

Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço (*)

Deepfake: artificial intelligence and algorithm causing risks to society in cyberspace

Deepfake: inteligencia artificial y algoritmo que causa riesgos a la sociedad en el ciberespacio

Moyana Mariano Robles-Lessa¹

Hildeliza Lacerda Tinoco Boechat Cabral²

Gilberto Fachetti Silvestre³

Sumário: Considerações iniciais. **1.** A inteligência artificial e a importância dos algoritmos. **2.** A atuação dos algoritmos na produção dos *deepfakes* e possíveis danos à sociedade no ciberespaço. **3.** A necessária regulamentação da prática dos *deepfakes* no âmbito cível e criminal. **4.** A cognição e a linguagem da inteligência artificial e sua má utilização nos *deepfakes*. – Considerações finais. – Referências.

(*) Recibido: 01/06/2020 | Aceptado: 10/06/2020 | Publicación en línea: 01/07/2020.



Esta obra está bajo una [Licencia Creative Commons Atribución-NoComercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

- ¹ Estudante do Curso do Direito; Licenciada em Letras; Pós-graduada em Direito Tributário com Docência do Ensino Superior; Pesquisadora do Grupo de Estudos e Pesquisa em Bioética e Dignidade Humana – GEPBiDH.
moyanarobles@hotmail.com
- ² Cursando Pós-doutorado em Direito Civil e Processual Civil (UFES); Doutora e Mestra em Cognição e Linguagem – UENF; Professora dos Cursos de Direito e Medicina; Miembro efectivo de la Asociación de Bioética Jurídica de la UNLP; Membro do Grupo de Pesquisa “Desafios do Processo”; Coordenadora do Grupo de Estudos e Pesquisa em Bioética e Dignidade Humana – GEPBiDH.
hildeboechat@gmail.com
- ³ Professor da Universidade Federal do Espírito Santo (UFES); Doutor em Direito Civil pela Pontifícia Universidade Católica de São Paulo (PUC/SP); Mestre em Direito Processual Civil pela Universidade Federal do Espírito Santo (UFES); Coordenador do Grupo de Pesquisa “Desafios do Processo”.
www.desafiosdoprocesso.ufes.br
gilberto.silvestre@ufes.br

Resumo: A contemporaneidade proporcionou um avanço tecnológico presente cotidianamente na vida do ser humano, tornando-o em diversos aspectos dependente das novas tecnologias. Diante dos fatos, surgiu recentemente através da inteligência artificial, uma ferramenta denominada *deepfake*, que foi desenvolvida mediante um algoritmo possuidor de aprendizagem profunda e com capacidade para autocorreção, assumindo a personalidade de outrem nas redes digitais sociais, através de vídeos e áudios, difundindo inverdades e cometendo crimes. Tem-se por objetivo neste artigo informar a existência deste novo perigo presente na internet, ao mesmo tempo que torna evidente a importância de uma regulamentação legal que penalize os usuários do *deepfake*. O problema deste artigo relaciona-se à inteligência artificial, procurando informar que seu uso pode e tem sido utilizado de forma negativa, prejudicial a toda comunidade global, alertando aos usuários da rede mundial de computadores para possíveis danos causados no ciberespaço. Para desenvolver este artigo, valeu-se de metodologia qualitativa, por meio de pesquisa bibliográfica em livros estrangeiros e artigos científicos; e, ainda, exploratória, por meio da análise de leis que tratam a respeito do uso da internet e dos internautas. Conclui-se que, por serem as novas tecnologias um advento da contemporaneidade, ainda não existem legislações que coíbam o mal uso na rede mundial de computadores relacionadas ao uso indevido da inteligência artificial e os prejuízos socioeconômicos por ela causados.

Palavras-chave: inteligência artificial, deepfake, algoritmos, rede mundial de computadores.

Abstract: Contemporaneity provided a technological advance present daily in the life of the human being, making it in several aspects dependent on new technologies. Given the facts, it recently emerged through artificial intelligence, a tool called *deepfake*, which was developed through an algorithm possessing deep learning and capable of self-correction, assuming the personality of others in social digital networks, through videos and audios, spreading untruths and committing crimes. The purpose of this article is to inform the existence of this new danger present on the Internet, while making evident the importance of a legal regulation that penalizes *deepfake* users. The problem of this article is related to artificial intelligence, seeking to inform that its use can and has been used in a negative way, harmful to the entire global community, alerting users of the worldwide computer network to possible damage caused in cyberspace. To develop this article, it used qualitative methodology, through bibliographical research in foreign books and scientific articles; and, also, exploratory, through the analysis of laws that deal with the use of the Internet and internet users. It is concluded that, because new technologies are an advent of contemporaneity, there are still no laws that restrain the misuse in the worldwide computer network related to the misuse of artificial intelligence and the socioeconomic damage caused by it.

Keywords: artificial intelligence, deepfake, algorithms, worldwide computer network.

