÃO: AMEAÇAS EM ÉPOCA DE PANDEMIA

DEEPFAKE AND DISINFORMATION: THREATS IN THE TIME OF PANDEMIA

Jéssica Amanda Fachin [1]
Tatiane Magalhães Barreto Fontes Lermen Eidt [2]

Resumo

O presente artigo aborda o Deepfake, que se apresenta na atualidade como uma nova ameaça à sociedade, principalmente em época de pandemia em que se verifica o compartilhamento massivo de notícias falsas relativas à crise sanitária. A investigação dessa tecnologia tem por escopo verificar de que modo ela opera no meio virtual e, desse modo, apresentar possíveis mecanismos jurídicos que dificultem ou inibam o compartilhamento de informações falsas.O trabalho fundamenta-se no método hipotético-dedutivo, baseado na revisão bibliográfica de textos de literatura especializada, de legislação, de dados estatísticos, de artigos, notícias e demais dados colhidos sobre o tema.

Palavras-chave: Deepfake, Desinformação, Deep learning,, Inteligência artificial,, Tecnologia

Abstract/Resumen/Résumé

This article deals with Deepfake, which presents itself today as a new threat to society, especially in a time of pandemic when there is a massive sharing of false news related to the health crisis. The investigation of this technology aims to verify how it operates in the virtual environment and, therefore, to present possible legal mechanisms that hinder or inhibit the sharing of false information. The work is based on the hypothetical-deductive method, based on the bibliographic review of specialized literature texts, legislation, statistical data, articles, news and other data collected on the topic.

Keywords/Palabras-claves/Mots-clés: Deepfake, Misinformation, Deep learning, Artificial intelligence, Technology

[1] Doutora em Direito Constitucional (PUCSP). Mestre em Ciência Jurídica (UENP). Coordenadora de Pós-Graduação (IDCC). Professora no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina. ORCID: 0000-0003-0486-7309.

[2] Mestranda no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina. Especialista em Direito e Processo do Trabalho pela PUC-RS.

1 Introdução

Os avanços tecnológicos possibilitaram grandes mudanças no cotidiano, ao alterar os hábitos da sociedade, de modo que a interação entre as pessoas ficou cada vez mais inumana, mais através de dispositivos eletrônicos. Dessa forma, o contato mais pessoal foi gradualmente deixado de lado e as máquinas foram tomando o lugar. Além disso, para agravar a situação, veio a pandemia do coronavirus e ajudou mais ainda nesse processo de distanciamento das pessoas.

Assim, esse cenário fica muito propício à disseminação de *fake news*, com o incentivo à população a não seguir as normas sanitárias, a não tomar vacinas, a consumir medicamentos ineficazes. Ou seja, com o estímulo a atos egoístas, que põem em risco a própria vida e a vida das outras pessoas. Essa disseminação da desinformação não é algo recente, já ocorria em tempos passados, mas na proporção que se vê hoje é algo preocupante, principalmente no âmbito da saúde, pois agora pode contar com a ajuda das novas tecnologias.

O desenvolvimento da tecnologia fez surgir o *deepfake*, que é um avanço tecnológico das *fake news*. Esse recurso, com a sua popularização, está ficando mais acessível a cada dia. Assim, torna-se uma nova ameaça para a sociedade, principalmente no contexto de pandemia, vivido atualmente, ao ajudar na disseminação da desinformação.

Deste modo, utilizando-se do método hipotético-dedutivo, através da pesquisa bibliográfica e documental, estudar-se-á, o assunto, ao dividi-lo em três seções. Primeiramente analisar-se-á a conceituação da Inteligência Artificial, com um enfoque no estudo do que seria o *Deepfake*. Em um segundo momento, analisar-se-á a relação do *Deepfake* com a desinformação Já em um terceiro momento, examinar-se-ão os métodos de combate ao *Deepfake*, com especial abordagem aos mecanismos jurídicos que poderiam ser aplicados para dificultar ou inibir o compartilhamento de informações falsas, observando-se o Direito brasileiro e o Direito comparado.

2 Inteligência Artificial

A sociedade passou por três Revoluções Industriais e, hoje, considera-se que está na Quarta Revolução Industrial (Indústria 4.0). Essa última Revolução Industrial começou a ser discutida na Alemanha, em 2011, e tem como marco a integração entre o mundo virtual e o real, através de tecnologias como, por exemplo, a Realidade Aumentada, a *Internet* das

Coisas, a Realidade Virtual e o *Big Data*.[1] No entanto, muitos países não estão no mesmo momento de revolução, ainda passam por momentos anteriores, como é o caso do Brasil[2] (GOEPIK, 2019, *online*).

As Revoluções Industriais iniciais diferem-se das novas tecnologias da informação, no sentido em que antes seus ritmos de evolução eram muito lentos, comparados ao desenvolvimento na atualidade, com a duração de século, e em lugares específicos. Já as novas tecnologias da informação se propagaram com uma velocidade impressionante, principalmente em meados dos anos 70 e 90, com o desenvolvimento computacional, dessarte, em menos de duas décadas, conectando o mundo. (CASTELLS, 2002, p. 70)

A atual revolução tecnológica caracteriza-se pela constante disseminação de informação e, desse modo, geração de conhecimento, que se auto aplica em um ciclo de realimentação cumulativo, assim, com o foco na aplicação desses conhecimentos (com o cerne: tecnologias da informação, processamento e comunicação). Essa Sociedade da Informação e do Conhecimento, derivada da atual revolução, utiliza a mente como uma força direta de produção, pela primeira vez na história, logo, não se resume a uma ferramenta no processo produtivo (CASTELLS, 2002, p. 68 e 69).

Com essas constantes mudanças tecnológicas, surgiu um novo campo de estudos, o qual modificou todo um pensamento vigente até aquele momento, oferecendo, assim, uma visão de futuro. As pesquisas sobre a Inteligência Artificial iniciaram-se depois da Segunda Guerra Mundial, quando várias pessoas começaram a trabalhar de forma independente em máquinas inteligentes (MCCARTHY, 2007, p. 4).

Apesar disso, Alan Turing, matemático inglês, pode ser considerado como o primeiro a pesquisar sobre esse assunto, já que, em 1947, ele deu uma palestra sobre a tecnologia referenciada, e, provavelmente, foi o primeiro a decidir que a I.A. era melhor pesquisada ao se fazer programações de computadores e não ao se construir máquinas. Assim, ao final da década de 50, já havia muitos pesquisadores de I.A., e a maioria deles estava focando seus trabalhos em programação de computadores (MCCARTHY, 2007, p. 4).