Resumen: La contemporaneidad proporcionó un avance tecnológico presente diariamente en la vida del ser humano, haciendo que en varios aspectos dependiera de las nuevas tecnologías. Dados los hechos, recientemente surgió a través de la inteligencia artificial, una herramienta

llamada *deepfake*, que fue desarrollada a través de un algoritmo que poseía un aprendizaje profundo y capaz de autocorrección, asumiendo la personalidad de los demás en las redes digitales sociales, a través de videos y audios, difundiendo falsedades y cometiendo crímenes. El **objetivo** de este artículo es informar la existencia de este nuevo peligro presente en Internet, haciendo evidente la importancia de un reglamento legal que penalice a los usuarios *de deepfake*. El **problema** de este artículo está relacionado con la inteligencia artificial, buscando informar que su uso puede y ha sido utilizado de manera negativa, perjudicial para toda la comunidad global, alertando a los usuarios de la red informática mundial sobre los posibles daños causados en el ciberespacio. Para desarrollar este artículo, se utilizó metodología cualitativa, a través de la investigación bibliográfica en libros extranjeros y artículos científicos; y, también, exploratorio, a través del análisis de las leyes que se ocupan del uso de Internet y de los usuarios de Internet. Se concluye que, debido a que las nuevas tecnologías son un advenimiento de la contemporaneidad, todavía no existen leyes que restrinjan el mal uso en la red informática mundial relacionada con el uso indebido de la inteligencia artificial y el daño socioeconómico causado por ella.

Palabras clave: inteligencia artificial, deepfake, algoritmos, red informática mundial.

“Hoje em dia, os robots humanizados conseguem executar as mesmas tarefas que os humanos, pois as máquinas têm funções cognitivas, tal como o homem, que lhes permite realizarem um processo de aprendizagem” (READS, Smart. 2017).

Considerações iniciais

A era contemporânea trouxe avanços tecnológicos antes inimagináveis ao ser humano. O expressivo avanço das novas tecnologias teve início no século XX, ampliando seu campo por meio das ciências da computação, principalmente pelo notável avanço da inteligência artificial nas máquinas. A criação dos algoritmos tornou possível o aprimoramento da inteligência artificial e a cada novo momento as máquinas são capazes de desenvolver a cognição e a linguagem de forma bem próxima àquela que o ser humano realiza. Recentemente, mais precisamente no ano de 2017, o ciberespaço foi invadido por uma ferramenta denominada *deepfake*, desenvolvida a partir de um algoritmo criado com aprendizagem profunda, capaz de se autocorrigir.

Sabe-se que o comportamento do usuário da internet determina a classificação do uso desse recurso como instrumento positivo ou negativo, ou ainda capaz de promover o bem ou a destruição. Nessa linha de intelecção, a presente pesquisa se propôs investigar o seguinte problema: de que forma os *deepfakes* podem causar riscos e danos à sociedade no ciberespaço?

Assim, os *deepfakes*, por meio de sua atuação no ciberespaço, difundem notícias falsas como se verdadeiras fossem, podendo impor sérias consequências a

toda rede mundial de computadores, sendo considerados prejudiciais de forma que a atuação deles pode causar prejuízos e até mesmo cometimento de crimes, tanto na esfera política, como na vida pessoal e social – fato que reclama por regulamentação.

O reconhecimento desta nova ameaça identificada no uso das redes sociais digitais, torna o estudo desta ferramenta – *deepfake* – relevante a toda sociedade global, já que possui capacidade para influenciar negativamente a opinião dos usuários do ciberespaço, e conseqüentemente toda a população mundial. Destaca-se ainda a urgência de regulamentação legal da prática desta conduta pelas graves intimidações que impõe à sociedade, inclusive em relação aos crimes provenientes da atuação dos sujeitos que implementam os *deepfakes* no ciberespaço.

O presente artigo busca compreender a evolução dos avanços tecnológicos na contemporaneidade e os efeitos que eles podem acarretar à sociedade, abordando-se os seguintes temas: a inteligência artificial e a importância dos algoritmos; a atuação dos algoritmos na produção dos *deepfakes* e possíveis danos à sociedade no ciberespaço; a necessária regulamentação da prática dos *deepfakes* no âmbito cível e criminal e; a cognição e a linguagem da inteligência artificial e sua má utilização nos *deepfakes*.

Espera-se este artigo seja capaz de despertar a atenção dos usuários da rede mundial de computadores a respeito de um novo perigo existente nas redes sociais digitais, que, já influencia negativamente as escolhas e interesses dos usuários da internet, levando-os a acreditarem em vídeos e áudios manipulados pelos *deepfakes*.

1. A inteligência artificial e a importância dos algoritmos

Com o advento das novas tecnologias, o mundo de forma globalizada deu início a uma nova era, na qual a comunicação em sua grande maioria se dá mediada pelos computadores interconectados à internet. O século passado adentrou às ciências da computação com enorme expectativa em buscar soluções para muitas dificuldades inerentes à vida do ser humano, vendo-se nas novas tecnologias uma infinidade de possibilidades que poderiam trazer conforto ao cotidiano da humanidade, como por exemplo resolução de cálculos mais complexos, resultados médicos precisos, engenharia desenvolvida, sem falar na perspectiva de melhoria e globalização na comunicação entre todos os povos.

Talvez, o que não se pensasse logo no início do século XX, era que os computadores teriam uma inteligência artificial, popularmente conhecida pelas siglas I.A. Somente a ficção retratava a possibilidade de um robô ou computador ter como atributo a inteligência artificial – sendo que na maioria das vezes, essas máquinas se rebelavam contra seus criadores. Porém, ainda no século XX, mais precisamente no ano de 1956, deu-se início à criação da inteligência artificial nos computadores. Um professor da Universidade *Dartmouth*, em *Hanover* nos Estados Unidos, “[...] selecionou um grupo de cientistas com os quais trabalhou durante um verão, estudando uma forma de ‘ensinar’ as máquinas. Para isso, seria necessário descrever precisamente aspectos do aprendizado e outras características da inteligência humana” (LAVAGNOLI, 2019). Foram criadas assim máquinas capazes de fazer uso da linguagem, solucionar problemas e aperfeiçoar-se progressivamente.

Relatório produzido por uma empresa holandesa em 2018 trata da evolução das tecnologias e suas ameaças e define a inteligência artificial como “[...] um ramo da ciência da computação que visa replicar recursos da inteligência humana em software” (PATRINI et al., 2018). E Mariana Preti (2018) caracteriza o algoritmo como “[...] um conjunto finito de diretrizes que descrevem como executar uma tarefa”. Essas definições se interligam desde a criação da inteligência artificial e os algoritmos tiveram um papel fundamental nesse processo, pois eles permitem que a inteligência artificial se materialize atualmente, inclusive promovendo novos acertos a partir de erros. Os algoritmos não só possibilitaram a inteligência artificial, como a aperfeiçoam a cada novo erro produzido por eles.

Qualquer máquina que apresente um ‘comportamento inteligente’, ou que seja ‘capaz de raciocinar’ reporta-se à inteligência artificial e a seus algoritmos de criação, sendo capaz de perceber o ambiente no qual está estabelecida, podendo decidir e atingir com sucesso, determinado objetivo. A inteligência artificial possui as seguintes características: percepção, aprendizagem, raciocínio, comunicação e comportamento de correção, mesmo em ambientes complexos. As ciências da computação têm como objetivo aperfeiçoar de forma progressiva os algoritmos, para que a inteligência artificial consiga superar o desempenho humano, ao executar a mesma tarefa (READS, 2017).

É fato que a inteligência artificial só se tornou possível, devido à incessante busca do ser humano por meios que contribuíssem para a vida social como um todo. A vida em sociedade é imanente ao homem, e nessa interação, o ser humano está sempre propenso a descobrir algo novo, que vá além de seu saber básico, com o objetivo de colaborar com a evolução da espécie humana e, ao mesmo tempo, proporcionar novas possibilidades à sociedade.

2. A atuação dos algoritmos na produção dos *deepfakes* e possíveis danos à sociedade no ciberespaço

As evoluções na área da tecnologia no século XX foram revolucionárias no cotidiano do ser humano, e essas evoluções não pararam, pois o século XXI também apresenta avanços tecnológicos cada vez mais expressivos. Agora, com um maior domínio pelo homem, as tecnologias proporcionam cada vez mais bem-estar à vida social, os avanços significativos da inteligência artificial oportunizam inúmeras aplicações positivas para toda a sociedade. Entretanto, Patrini; Cavalli e Adjer (2018), em seu relatório, apresentam que nem só com o intuito de beneficiar o homem as tecnologias foram criadas. Os autores expõem que as técnicas modernas das ciências da computação estão sendo também exploradas de má forma, com o objetivo de denegrir e prejudicar toda a população.

Mattos, Souza e Manhães (2012), reforçam essa noção de posicionamento, ao afirmarem: “Tratar, estudar e apresentar os efeitos negativos trazidos pela forma astutamente veloz com que o avanço tecnológico acontece e se apresenta, parece, para muitos, um discurso mais propriamente baseado no conservadorismo do que realmente fundamentado em bases sólidas e importantes”. Os autores ainda advertem:

É possível perceber que a velocidade da evolução violenta o ser humano em muitos aspectos. Esta violência, muitas vezes, é deturpada ou maquiada por estratégias de imposição em massa dos processos tecnológicos, como se tudo fosse natural e como se

não houvesse outro meio ou forma de ser feito. (MATTOS; SOUZA; MANHÃES, 2012, p.186).