Já o termo Inteligência Artificial surgiu quando o professor de Ciência da Computação da Universidade de Stanford, John McCarthy, o empregou, pela primeira vez, em uma carta, em 1955. Essa carta era um convite para uma conferência sobre a I.A., que se realizou em

[1] Nesse sentido, ver: SCHWAB, Klaus. **A Quarta Revolução Industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

[2] Considera-se que o Brasil ainda está em transição entre a Segunda Revolução Industrial e a Terceira Revolução Industrial. Dessa forma, até o presente momento, não se pode falar em uma Quarta Revolução Industrial acontecendo (GOEPIK, 2019, *online*).

1956, endereçada a nomes lendários da computação como Marvin Minsky, Nathaniel Rochester e Claude Shannon (ÉPOCA NEGÓCIOS ONLINE, 2019, *online*; MCCARTHY, 2007, p. 2).

Para McCarthy (2007, p. 2), o conceito de Inteligência Artificial perpassa o objetivo de criar máquinas inteligentes mais parecidas com o ser humano, quanto a sua racionalidade, assim, ele define a I.A. como:

> É a ciência e a engenharia de fazer máquinas inteligentes, especialmente programas de computador inteligentes. Está relacionado à tarefa semelhante de usar computadores para entender a inteligência humana, mas a IA não precisa se confinar a métodos biologicamente observáveis (MCCARTHY, 2007, p. 2, tradução nossa).

Ainda, é relavante mencionar que o mesmo autor conceitua o que seria somente a Inteligência, e observa uma dificuldade nessa definição, já que até o presente momento esse campo de pesquisas se apresenta bastante incipiente:

> Inteligência é a parte computacional da habilidade de atingir objetivos no mundo. Vários tipos e graus de inteligência ocorrem em pessoas, muitos animais e algumas máquinas. [...]
> O problema é que ainda não podemos caracterizar em geral quais tipos de procedimentos computacionais queremos chamar de inteligentes. Nós entendemos alguns dos mecanismos de inteligência e não outros (MCCARTHY, 2007, p. 2 e 3, tradução nossa).

Villani (2018, p. 6) lançou, em seu relatório, um olhar sobre o que seria a Inteligência Artificial e o seu contexto:

> Definir inteligência artificial (AI) não é fácil. O campo é tão vasto que não pode ficar restrito a uma área específica de pesquisa: é um programa multidisciplinar. Originalmente, buscou imitar os processos cognitivos dos seres humanos. Já atualmente, seus objetivos são desenvolver autômatos que resolvam alguns problemas melhor do que os humanos, por todos os meios disponíveis (VILLANI, 2018, p. 6, tradução nossa).

A I.A., com o passar do tempo, foi cada vez mais estudada e polemizada, mas sua definição, como já referido, mesmo com os inúmeros estudos já feitos e os que estão em progresso, ainda não é tão fácil de ser conceituada, já que envolve muitas áreas de pesquisa, apresentando-se como um campo multidisciplinar:

> A IA está na encruzilhada de várias disciplinas: ciência da computação, matemática (lógica, otimização, análise, probabilidades, álgebra linear) e ciências cognitivas, isso sem falar no conhecimento especializado dos campos aos quais queremos aplicá-lo. Os algoritmos que o sustentam são baseados em abordagens igualmente variadas: análise semântica, representação simbólica, aprendizagem estatística e exploratória, redes neurais e assim por diante (VILLANI, 2018, p. 6, tradução nossa).

No relatório de Villani ainda é pontuado que os avanços recentes significativos na I.A. foram propiciados com o surgimento do *machine learning* (aprendizado de máquinas), que possibilitou uma maior independência da máquina em relação ao ser humano. Isso ocorreu devido a desnecessidade de uma programação ser realizada a cada futura tarefa executada, bastando um ajuste inicial para que, a partir daquele momento, a máquina descobrisse as regras por si mesma (VILLANI, 2018, p. 6).

Além disso, o relatório aponta as várias facetas, em que a Inteligência Artificial se reveste na vida cotidiana, para o bem e para o mal da sociedade, proporcionado pelo acesso e o poder de armazenamento de dados pela evolução da computação:

> A IA também está se desenvolvendo rapidamente devido à "dataização" internacional de todos os setores (ou seja, *big data*) e ao aumento exponencial no poder de computação e nas capacidades de armazenamento de dados. Os aplicativos estão se multiplicando e afetando diretamente nossas vidas diárias: reconhecimento de imagem, carros autônomos, detecção de doenças e recomendação de conteúdo são algumas das muitas possibilidades que estão sendo exploradas. A natureza universal da IA e suas muitas variações anunciam uma nova revolução, com sua parcela de armadilhas e oportunidades. (VILLANI, 2018, p. 6, tradução nossa)

Apesar das dificuldades de conceituação, Cossetti (2018, *online*) define a Inteligência Artificial como a capacidade das máquinas de pensar de forma racional como os seres humanos, com as funções de aprender, perceber e decidir quais caminhos seguir diante de determinadas situações, com a imitação, desse modo, das funções cognitivas dos humanos.

Para chegar nesse nível de desenvolvimento e tornar a I.A. finalmente possível foi preciso contar com a fórmula: *big data* + computação em nuvem + bons modelos de dados. Essa fórmula surgiu da evolução de três grandes pilares:

> - Bons modelos de dados para classificar, processar e analisar;
> - Acesso a grande quantidade de dados não processados;
> - Computação potente com custo acessível para processamento rápido e eficiente (COSSETTI, 2018, *online*).

Isso tornou factível a evolução da computação simples para a atual, da Inteligência Artificial. Ademais, para conseguir ter essa cognição racional mais próximo do ser humano a I.A. tem três tecnologias principais que permitem o seu funcionamento - *Machine Learning*, *Deep Learning* e Processamento de Linguagem Natural (PLN):

> *Machine Learning*:
> Em vez de programar regras para uma máquina e esperar o resultado, conseguimos deixar que a máquina aprenda essas regras por conta própria a partir dos dados, chegando ao resultado de forma autônoma. As recomendações personalizadas na Netflix e na Amazon, por exemplo, indicam os títulos de acordo com o que o usuário assiste. Conforme você inclui dados (assiste) o sistema aprende o que você gosta (COSSETTI, 2018, online).

O *Deep Learning* significa aprendizado profundo, já que há a análise de camadas mais profundas e, assim, a possibilidade da realização de tarefas mais complexas e de respostas mais precisas aos desafios postos:

> *Deep Learning*:
> Quando falamos de aprendizado profundo, estamos nos referindo à uma parte do aprendizado de máquina que utiliza algoritmos complexos para "imitar a rede neural do cérebro humano" e aprender uma área do conhecimento com pouco ou sem supervisão. O sistema pode aprender como se defender de ataques, sozinho (COSSETTI, 2018, online).