Como exemplo da exposição supra, tem-se a matéria recém-divulgada pelo jornal Fantástico, no dia 10 de novembro de 2019, tratando das influências negativas que a sociedade vem sofrendo com a desinformação provocada pelas novas tecnologias. A reportagem evidencia que a população brasileira, em sua grande maioria, acredita nas redes sociais digitais e tem nelas a principal fonte de informação, a saber:

[...] a Nana Queiroz é de uma ONG de mobilização social: a Avaaz, essa ONG e a Sociedade Brasileira de Imunizações, encomendaram ao IBOPE uma pesquisa, que trouxe os seguintes números: de cada dez pessoas entrevistadas, sete disseram que acreditaram em pelo menos uma notícia falsa sobre vacina; 57% dos que não se vacinaram citaram um motivo relacionado a desinformação; e 48% dos entrevistados falaram que têm redes sociais e aplicativos como uma das principais fontes de informação sobre vacina. (FANTÁSTICO, 2019).

Fatos assim evidenciam como e quanto as pessoas estão vulneradas aos fatos o que acontecem e são divulgados nas redes sociais digitais, inclusive podendo causar risco à saúde, como o exemplo apresentado na matéria do jornal. Torna-se oportuno se observar que aplicativos maliciosos estão sendo criados exclusivamente com o propósito de divulgar e propagar notícias falsas no ciberespaço – que é explicado como “[...] a virtualização, a atualização em um lugar, de dados registrados em outro lugar, interconectados por redes, e que, por suas características técnicas de programação, permite a mediação da comunicação entre seres humanos, e com a própria cultura por eles produzida” (SOUZA; COSTA, 2005).

Nesses termos, a comunicação mediada pelas redes sociais digitais permite difundir tanto o bem, quanto o mal, dependendo somente do interesse do propagador. Para uma melhor compreensão das possibilidades negativas disponíveis nas redes sociais digitais, faz-se necessário entender a criação e o significado da tecnologia denominada *deepfake*.

A inteligência artificial possui duas categorias de algoritmos denominadas *Machine Learning* (ML) e *Deep Learning* (DL ou Rede Neural Profunda) (GUILLOU, 2018). O *Deep Learning* é um algoritmo que aprende com seus erros. E esta explicação relaciona-se aos *deepfakes*, conforme elucidação de Michael K. Spencer, em seu artigo intitulado “Deep Fake, a mais recente ameaça distópica”, publicado em maio do presente ano, descreve:

Deepfakes são, essencialmente, identidades falsas criadas com o *Deep Learning* [aprendizagem profunda, por meio de uso maciço de dados], por meio de uma técnica de síntese de imagem humana baseada na inteligência artificial. É usada para combinar e sobrepor imagens e vídeos preexistentes e transformá-los em imagens ou vídeos “originais” [...] Essa combinação de vídeos existentes e “originais” resulta em vídeos falsos, que mostram uma ou algumas pessoas realizando ações ou fazendo coisas que nunca aconteceram na realidade. Em 2019, também estamos vendo uma explosão de faces *fake*, através das quais a IA é capaz de conjurar pessoas que não existem na realidade, e que têm um certo fator de fluência. (SPENCER, 2019).

Em 2017, a rede social virtual *Reddit*, teve o primeiro caso de *deepfake* quando um usuário divulgou vídeos falsos nos quais atrizes de *Hollywood* tiveram seus rostos inseridos em vídeos de conteúdo adulto (impróprio aos menores, como por exemplo, material pornográfico). Neste caso, a inteligência artificial foi utilizada

para produzir e/ou editar um conteúdo falso, algo que até então, não havia acontecido. A tecnologia do *deepfake* usa o algoritmo *Deep Learning* na elaboração de conteúdos falsos, criando situações embaraçosas e disseminando conteúdo e informações falsas. Os *deepfakes* não atuam somente em sites de conteúdo adulto, as implicações do uso desta tecnologia podem causar situações muito piores quando associadas à política, à veiculação de notícias falsas, causando na população mundial um sentimento de instabilidade e ceticismo ao ver ou ouvir essas notícias em seu cotidiano (YOUNG, 2019).

Em 2018, a expressão *deepfake* obteve outras técnicas associadas ao seu nome, como por exemplo: reconstituição da expressão facial, manipulação de corpo inteiro e plano de fundo e síntese de áudio (PATRINI et al, 2018).

Nesse novo mundo, a IA é capaz de mimetizar conteúdo humano, e tem o potencial de ser usada por maus atores, e campanhas financiadas por Estados, para influenciar os sentimentos da população de várias formas. Estamos testemunhando uma explosão de fraude online. [...] Personagens e textos *fake* são os próximos fronts do debate em torno do *deepfake*, que está só começando e é ainda outra maneira com a qual a inteligência artificial pode ser aproveitada como máscara e alterar o sentimento coletivo através de truques digitais [...]. Humanos digitais, âncoras de jornais de inteligência artificial, personas virtuais — tudo é possível na nova internet. O mercado de farsa online já está maduro (SPENCER, 2019).