Já o PLN é usado como se fosse um tradutor para a máquina entender a linguagem do ser humano e, assim, elaborar as devidas respostas, por meio de textos ou áudio:

> Processamento de Linguagem Natural:
> Esse processamento utiliza as técnicas de machine learning para encontrar padrões em grandes conjuntos de dados puros e reconhecer a linguagem natural. Assim, um dos exemplos de aplicação do PLN é a análise de sentimentos, onde os algoritmos podem procurar padrões em postagens de redes sociais para compreender como os clientes se sentem em relação a marcas e produtos específicos (COSSETTI, 2018, online).

Dessas 3 tecnologias, o *Deep Learning* - que é o aprofundamento do *Machine Learning*, pois usa redes neurais mais complexas, com muitas camadas, assim, com um entendimento mais detalhado dos pensamentos humanos - é a tecnologia utilizada para a criação do *Deepfake*. Essa técnica é uma evolução das metodologias de aperfeiçoamento de Inteligência Artifical.

2.1 O que é *Deepfake*?

Deepfake é a junção de duas expressões: *Deep Learning* (aprendizado profundo) e *fake* (falso). Essa técnica, que é considerada um avanço tecnológico das *fake news*, consiste na criação de vídeos falsos, com a utilização do sistema de reconhecimento facial, ao substituir os rostos das pessoas e sincronizar seus movimentos labiais e expressões, colocando elas para agirem e falarem de um modo como nunca fizeram na vida real (SILVA, 2019, *online*).

Ele se distingue do *shallow fake* (vídeo que não usa a I.A. para fazer a substituição de rostos, mas sim ferramentas de pós-produção como o *After Effects*) e da *dumb fake* (vídeo em que a montagem é feita de maneira muito grosseira, isso evidencia a falsidade dele, mesmo que ocorra a troca de rostos) (SILVA, 2019, *online*). No entanto, como ainda é uma tecnologia muito recente, sua definição é fluida.

Rostos e cenas criadas no audiovisual por efeitos especiais de computador não são novidades, já que na indústria do cinema isso já ocorria há um tempo como, por exemplo, quando o diretor James Cameron, no clássico Avatar, coloca o rosto dos atores Sam Worthington e Zoe Saldana nos gigantes azuis criados por computador. Além disso, outro exemplo é no processo que permite rejuvenescer atores de maneira muito convincente (usado em Samuel L. Jackson no filme Capitã Marvel e em Al Pacino e Robert de Niro no filme The Irishman) (SILVA, 2019, *online*).

Apesar disso, as tecnologias usadas em Hollywood e no *Deepfake* são diferentes, pois naquela há a necessidade da experiência humana, ao utilizar-se modelos 3D. Já neste, como há a utilização de imagens, com o processamento pela técnica do *Deep Learning*, dispensa-se a experiência humana (DODGSON, 2018, *online*).

Ademais, um interessante panorama é apresentado por Hao Li, professor de Ciência da Computação na Universidade do sul da Califórnia, com a observação do início do *Deepfake* nos anos 90, depois o surgimento da fama por volta de 2014 e, por fim, a sua popularidade em 2017 (BATTAGLIA, 2020, *online*).

Assim, em dezembro de 2017, quando um usuário do Reddit, que se autodenominava "*deepfakes*", começou a utilizar a tecnologia de *Deepfake* para postar vídeos falsos de celebridades, como as atrizes Gal Gadot e Emma Watson, em situações sexuais comprometedoras, essa técnica veio à tona e se tornou cada vez mais comum com o passar dos anos (CABRAL, 2018, *online*).

O *Deepfake*, como já visto, é um tipo de vídeo que utiliza técnicas parecidas, mas não iguais, aos efeitos especiais de Hollywood, ao inserir digitalmente no audiovisual uma pessoa

que originalmente não faz parte dele. Atualmente, o maior uso dessa tecnologia é na indústria pornográfica, que utiliza o *Deepfake* para inserir o rosto das celebridades nos corpos de atrizes e atores pornôs, criando, assim, vídeos falsos de sexo. Além disso, ela também é utilizada, em menor escala que no primeiro caso, para a criação de conteúdos humorísticos e alguns discursos políticos falsos (SILVA, 2019, *online*).

Para a criação do *Deepfake*, Silva analisa como é feito o processo:

> A técnica mais usada para esse tipo de vídeo é a chamada "troca de cabeças", que consiste do uso de uma "pessoa-origem" (a pessoa que você quer inserir no vídeo) e de uma "pessoa-destino", cuja imagem será substituída pela da "pessoa-origem". Assim, com o uso de *softwares* específicos que utilizam algoritmos de inteligência artificial (IA), é possível transferir o rosto da "pessoa-origem" para o corpo da "pessoa-destino" de forma que pareça que a "pessoa-origem" realmente faz parte do vídeo, com uma dose assustadora de realismo (SILVA, 2019, *online*).

Ele continua com uma abordagem mais específica da técnica referida:

> Para fazer essas montagens, o *software* usado para isso cria um modelo 3D do rosto que se pretende inserir no vídeo, e então utiliza diversas equações matemáticas para calcular "pontos de contato" entre o modelo o rosto da pessoa-origem e o da pessoa-destino, fazendo assim as modificações necessárias para se efetuar o "transplante" de rosto. (SILVA, 2019, *online*)

Ainda, acrescenta à explanação como funciona o algoritmo *anti deepfake*, utilizado em uma das etapas do processo de criação do *Deepfake*:

> Após esse processo, o programa roda um algoritmo "anti *deepfake*", que faz a análise da transposição de rosto e marca os pontos onde essa transposição está mal-feita: ou seja, pontos onde fica claro que o olho humano consegue perceber que aquilo se tratou de uma montagem. O algoritmo de transposição então volta a trabalhar, ajustando esses pontos que foram marcados como problemáticos pela checagem, e esse processo se repete até que haja um equilíbrio entre ambos — até que o algoritmo de checagem não consiga mais detectar mais nenhum ponto problemático no vídeo. (SILVA, 2019, *online*)

Por fim, ele explica a atual necessidade de uma gama de dados, para a maioria dos programas existentes, com a finalidade de tornar o *Deepfake* cada vez mais real para quem assiste:

> Para que esses dois algoritmos consigam fazer seu trabalho de maneira adequada, é necessário que exista uma grande gama de "dados de treinamento" — ou seja, amostras de fotos e vídeo do rosto que se quer

> inserir no vídeo falso, pois quanto maior o número de amostras diferentes existentes sobre o mesmo rosto, mais pontos de comparação a IA terá para fazer a transposição, e mais real essa inserção digital será. É por isso que os principais alvos das *deepfakes* são políticos e celebridades, pois a natureza de suas profissões garante que haja uma enorme quantidade de fotos e vídeos públicos que podem ser usados para treinar a IA que irá desenvolver esses *deepfakes*. (SILVA, 2019, *online*)

Nesse sentido, Westerlund também detalha o procedimento da criação do *Deepfake* e suas particularidades:

> Quanto à tecnologia, *deepfakes* são o produto de *Generative Adversarial Networks* (GANs), ou seja, duas redes neurais artificiais trabalhando juntas para criar mídia de aparência real. Essas duas redes chamadas de "gerador" e "discriminador" são treinadas no mesmo conjunto de dados de imagens, vídeos ou sons. O primeiro tenta criar novos exemplos que sejam bons o suficiente para enganar a segunda rede, que trabalha para determinar se a nova mídia que vê é real. Dessa forma, eles impulsionam um ao outro a melhorar. Um GAN pode ver milhares de fotos de uma pessoa e produzir um novo retrato que se aproxima dessas fotos sem ser uma cópia exata de nenhuma delas (WESTERLUND, 2019, p. 2 e 3, tradução nossa).

Ainda, a autora continua a explanação sobre os GANs e apresenta um exemplo do que a tecnologia já consegue fazer:

> Em um futuro próximo, os GANs serão treinados com menos informações e serão capazes de trocar cabeças, corpos inteiros e vozes. Embora *deepfakes* geralmente exijam um grande número de imagens para criar uma falsificação realista, os pesquisadores já desenvolveram uma técnica para gerar um vídeo falso alimentando-o com apenas uma foto, como uma *selfie* (WESTERLUND, 2019, p. 3, tradução nossa).

Segundo Battaglia, nessa lógica apresentada por Westerlund, um programa da Samsung já consegue criar vídeos falsos com apenas uma imagem de referência. Aliás, no Zao, um aplicativo chinês que faz com que o seu rosto seja transportado para uma cena de filme ou série, basta tirar uma *selfie* para que isso ocorra (BATTAGLIA, 2020, *online*).

No caso do usuário do *Reddit*, segundo uma entrevista ao *site Motherboard*, foi utilizada uma API de *Deep Learning* escrita em linguagem *Python*, no caso o *TensorFlow* aliado ao *Keras* (*softwares* baseados em bibliotecas de código aberto voltadas ao aprendizado de máquina). Assim, quem programa a máquina fornece centenas e até milhares de fotos e vídeos das pessoas envolvidas, sendo elas automaticamente processadas por uma rede neural (CABRAL, 2018, *online*).

Esse processo se dá como um treinamento, em que o computador aprende como é determinado rosto, como ele se mexe e como ele reage a luz e às sombras, com dados do rosto do vídeo original e com o novo rosto. A partir daí, o treinamento só acaba quando o programa seja capaz de encontrar um ponto comum entre as duas faces e ligar uma sobre a outra. Dessa forma, o procedimento envolve uma espécie de truque, já que o *software* recebe a imagem da pessoa "A" e a processa como se fosse a pessoa "B" (CABRAL, 2018, *online*).

As máquinas utilizadas para a criação do *Deepfake* não necessitam mais ser extremamente avançadas. Hoje, com os avanços da tecnologia, essa técnica agora pode ser realizada em computadores domésticos, suficientes para rodar os jogos mais recentes e isso torna-se um problema já que, na atualidade, mais pessoas estão em contato com essa tecnologia utilizando-a para o bem e para o mal. Assim, como toda tecnologia, o problema do *Deepfake* não está na técnica em si, mas como ela será usada.

3 *Deepfake* e a Desinformação

As *fake news*[3] já são grandes problemas ao redor do mundo, ainda mais com a popularização das redes sociais[4], conhecidas como o grande mal da *internet* nos últimos cinco anos e que não devem sumir tão cedo, vindo a se agravar a cada dia. Essa questão é uma das principais preocupações das grandes empresas de tecnologia, governos e imprensa (SILVA, 2019, *online*).

O cenário atual de desinformação é bem avançado, já que se vive em uma época em que as pessoas têm alguma opinião formada sobre um assunto antes mesmo de procurar saber mais sobre ele. Então, nesse ambiente as notícias falsas são aceitas com mais facilidade, pois quando já se tem uma opinião formada sobre dado assunto, há uma maior propensão a ver as notícias não como fontes de informação, mas com uma visão de ataque ou de confirmação a sua "certeza" de mundo (SILVA, 2019, *online*).

Além disso, com os avanços da tecnologia, a iminente chegada do *Deepfake* promete complicar ainda mais uma situação já caótica. Atualmente, já é difícil conter as *fake news*, quanto mais o *Deepfake*, quando começar a ser mais comum o uso dessa ferramenta com o

[3] "Pesquisa global revela que 86% dos internautas já acreditaram em 'fake news'. O Centro para a Inovação em Governança Internacional, que fica no Canadá, entrevistou usuários de internet de 25 países" (AFP, 2019, *online*).

[4] "As plataformas de redes sociais foram apontadas como as principais responsáveis pela propagação de 'fake news' por uma maioria esmagadora (82%) dos consultados em uma pesquisa da Ipsos para o grupo de análise canadense Centro para a Inovação em Governança Internacional" (AFP, 2019, *online*).

objetivo de desinformar a população. Ainda que o *Deepfake* possa ser utilizado, por exemplo, em paródias humorísticas, em videoclipes[5] ou por alguém que tenha perdido a voz, os problemas que ele pode causar na sociedade são muitos e bem claros (SILVA, 2019, *online*).

Um dos grandes problemas será quando o *Deepfake* começar a ser usado para desinformar a sociedade acerca das medidas sanitárias, das vacinas, dos remédios, com a criação de vídeos de reportagens e pronunciamentos falsos e ao inserir rostos de autoridades da área da saúde, jornalistas conhecidos para passar credibilidade, assim, divulgando conhecimentos que não são verdadeiros, como se aqueles vídeos fossem reais. Isso contribuiria para a desinformação e para o caos na sociedade, com ameaças latentes, ainda mais em época de pandemia pelo coronavirus, quando esforços estão sendo feitos para a sua superação e pessoas estão utilizando mais as redes sociais, devido às situações de *lookdown* ao redor do mundo.

Dessa forma, com a chegada do *Deepfake*, isso poderá representar o início de uma era em que devemos desconfiar de basicamente tudo o que ouvimos e vemos nas mídias, até em conteúdos em vídeo, que é o que até hoje trazia uma maior segurança e credibilidade para a sociedade (SILVA, 2019, *online*).