Nesse contexto, o ciberespaço é definido como um ambiente de comunicação:

[...] o espaço constituído com base em uma comunicação, em linguagens e diálogos homem-máquina, máquina-máquina. Vemos a tela, mas não visualizamos a quantidade informações, de comandos, expressões e códigos que estão por trás das imagens inônicas que vemos nas telas (Souza; Costa, 2005)

Torna-se interessante conferir a afirmativa de que o ciberespaço está conectado com a cibercultura, que se define da seguinte forma:

Pode-se observar que a cibercultura representa o conjunto de costumes, conhecimentos, efeitos e impacto do avanço tecnológico em nossa vida cotidiana, do pessoal ao profissional. É importante observarmos que estes costumes, agregados a todo o aparato tecnológico disponível, são ainda baseados nos costumes tradicionais. A internet representa ícone maior da cibercultura. (MATTOS; SOUZA; MANHÃES, 2012, p.183).

Entretanto, esse ambiente denominado “ciberespaço”, já não é mais seguro. O crescimento dos *deepfakes* apresenta uma nova concepção à rede social virtual, pois essa nova inteligência artificial trouxe ao cotidiano mundial a desinformação, que tende a se aprimorar, colocando em risco a relação de confiança entre o ser humano e a internet. Nesse sentido, afirma Spencer (2019): “O perigo dos *deepfakes* representa um novo tipo de ameaça à cybersegurança, na qual o que pode ser feito está muito à frente de como combatê-lo”.

3. A necessária regulamentação da prática dos *deepfakes* no âmbito cível e criminal

A centralização do uso das redes sociais digitais faz parte da realidade mundial deste novo milênio, pois o ser humano já está mergulhado na internet e vice-versa e o acesso à rede mundial de computadores se tornou ao mesmo tempo usual e essencial no cotidiano do homem. Porém, a legislação brasileira não se atualizou neste sentido, a virtualização caminha a passos largos, evolui quase que

instantaneamente, enquanto as leis se tornam obsoletas e ineficazes. São inúmeras as transformações apresentadas pelo uso livre da internet, embora muitos ainda não saibam lidar com as novas tecnologias, nem identificar os perigos que as redes sociais digitais podem causar:

Imaginou-se que a internet deveria ser "terra sem lei", onde tudo seria permitido pela aparente impossibilidade de descoberta da verdadeira identidade da pessoa. Percebeu-se a deficiência do direito penal tradicional no combate à criminalidade virtual. Os Códigos Penais e legislações penais especiais foram afetados por essa nova realidade, porque o direito penal é fortemente ligado à questão da soberania nacional, enquanto a internet, por sua vez, não conhece Estados por ser manifestação de uma verdadeira "aldeia global". Tradicionais regras de aplicação da lei penal no espaço, com exemplos quase hipotéticos, tais como o de cometimento de um crime de um lado da fronteira e concluí-lo após ter passado pela imigração, ganham importância na tentativa de combate aos criminosos, ao mesmo tempo em que estas são inúteis, porque crimes podem ser praticados de qualquer parte do mundo. Ao largo dessas reflexões sobre o direito penal, também se procurou enfrentar a contrafação na internet mediante ações contra quem distribuisse materiais protegidos pelo direito de autor, o que não deu certo pela impossibilidade de apreensão física das obras em formato digital. (TOMASEVICIUS FILHO, 2016).

Por se apresentar como um recurso muito novo nas redes sociais digitais, muitos usuários da internet ainda não reconhecem a tecnologia produzida pelo *deepfake* e seu potencial poder de confundir e enganar a sociedade. A falta de conhecimento e desinformação, aliadas à ausência de uma legislação que regule esse novo mecanismo utilizado na internet, certamente irá aumentar os problemas que envolvem o uso da rede mundial de computadores quando associadas à vida privada, política e social. Pesquisadores e estudiosos de áreas diversas começam a se preocupar com os efeitos negativos e até mesmo destruidores que os *deepfakes* podem causar:

Quanto mais realista os vídeos se tornarem mais a diferença entre seu alcance e o conhecimento de que tais conteúdos são forjáveis se acentuará, fazendo com que eles sejam tidos como verdadeiros pela maioria de seus consumidores [...] pela ausência de leis específicas, advogados civis precisam ficar "criativos", usando violação de direitos autorais e ações de difamação para trazer justiça a seus clientes. (LARA et al, 2018).

A Convenção de Budapeste é um Tratado Internacional de Direito Penal e Direito Processual Penal, e está em vigor desde 2004 - esta é a primeira convenção sobre cibercrimes - sendo firmado principalmente por países europeus, com o intuito de haver uma colaboração entre eles para o combate aos crimes praticados na internet. Entretanto, o Brasil não quis acolher à Convenção de Budapeste, justificando que por não ter participado de sua criação não seria interessante segui-lo. Apesar desta declaração, em 2013, começou a vigorar as Leis 12.737/2012 e 12.735/2012, conhecidas respectivamente como Lei Carolina Dieckman, e Lei Azeredo, todavia, são possuidoras - para não dizer réplica - de artigos contidos na Convenção de Budapeste de 2004. (LARA et al, 2018), e ainda complementam:

Isso significa, que o Brasil, por motivos de vaidade política, demorou 8 anos mais para perceber e legislar o que outros Estados já haviam visto como problema social tentaram uma união de interesse global para combater os *cybercrimes*, pois como foi explicado anteriormente o criminoso age dentro do *cyberspace* que não possui fronteiras.

A Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, é a Lei que regula o uso da internet no Brasil, através da previsão de princípios, garantias,

direitos e deveres para quem usa a rede mundial de computadores, ao mesmo tempo que orienta as diretrizes de atuação do Estado. A Lei nº 12.965/14 regulamenta o uso de ferramentas de interação e comunicação, estimula a criação de novas tecnologias, e protege o usuário e o provedor, através de seus princípios. Entretanto, esta Lei foi criada em 2014 e à época a ferramenta de inteligência artificial – *deepfake* – não havia sido concebida, portanto, não há nesta Lei, a previsão para o uso desta ferramenta. Em 2018, a legislação brasileira promulgou as Leis nº 13.709 e nº 13.718, que dispõem sobre a proteção e o tratamento de dados pessoais, bem como a divulgação de cenas criminosas, inclusive nos meios digitais, ainda assim, alguns doutrinadores defendem que estas novas leis não poderiam ser aplicadas em casos de *deepfakes*, pois não há previsão expressa nas legislações apontadas (SIQUEIRA, 2019). Dito isso, comprova-se a dificuldade de limitar legislativamente o uso do *deepfake* no mundo contemporâneo, já que por ser uma inovação, ainda não existe uma lei própria que o regule.

4. A cognição e a linguagem da inteligência artificial e sua má utilização nos *deepfakes*

José Saramago – escritor português e Prêmio Nobel de Literatura de 1998 – escreveu em 2000 o texto “Para que serve a comunicação?”, no qual constata:

As novas tecnologias da comunicação multiplicam de modo excepcional a quantidade de informações disponíveis. Isso é ao mesmo tempo fascinante e inquietante. Fascinante porque se nota que transformações muito positivas, em matéria de educação e formação, estão ao alcance da mão. Inquietante porque tudo isso mostra um mundo sobre o qual pairam as ameaças de desumanização e de manipulação. (SARAMAGO apud RODRIGUES, 2015).

Saramago, já se atentava para os avanços das novas tecnologias e os interligava ao conhecimento e as novas linguagens que estavam por vir junto à rede mundial de computadores, bem como os problemas que poderiam surgir através destas tecnologias. Já é sabido que o algoritmo de criação dos *deepfakes* possui um aprendizado profundo que analisa e prevê automaticamente, corrigindo prováveis erros. Tem-se a inteligência artificial produzindo máquinas capazes de utilizar o conhecimento e a linguagem de uma forma bem próxima da que o ser humano realiza. A inteligência artificial caminha cada vez mais rápido, permitindo que as ciências da computação crie suas máquinas com capacidade de inteligência cada vez mais próxima à realidade do homem. Da mesma forma que os seres humanos utilizam a cognição e a linguagem para evoluir e comunicar, a inteligência artificial busca através de seus algoritmos que as funções cognitivas e comunicativas humanas, sejam reproduzidas pelos programas virtuais.

Para a abordagem de um modelo cognitivo nas ciências da computação é necessário que exista um determinado programa, que busque representar através dos algoritmos, o pensamento humano. O campo interdisciplinar da ciência cognitiva e da psicologia experimental reúnem-se tentando trazer às máquinas o funcionamento da mente humana. E como a linguagem está relacionada ao pensamento? Tanto a linguística moderna, quanto a inteligência artificial, trabalham com o intuito de aprimorar o complexo campo da compreensão da linguagem. Como a inteligência artificial é um ramo da ciência da computação, sua metodologia busca a construção de máquinas que exerçam automaticamente a linguagem e cognição

humana, em mídias complexas e se aperfeiçoem a cada nova tentativa (RUSSELL; NORVIG, 2004).

Stuart J. Russell e Peter Norvig observam que a inteligência artificial é capaz de fazer um planejamento autônomo a centenas de milhões de quilômetros da Terra, de jogar xadrez com um campeão mundial e sair vencedor, possui controle autônomo sendo treinado para dirigir um veículo sem que precise de um humano ao volante, realiza diagnósticos médicos em níveis semelhantes aos de médicos especialistas em algumas áreas da medicina, possui planejamento logístico de transporte, utiliza a robótica como assistente em microcirurgias e, possui um processamento de linguagem e solução de problemas capaz de resolver palavras cruzadas de forma mais aprimorada do que a maioria dos humanos (RUSSELL; NORVIG, 2004).