Nessa linha, Westerlund aponta a questão da desconfiança gerada pelo *Deepfake* e pela propagação da desinformação:

> Os *deepfakes* provavelmente prejudicam a alfabetização digital e a confiança dos cidadãos em relação às informações fornecidas pelas autoridades, já que vídeos falsos que mostram funcionários do governo dizendo coisas que nunca aconteceram fazem as pessoas duvidar das autoridades. Na verdade, as pessoas hoje em dia são cada vez mais afetadas por *spam* gerado por IA e por notícias falsas que se baseiam em texto preconceituoso, vídeos falsos e uma infinidade de teorias da conspiração (WESTERLUND, 2019, p. 4 e 5, tradução nossa).

A autora ainda pontua as repercussões que a desconfiança, causada pela disseminação do *Deepfake*, pode ter nas pessoas:

[5] Um exemplo é que, agora, tem-se o primeiro videoclipe musical brasileiro que faz uso da técnica de *Deepfake*. "No caso, trata-se de 'Oooh (I Like It)!', do Tropkillaz, dupla formada pelos djs e produtores André Laudz (Laudz) e Zé Gonzales (Zegon). Lançado no dia 22 de janeiro de 2021, o videoclipe mostra a dupla em situações inusitadas, sendo que, na maioria das vezes, seus rostos foram incluídos em apresentações do Soul Train (programa de TV dos EUA da década de 1970, que contava com apresentações de grupos de música negra) e em vídeos de dança e ginástica antigos". Esse videoclipe "foi dirigido por Marco Loschiavo, e a parte de *Deepfake* foi criada pelo programador Leandro 'Na Prática' e o diretor de arte Fernando 3D - que, inclusive, trabalha com Bruno Sartori, famoso pelos seus *Deepfakes* do Presidente Jair Bolsonaro" (TAGIAROLI, 2021, *online*).

> No entanto, o aspecto mais prejudicial dos *deepfakes* pode não ser a desinformação em si, mas sim como o contato constante com a desinformação leva as pessoas a sentir que muita informação, incluindo vídeo, simplesmente não é confiável, resultando em um fenômeno denominado "apocalipse da informação" ou “apatia da realidade”. Além disso, as pessoas podem até descartar as filmagens genuínas como falsas, simplesmente porque se enraizaram na noção de que tudo o que não querem acreditar deve ser falso. Em outras palavras, a maior ameaça não é que as pessoas sejam enganadas, mas que passem a considerar tudo como engano (WESTERLUND, 2019, p. 5, tradução nossa).

Por fim, ainda apresenta alguns exemplos usados com essa tecnologia:

> A maioria dos *deepfakes* hoje em plataformas sociais como YouTube ou Facebook pode ser vista como diversão inofensiva ou trabalhos artísticos usando figuras públicas vivas ou mortas. Mas também há exemplos do lado negro dos *deepfakes*, nomeadamente pornografia de celebridades e vingança, bem como tentativas de influência política e apolítica (WESTERLUND, 2019, p. 5, tradução nossa).

Ainda, Silva exemplifica, com um caso ocorrido aqui no Brasil, durante as eleições, com o então candidato a governador João Dória, como o *Deepfake* pode ser usado com fins prejudiciais:

> Uma história parecida aconteceu também aqui no Brasil, durante as eleições do ano passado. Alguns dias antes da eleição para governador, o então candidato João Dória também foi vítima de um vídeo *deepfake*, onde ele aparece em uma orgia sexual. Apesar do conteúdo explícito ter sido amplamente compartilhado pelas redes sociais, o vídeo acabou não tendo qualquer impacto para Dória, que foi eleito como governador e, apenas um ano depois, a população praticamente esqueceu da existência desse *deepfake* — ao contrário de Rana Ayyub, que ainda precisa ficar se defendendo de trolls que a todo momento a relembram do vídeo falso de sexo feito com a imagem dela (SILVA, 2019, *online*).

Já neste exemplo, Silva relacionou um caso ocorrido no México, devido às *fake news*, a uma situação que poderá se suceder se mais para frente houver um descontrole do *Deepfake*, assim como já ocorre com as *fake news*:

> Esse é o verdadeiro terror das deepfakes atualmente, pois elas conseguem criar campanhas de difamação, silenciamento e descrédito. Imagine só: se hoje, apenas compartilhando a foto de alguém e um texto falando que a pessoa se trata de um abusador de crianças, sem qualquer outra prova, já é o suficiente para fazer com que essa pessoa se tornem alvo da população (como aconteceu no ano passado na cidade de Acatlán, no México, onde dois homens inocentes foram linchados e queimados pela população por causa de fake news do WhatsApp), imagine se, com a mesma facilidade que

> você consegue escrever um texto, também for possível criar um vídeo onde essas pessoas estão praticando o ato da qual são acusadas (SILVA, 2019, *online*)?

Logo, mesmo que o *Deepfake* ainda não represente um grave problema na socidade, ele é uma questão latente, que algum dia poderá estourar, conforme as pessoas forem usando suas técnicas e deturpando-as e com a constante evolução da sociedade. Dessa forma, é preciso não apenas divulgar sobre a existência dessa técnica e seus usos maléficos, com o fim de conscientizar as pessoas, mas também ensinar a sociedade a como descobrir se um vídeo é falso ou não.

4 Métodos de Combate

Fazer a detecção do *Deepfake* é muito difícil, já que nos vídeos se usam imagens reais, o áudio pode ter som autêntico e se espalham nas redes sociais rapidamente. Mesmo que a maior parte dos vídeos feitos atualmente com essa tecnologia ainda apresentem qualidade inferior e se possa identificar que são falsos, já começam a aparecer alguns que colocam em dúvida se seriam manipulados ou não, de tão bem feitos que são.

Segundo Sohrawardi e Wright, a detecção do *Deepfake*, como um campo de pesquisa, se iniciou há pouco mais de três anos. Ademais, eles revelam outros aspectos quanto às pesquisas feitas sobre o tema e a agilidade com que essa técnica evolui:

> Os primeiros trabalhos se concentraram na detecção de problemas visíveis nos vídeos, como *deepfakes* que não piscavam. Com o tempo, no entanto, as falsificações ficaram melhores em imitar vídeos reais e se tornaram mais difíceis de detectar, tanto para as pessoas quanto para as ferramentas de detecção. (SOHRAWARDI e WRIGHT, 2020, *online*, tradução nossa)

Já Westerlund acredita em quatro maneiras de combater o *Deepfake*:

> - Legislação e regulamentação;
> - Políticas corporativas e ações voluntárias (por exemplo, os políticos podem se comprometer a não usar táticas ilícitas de campanha digital ou espalhar desinformação, como *deepfakes*, em suas campanhas eleitorais);
> - Educação e treinamento;
> - Tecnologia anti-*deepfake* que inclui detecção de *deepfake*, autenticação de conteúdo, e prevenção *deepfake* (WESTERLUND, 2019, p. 6, tradução nossa).

Conforme Vizoso, Vaz-Álvarez e López-García (2021, p. 5), provedores como Google, Facebook e Twitter, nos últimos meses, começaram diferentes iniciativas cujo objetivo único é encontrar maneiras eficientes de detectar e impedir a propagação da desinformação e, mais recentemente, o *Deepfake*. Essas diferentes iniciativas são:

> O Google, por exemplo, disponibilizou para a comunidade de pesquisa um grande conjunto de vídeos manipulados e não manipulados (Dufour & Gully, 2019). Com essa iniciativa, eles querem ajudar no desenvolvimento de técnicas de identificação, aproveitando a grande quantidade de informações armazenadas em seus arquivos. Além disso, eles colaboram com a Agência de Projetos de Pesquisa Avançada de Defesa para financiar diferentes pesquisadores que estão desenvolvendo ferramentas forenses de mídia (Vizoso, Vaz-Álvarez e López-García, 2021, p. 5, tradução nossa).

O Facebook, segundo os autores, optou por financiar projetos de pesquisa com vistas ao combate ao *Deepfake*:

> Por outro lado, o Facebook está financiando diferentes projetos de pesquisa dentro de seu *'Deepfake Detection Challenge*'. Esta iniciativa, impulsionada por empresas como Facebook, Microsoft e Amazon *Web Services* e unidades de pesquisa de várias universidades nos Estados Unidos, tenta ajudar os pesquisadores que estão trabalhando no desenvolvimento de ferramentas de detecção de *deepfake* baseadas em inteligência artificial. Assim, um corpus de mais de 100.000 vídeos ficou à disposição desses pesquisadores que lutam por apresentar mecanismos úteis para ganhar diferentes prêmios (Vizoso, Vaz-Álvarez e López-García, 2021, p. 5 e 6, tradução nossa).

Ainda acrescentam outra medida tomada pelo Facebook:

> Além disso, a rede social de Mark Zuckerberg tenta neutralizar essa forma de desinformação excluindo vídeos ou fotos adulterados, ou rotulando-os como notícias falsas com a ajuda de meios de comunicação de verificação de fatos (Bickert, 2020). Isso é particularmente importante para aqueles relacionados à corrida pelos Estados Unidos em 2020, devido à influência que notícias falsas podem ter nesse processo (Vizoso, Vaz-Álvarez e López-García, 2021, p. 6, tradução nossa).

De outra parte, os autores pontuam as iniciativas do Twitter para o combate dessa técnica:

> Por fim, o Twitter mostra uma abordagem mais simples para esse problema. Eles resumem sua estratégia nas seguintes quatro regras (Harvey, 2019): Identificação por meio de um aviso de *Tweets* com conteúdo manipulado, alertando sobre sua condição de manipulação antes de compartilhá-lo, inclusão de um *link* para artigos de notícias ou outras fontes verificadas nas quais os usuários possam encontrar descobrir por que e como o conteúdo foi

> adulterado e eliminação de todo o conteúdo manipulado potencialmente prejudicial ou ameaçador à segurança de alguém (Vizoso, Vaz-Álvarez e López-García, 2021, p. 6, tradução nossa).

No campo jurídico, ainda é notável a escassez de legislação sobre *Deepfake* tanto no Brasil, quanto em outros países. No Brasil, há inúmeros projetos de lei em tramitação na Câmara dos Deputados e no Senado, com vistas ao combate à desinformação, mas um projeto de lei, mais especificamente sobre às *fake news*, se destaca pelo avanço na tramitação. Esse projeto de lei é o PL 2630/2020 de iniciativa do Senador Alessandro Vieira, com tramitação desde 2020, o qual institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, a Lei das *Fake News*. No dia 15 de abril de 2021, a situação foi atualizada com o despacho de "Proposição Sujeita à Apreciação do Plenário. Regime de Tramitação: Prioridade" (BRASIL, 2020, *online*).

No entanto, para uma possível resolução do problema de *Deepfake* que venha a surgir, enquanto não advém uma lei específica para regular esse tema, poderia se utilizar a recente Lei Geral de Proteção dos Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018, que começa a viger a partir deste ano.

Em seus arts. 2º e 7º, traz, além de outros, a proteção ao direito à imagem e à honra, com a implementação de uma série de medidas que impedem o uso de dados pessoais sem o consentimento do titular, visando a preservação da intimidade. Assim, mesmo que essa lei não trate especificamente dos usos com finalidades ilícitas de ferramentas como a I.A. para criação de *Deepfake*, ela poderá ser utilizada, por enquanto, para suprir a lacuna existente no direito brasileiro.

Além disso, quanto à proteção aos direitos de personalidade, combina-se a sua utilização com o art. 5°, X da Constituição Federal, que trata o assunto de forma genérica, e com o Código Civil, que trata mais especificamente o tema, em seus arts. 11 ao 21, já que os direitos de personalidade, em específico o direito à imagem, foram violados com a prática do *Deepfake*. Além do direito à honra, cabível também se desse episódio resultasse um abalo indenizável a esse outro direito de personalidade.

Um instrumento que também poderia ser utilizado, nesses casos, é o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), principalmente com base em seu art. 7º, o qual aborda os direitos e garantias dos usuários da *Internet*, em que há a possibilidade da vítima do conteúdo falso pedir na plataforma a sua retirada, e, se não for atendido, ingressar na Justiça com o pleito de remoção desse conteúdo pernicioso, com uma possível responsabilização, se houver o descumprimento de ordem judicial.

Outro ponto a ser mencionado é que o reconhecimento facial - parecido com um sistema de biometria, pois cada rosto tem pontos específicos, que não são iguais a outros - utilizado na técnica de *Deepfake*, armazena dados pessoais, com a violação da intimidade pessoal, contrariando, assim, os direitos fundamentais da vítima.

Assim, se a utilização do *Deepfake* violar o direito à imagem ou o direito à honra de alguma pessoa, com a extrapolação do direito de informar, causando danos, isso caracteriza a abusividade e o consequente dever de indenização, preconizado pelos arts. 186, 187 e 927 do Código Civil, seja ele moral e/ou material, independentemente de culpa.

No direito comparado, há alguns exemplos de medidas que foram tomadas para tentar frear esse avanço desordenado das novas tecnologias, mesmo com o vácuo legislativo generalizado quanto ao *Deepfake*, já que elas podem trazer possíveis repercussões negativas para a sociedade.