Os algoritmos dos *deepfakes* possuem uma codificação automática, produzidos por meio de uma rede neural artificial utilizada para absorver dados em séries, através de um processo chamado de aprendizagem não supervisionada, este processo codifica os dados, corrigindo possíveis erros automaticamente, se tornando bem próximo do conhecimento e da linguagem dos seres humanos, por isso, identificar uma imagem ou um áudio falso, tem se tornando cada vez mais difícil. Como exemplo do desenvolvimento dos *deepfakes* tem-se: resolução de problemas, reconhecimento de fala, aprendizado e planejamento. O processo de inteligência artificial nos *deepfakes* inclui, a aprendizagem: que recebe informações e regras que regem o uso desta; o raciocínio: que faz uma conclusão definitiva ou bem próxima das regras criadas pelo algoritmo; e a autocorreção, ou seja, os algoritmos dos *deepfakes* foram codificados com o intuito de serem uma versão automatizada da inteligência humana e das habilidades cognitivas (YOUNG, 2019).

Diante do exposto, compreende-se a preocupação relacionada às tecnologias que utilizam a inteligência artificial e seus algoritmos com autocorreção, aproximando-se assim, do vocabulário e da compreensão humana. “[...] A maneira sofisticada pela qual informações falsas podem ser criadas, a rapidez com que podem ser criadas e o quão infinitamente elas podem ser disseminadas está em um nível diferente. No passado, eu poderia ter espalhado mentiras, mas meu alcance seria limitado.” (WACHTER, 2019).

Considerações finais

Faz-se necessário compreender os *deepfakes* como criação da inteligência artificial em relação aos possíveis prejuízos à sociedade no ciberespaço, pois deste modo a comunidade global estará preparada para identificar possíveis notícias falsas, criadas com o intuito de difundir o pânico, o caos, e inverdades nas redes sociais digitais. A atuação dos *deepfakes* no ciberespaço objetiva disseminar a insegurança no que é transmitido pela rede mundial de computadores e, a contemporaneidade trata de assuntos diversos pela rede mundial de computadores, quer seja algo mais simples, quer seja algo de grande repercussão e influência mundial.

Conteúdos diversos são tratados pela internet: política, religião, compra e venda, moda, lazer, educação, nutrição e saúde são alguns dos exemplos. Uma infinidade e variedade de assuntos com acesso imediato nunca imaginado pelo ser

humano antes do advento das novas tecnologias. E a inteligência artificial evoluiu a ponto de se indagar o que é real? O que tem origem verdadeira em sua criação? Será que a máquina está manipulando a vontade humana? O que de fato é verdade e contribui para a evolução da espécie humana? Os questionamentos levam à reflexão sobre a utilização das máquinas e os conteúdos por elas difundidos. O objetivo que motivou a criação da inteligência artificial foi a ajuda que os seres humanos obteriam mediante esse advento tecnológico, entretanto, a contemporaneidade apresenta os *deepfakes* como uma falha no canal de cooperação entre homem e máquina, já que não é mais possível definir com precisão o que é verdadeiro e o que é montagem dissimulada.

A atuação dos *deepfakes* no Ciberespaço clama por uma regulamentação legal específica que garanta a segurança do que é divulgado à sociedade por meio da internet, que é uma ferramenta usual presente no cotidiano da comunidade mundial – dir-se-ia até mesmo indispensável na contemporaneidade. Os *deepfakes* necessitam somente da criatividade do editor e da quantidade de vídeos e áudios disponíveis na internet para que sejam modificados e divulgados como verdadeiros, criando uma cadeia mundial de publicação de inverdades. Essa ferramenta pode atingir a qualquer pessoa, seja ela figura pública ou um cidadão comum, já que usualmente publicam-se vídeos e áudios em todos os canais de comunicação que a rede mundial de computadores fornece. Faz parte do cotidiano humano se comunicar mediado pelas tecnologias digitais.

Poucas tecnologias são tão democráticas quanto à internet, pois sua utilização se dá por pessoas de lugares distintos e com graduações diferentes de conhecimento, todas com o mesmo acesso ao que é veiculado pelas mídias sociais digitais, dito isso, há que se levar em consideração dois pontos fundamentais ao se tratar dos *deepfakes*: o primeiro se relaciona com a criação recente dessa ferramenta de aprendizagem profunda, fazendo-se necessário a publicidade de sua atuação na rede mundial de computadores, pois os usuários da internet precisam conhecer o funcionamento dos *deepfakes*, estando cientes dos perigos por ele causados; em segundo e com um mesmo grau de importância se refere à necessidade de uma proteção jurídica que garanta o interesse público e a utilidade social das redes sociais digitais, que abrange toda a população mundial integrada e interconectada.

Por derradeiro, registra-se que a inteligência artificial utilizada nos *deepfakes* atua diretamente na desinformação global, reproduzindo informações falsas, enganosas, descontextualizadas e projetadas com o intuito de causar malfeitorias à coletividade, causando um colapso de confiança a tudo que é publicado na rede mundial de computadores – fato que exige dos usuários da internet uma verificação sobre a veracidade das informações recebidas. É notório que as redes sociais digitais influenciam diretamente o comportamento humano, desse modo, há que se pensar na importância da checagem dos fatos antes de compartilhá-los com toda a rede de amigos digitais, sendo esse o primeiro passo de confronto à desinformação provida por ferramentas da inteligência artificial. É responsabilidade humana a tutela dos princípios fundamentais em uma sociedade plural, democrática e interconectada.