Um caso curioso ocorreu na Malásia, que foi um dos primeiros países que instituíram uma legislação para conter a desinformação, nesse caso a política, em que a prática dessa desinformação foi considerada crime passível de prisão de até seis anos. Entretanto, essa legislação foi considerada extremamente nociva, e, em agosto de 2018, foi noticiado que a Malásia teria retrocedido e revogado a referida lei (PINTO, 2019, p. 195 e 196).

Na Europa, para regular as questões sobre a proteção dos dados, há a *General Data Protection Regulation* (GDPR), que entrou em vigou maio de 2018. Essa lei, que serviu de inspiração para a lei brasileira de proteção dos dados, foi bem agressiva quanto ao lado regulatório e legislativo (PINTO, 2019, p. 196).

O GDPR, além de obrigar as empresas que coletam e manuseiam dados pessoais a identificar suas bases técnicas e jurídicas e utilizá-los só com o consentimento dos envolvidos, trouxe uma abrangência extraterritorial à lei, em que empresas, independentemente de estarem sediadas ou terem filiais na Europa, se colhem ou manipulam dados de pessoas que vivem na Europa, devem se submeter a essa lei. Além, é claro, da possibilidade de pedir judicialmente ou administrativamente a exclusão do material em questão (PINTO, 2019, p. 196).

A Alemanha adotou a linha da responsabilização dos provedores das redes sociais com a edição do Ato de Cumprimento da Lei nas Redes Sociais, de outubro de 2017, que impõe multa pesada às redes se elas não removerem material ofensivo ou ameaçador após vinte e quatro horas da decisão judicial ou da reclamação da vítima. Assim, além do Estado se preocupar com a desinformação, também há um maior zelo em se tratar o discurso de ódio direcionado aos imigrantes do país (PINTO, 2019, p. 197).

A China colocou em prática novas regras de publicação de conteúdo escrito, em vídeo e áudio *online*, com o estabelecimento de que qualquer alteração realizada por Inteligência Artificial ou Realidade Virtual, nesses meios, precisa estar sinalizada. Assim, abrangiu também a proibição da disseminação de notícias falsas produzidas por *Deepfake*. Essas novas regras, que estavam previstas para vigorar a partir do dia primeiro de janeiro de 2020, são de autoria da Administração do *Ciberespaço* da China (CAC), e seu desrespeito é considerado ofensa criminal (RAUPP, 2019, *online*).

Por fim, nos Estados Unidos, além de muitos projetos de lei que atualmente tramitam sobre *Deepfake*, alguns estados elaboraram algumas leis específicas para tentar regular esse tema e combatê-lo. O Texas aprovou uma lei com a criminalização da conduta de publicar e dissemir vídeos, que utilizem a técnica do *Deepfake* para prejudicar um candidato durante o processo eleitoral.

No estado da Califórnia, foi promulgada uma lei em 2019, que tornou ilegal a criação ou distribuição de Deepfake, dentro de sessenta dias após a eleição, com o intuito de enganar eleitores e prejudicar candidatos no âmbito político (Vizoso, Vaz-Álvarez e López-García, 2021, p. 6).

Outro estado dos Estados Unidos, que também abordou esse tema, foi a Virgínia ao estabelecer uma atualização, em 2019, em sua lei contra a prática da pornografia de vingança e sua distribuição por diversos meios. Nessa atualização passou a se incluir também o Deepfake como ato criminoso, ao abranger vídeos ou imagens falsas. Assim, a lei confere a esse delito uma posição de contravenção "classe 1", com pena de até doze meses de prisão ou multa de até 2,5 mil dólares (RAUPP, 2019, *online*).

Desse modo, navegar na internet, atualmente, e evitar vídeos e notícias falsas é quase como andar por um campo minado, pois mesmo ao desviar e tomar todas as precauções, pode-se pisar em uma bomba. Mas isso não é motivo para deixar de cuidar e simplesmente avançar cegamente, sem nenhuma atenção. O importante é manter a sociedade informada quanto aos perigos iminentes e todas as medidas tomadas em relação a eles e, além disso, também divulgar como se proteger caso apareçam. Assim, essas são as maneiras encontradas de se evitar danos maiores para a população.

5 Considerações Finais

Diante do exposto, observa-se que, com a evolução da tecnologia, novas técnicas surgiram e, mesmo se elas inicialmente não fossem usadas para o mal, poderia chegar um

momento em que elas precisassem ser combatidas para evitar um dano maior à sociedade. Então, como ocorre atualmente com as *fake news* - em que há um grande descontrole na sua propagação - ao serem consideradas o grande mal da *internet* nos últimos cinco anos, há uma premente necessidade de se falar também sobre o *Deepfake*, que surgiu como sua evolução técnica.

Percebe-se que já há um grande número de pesquisas realizadas para a detecção e o combate ao *Deepfake*, mas como o número de pessoas que fazem os *Deepfakes* são maiores do que o número das que tentam solucionar os seus problemas, quando se acha que chegou em um ponto fraco dessa tecnologia, o sistema vem e melhora aquilo que outrora seria o defeito e a solução para a desinformação gerada.

Nesse sentido, há uma afirmação feita por Hao Li que corrobora com o que foi dito, quanto à rapidez com que o *Deepfake* evolui e sobre a busca constante que se deve ter por soluções de detecção: "This is developing more rapidly than I thought. Soon, it's going to get to the point where there is no way that we can actually detect [deepfakes] anymore,so we have to look at other types of solutions."[6] (WESTERLUND, 2019, p. 1).

Dessa forma, para evitar a desinformação em maior nível, deve-se conhecer mais a fundo essa nova técnica e divulgar mais sobre esse assunto e sobre os estudos em andamento para dar mais visibilidade ao iminente problema. Isso evita que a sociedade não seja ludibriada por essa técnica e passe a ter mais cuidado ao compartilhar informações e vídeos, assim, para não contribuir com a desinformação e seus efeitos nefastos. Com isso, não se deve ignorar as quatro importantes frentes de combate: Legislação e regulamentação; Políticas corporativas e ações voluntárias; Educação e treinamento e Tecnologia anti-*deepfake*.

Por conseguinte, mesmo com a observação da escassez de legislações sobre *Deepfake* a nível global, pela atualidade da matéria e recente discussão, alguns países já estão nessa busca antecipada por meios de combate e regulamentação antes que o problema se torne maior e incontrolável, como atualmente é o caso das *fake news*, em que também há uma dificuldade generalizada na sua abordagem.