Referências

- GIRARDI, Giuliana. **Brasil sofre com epidemia de desinformação sobre vacinas, revela estudo inédito**. Fantástico, São Paulo: Rede Globo, 10 de novembro de 2019. Reportagem Televisiva.
- GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.
- GUILLOU, Pierre. **Qual é o princípio de funcionamento de um algoritmo de inteligência artificial?** Disponível em <https://medium.com/@pierre_guillou/qual-é-o-principio-de-funcionamento-de-um-algoritmo-de-inteligência-artificial-d68619ce2b4>. Acesso em 02 de outubro de 2019.
- LARA et al. Implicações políticas, sociais e ética da popularização de *deepfakes* por meio de softwares livres. **Anais do Congresso Nacional Universidade, EAD e Software Livre**, v.2, n.9, 2018. Disponível em: <<http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/view/14431>>. Acesso em 10 de outubro de 2019.
- LAVAGNOLI, Silvia. **Como surgiu a Inteligência Artificial?** Disponível em: <<https://www.opencadd.com.br/como-surgiu-a-inteligencia-artificial/>>. Acesso em 01 de outubro de 2019.
- MATTOS, Matheus Carvalho de; SOUZA, Carlos Henrique Medeiros de; MANHÃES, Fernanda Castro. **A dromocracia cibercultural nas redes sociais digitais**. Revista Científica Internacional InterSciencePlace, v. 1, n. 21, p. 178-196. 2012. Disponível em: <<http://interscienceplace.org/isp/index.php/isp/article/view/208>>. Acesso em 10 de outubro de 2019.
- PATRINI, Giorgio; CAVALLI, Francesco; AJDER, Henry. **The state of deepfakes: reality under attack**. Annual Report v.2.3, 2018. Disponível em: <<https://s3.eu-west-2.amazonaws.com/rep2018/2018-the-state-of-deepfakes.pdf>>. Acesso em 01 de outubro de 2019.
- PRETI, Mariana. **Entenda o que é Algoritmo e qual o papel dele na sua vida**. Disponível em: <<https://c2ti.com.br/blog/entenda-o-que-e-algoritmo-e-como-ele-determinar-o-que-voce-ve-na-internet-tecnologia>>. Acesso em 01 de outubro de 2019.
- READS, Smart. **“Inteligência Artificial: Compreender em Que Consiste a I.A. e o Que Implica a Aprendizagem das Máquinas”**. Tradução de Patrícia Pinto. *Smart Reads*, 2017. Edição Kindle, 62p.
- RODRIGUES, Juliana Souza. **Para que serve a comunicação? “José Saramago”** – Texto na íntegra e comentário crítico. Disponível em: <<https://juhroyal.wordpress.com/2015/03/10/para-que-serve-a-comunicacao-jose-saramago-texto-na-integra-e-comentario-critico/>>. Acesso em 11 de outubro de 2019.

- RUSSELL, Stuart J.; NORVIG, Peter. **Inteligencia Artificial. Un Enfoque Moderno**. Tradução de Juan Manuel Corchado Rodríguez. 2. ed. Madrid: Pearson, 2004, 1240p.
- SIQUEIRA, Paulo Alexandre Rodrigues de. **O 'Deep Fake' e a Legislação Brasileira** – utilização de instrumentos legais para a proteção à imagem. Disponível em: <<https://www.conteudojuridico.com.br/consulta/artigo/53256/o-deep-fake-e-a-legislao-brasileira-utilizao-de-instrumentos-legais-para-a-proteo-imagem>>. Acesso em 11 de outubro de 2019.
- SPENCER, Michael K. **Deep Fake, a mais recente ameaça distópica**. Tradução de Gabriela Leite. Disponível em: <<https://outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia/>>. Acesso em 05 de outubro de 2019.
- SOUZA, Carlos Henrique Medeiros; COSTA, Marco Aurélio Borges. **Abordagens antropológicas do ciberespaço e da cibercultura**. Disponível em: <<http://www.portcom.intercom.org.br/pdfs/164913370240515589548494073408862492935.pdf>>. Acesso em 05 de outubro de 2019.
- TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet**: uma lei sem conteúdo normativo. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269>. Acesso em 10 de outubro de 2019.
- WACHTER, Sandra. The Guardian [entrevista]. **Mundo + Tech** (Blog Embratel). Disponível em <<https://mundomaistech.com.br/inteligencia-artificial/ha-um-lado-bom-no-deepfake/>> 2019. Acesso em 18mar.2020.
- YOUNG, Norbet. **DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media**. 2019. Edição Kindle, 160p.