Assim, no Brasil, acredita-se que a recente Lei Geral de Proteção dos Dados atende à normatização do problema, juntamente com o Marco Civil da Internet e com a Constituição Federal e o Código Civil, no que toca aos Direitos de Personalidade, mais especificamente ao Direito à Imagem e ao Direito à Honra.

[6] Isso está se desenvolvendo mais rapidamente do que eu pensava. Em breve, chegará ao ponto em que não haverá mais como detectar [*deepfakes*], então temos que olhar para outros tipos de soluções. (tradução nossa)

Referências

AFP. Pesquisa global revela que 86% dos internautas já acreditaram "fake news". **EXAME**, 12 jun. 2019. Disponível em: https://exame.com/brasil/pesquisa-global-revela-que-86-dos-internautas-ja-acreditaram-fake-news/. Acesso em: 02 abr. 2021.

BATTAGLIA, Rafael. Afinal, o que são deepfakes? **Super Interessante**, 07 jan. 2020. Disponível em: https://super.abril.com.br/tecnologia/afinal-o-que-sao-deepfakes/. Acesso em: 02 abr. 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.630, 03 jul. 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735. Acesso em: 16 abr. 2021.

CABRAL, Isabela. O que é deepfake? Inteligência artificial é usada pra fazer vídeo falso. **TechTudo**, 28 jul. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/07/o-que-e-deepfake-inteligencia-artificial-e-usada-pra-fazer-videos-falsos.ghtml. Acesso em: 02 abr. 2021.

CASTELLS, Manuel. **A sociedade em rede.** 6. ed. rev. ampl. São Paulo: Paz e Terra, 2002. v. 1. 700 p.

COSSETTI, Melissa Cruz. O que é inteligência artificial? **Tecnoblog**, 2018. Disponível em: https://tecnoblog.net/263808/o-que-e-inteligencia-artificial/. Acesso em: 02 abr. 2021.

DODGSON, Neil. Face-swap on steroids: How ‘deepfake’ videos are messing with reality. **The Spinoff**, 22 fev. 2018. Disponível em: https://thespinoff.co.nz/science/22-02-2018/face-swap-on-steroids-how-deepfake-videos-are-messing-with-reality/. Acesso em: 02 abr. 2021.

ÉPOCA NEGÓCIOS ONLINE. Leia o texto do convite que criou o termo inteligência artificial. **Época Negócios Online**, 13 mar. 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/03/leia-o-texto-do-convite-que-criou-o-termo-inteligencia-artificial.html. Acesso em: 01 abr. 2021.

GOEPIK. NÃO CONFUNDA: Indústria 4.0 e Indústria 3.0. **GoEpik**, 30 dez. 2019. Disponível em: https://www.goepik.com.br/entenda-industria40-e-industria30. Acesso em: 04 abr. 2021.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

MCCARTHY, John. **What is Artificial Intelligence?** 12 nov. 2007. 15 p. Disponível em: http://www-formal.stanford.edu/jmc/whatisai.pdf. Acesso em: 02 abr. 2021.

PINTO, Kleber Couto. **A problemática das *fake news*.** 2019. 229 p. Disponível em: https://portal.estacio.br/media/4684338/kleber-couto-pinto.pdf. Acesso em: 04 abr. 2021.

RAUPP, Eric. Com potencial de destruir reputações, "deepfakes" se tornam acessíveis. **Correio do Povo**, 04 out. 2019. Disponível em: https://www.correiodopovo.com.br/jornalcomtecnologia/com-potencial-de-destruir-reputa%C3%A7%C3%B5es-deepfakes-se-tornam-acess%C3%ADveis-1.370284. Acesso em: 04 abr. 2021.

SILVA, Rafael Rodrigues da. Deepfakes no Brasil | Parte 1: o estado das fake news brasileiras em 2019. **CanalTech**, 20 out. 2019. Disponível em: https://canaltech.com.br/redes-sociais/deepfakes-no-brasil-parte-1-o-estado-das-fake-news-brasileiras-em-2019-152981/?fbclid=IwAR0dhKpf_xr_nD0KEj7TnnE9pCa3uhBnGyAr8omPA-HXLWZq4bvLhwv4r6E. Acesso em: 02 abr. 2021.

SILVA, Rafael Rodrigues da. Deepfakes no Brasil | Parte 2: a ameaça fantasma de nossa democracia. **CanalTech**, 24 out. 2019. Disponível em: https://canaltech.com.br/internet/deepfakes-no-brasil-parte-2-a-ameaca-fantasma-de-nossas-democracias-153453/. Acesso em: 02 abr. 2021.

SILVA, Rafael Rodrigues da. Deepfakes no Brasil | Parte 3: Como se proteger dos vídeos falsos. **CanalTech**, 03 nov. 2019. Disponível em: https://canaltech.com.br/inteligencia-artificial/deepfakes-no-brasil-parte-3-como-se-proteger-dos-deepfakes-153963/. Acesso em: 02 abr. 2021.

SOHRAWARDI, John; WRIGHT, Matthew. In a battle of AI versus AI, researchers are preparing for the coming wave of deepfake propaganda. **The Conversation: Science + Technology**: Boston - EUA, 09 out. 2020. Disponível em: https://theconversation.com/in-a-battle-of-ai-versus-ai-researchers-are-preparing-for-the-coming-wave-of-deepfake-propaganda-146536. Acesso em: 02 abr. 2021.

TAGIAROLI, Guilherme. Dupla de djs Tropkillaz rebola em 1º clipe brasileiro que usa deepfake. **Tilt/UOL**; São Paulo, 23 jan. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/01/23/primeiro-clipe-brasileiro-com-deepfake-faz-tropkillaz-dancarem-e-rebolarem.htm. Acesso em: 02 abr. 2021.

VILLANI, Cédric. **Donner un sens à l'intelligence artificielle: pour une stratégie nationale et européenne.** França: AI for Humanity, mar. 2018. 22 p. Disponível em: https://www.aiforhumanity.fr/pdfs/MissionVillani_Presse_FR-VF.pdf. Acesso em: 01 abr. 2021.

VIZOSO, Ángel, VAZ-ÁLVAREZ, Martín e LÓPEZ-GARCÍA, Xosé. Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation. **Media and Communication**; vol. 9, n. 1, p. 291-300, 03 mar. 2021. Disponível em: http://dx.doi.org/10.17645/mac.v9i1.3494. Acesso em: 02 abr. 2021.

WESTERLUND, Mika. The Emergence of Deepfake Technology: A Review. **Technology Innovation Management Review;** Ottawa**,** vol. 9, ed. 11, p. 39-52, nov. 2019. Disponível em: https://search.proquest.com/docview/2329154005?pq-origsite=primo&gathStatIcon=true. Acesso em: 02 abr. 2021.