VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

JONATHAN BARROS VITA

YURI NATHAN DA COSTA LANNES

D597

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

Coordenadores: Jonathan Barros Vita; Yuri Nathan da Costa Lannes – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-747-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

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

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O VI Encontro Virtual do CONPEDI, realizado em parceria com a Faculdade de Direito de Franca (FDF) e da Faculdades Londrina, entre os dias 20 e 24 de junho de 2023, apresentou como temática central "Direito e Políticas Públicas na Era Digital". Esta questão suscitou intensos debates desde o início e, no decorrer do evento, com a apresentação dos trabalhos previamente selecionados, fóruns e painéis que ocorreram virtualmente.

Os trabalhos contidos nesta publicação foram apresentados como artigos no Grupo de Trabalho "DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III", realizado no dia 23 de junho de 2023, que passaram previamente por no mínimo dupla avaliação cega por pares. Encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-Graduação em Direito, que retratam parcela relevante dos estudos que têm sido produzidos na temática central do Grupo de Trabalho.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes, os grupos temáticos para organização dos trabalhos ficou organizado da seguinte maneira:

1 – Inteligência Artificial, Marco Civil da Internet e Regulação

1. A EVOLUÇÃO TECNOLÓGICA E O IMPACTO DA INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO: UMA ANÁLISE DO DIREITO NA ERA DIGITAL - José Laurindo De Souza Netto , Higor Oliveira Fagundes , Amanda Antonelo

2. INTELIGÊNCIA ARTIFICIAL E O SISTEMA DE PRECEDENTES: PROJETO VICTOR DO SUPREMO TRIBUNAL FEDERAL - José Laurindo De Souza Netto , Higor Oliveira Fagundes , Amanda Antonelo

3. A INTELIGÊNCIA ARTIFICIAL NAS RELAÇÕES DE TRABALHO: A SUBORDINAÇÃO ALGORÍTMICA DOS MOTORISTAS DE APLICATIVO - Carlos Alberto Rohrmann , Alefe Lucas Gonzaga Camilo

4. CONSIDERAÇÕES ACERCA DA INTELIGÊNCIA ARTIFICIAL NA ARRECADAÇÃO DO ITBI NO MUNICÍPIO DE GAROPABA/SC: A(I)LEGALIDADE NA APURAÇÃO DA BASE DE CÁLCULO. - Agatha Gonçalves Santana , Ana Carolina Leão De Oliveira Silva Elias

5. OS CHATBOTS EM DESENVOLVIMENTO PELAS GRANDES EMPRESAS DE TECNOLOGIA: VANTAGENS, DESVANTAGENS E PRECAUÇÕES - Jamile Sabbad Carecho Cavalcante

6. DESAFIOS DA LEGISLAÇÃO DO CIBERESPAÇO NO BRASIL: UMA ANÁLISE SOB A PERSPECTIVA DA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS E DA AMPLIAÇÃO DA REGULAMENTAÇÃO - Marcelo Barros Mendes , Eduardo Augusto do Rosário Contani

7. O DIREITO DIGITAL, ARQUITETURA DA INTERNET E OS DESAFIOS NA REGULAMENTAÇÃO DO CIBERESPAÇO - Alex Sandro Alves , Eduardo Augusto do Rosário Contani

8. MARCO CIVIL DA INTERNET E A RESPONSABILIDADE DOS PROVEDORES DE APLICAÇÃO DE INTERNET: ANÁLISE DE DECISÕES JUDICIAIS SOBRE O ARTIGO 19 - Yuri Nathan da Costa Lannes , Jéssica Amanda Fachin , Stella Regina Zulian Balbo Simão

2 – Proteção de Dados

9. LESÃO MORAL CAUSADA PELA INTERNET E O DEVER DE PROTEÇÃO INTEGRAL: TUTELA DAS CRIANÇAS E ADOLESCENTES NO MEIO DIGITAL - Antonio Jorge Pereira Júnior, Patrícia Moura Monteiro Cruz

10. APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS CLÍNICAS MÉDICAS - Fábio Da Silva Santos, Saulo José Casali Bahia , Mario Jorge Philocreon De Castro Lima

11. LGPD E A DOUTRINA DA PROTEÇÃO INTEGRAL: UM OLHAR CRÍTICO PARA OS DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES NO BRASIL - Clara Cardoso Machado Jaborandy , Letícia Feliciana dos Santos Cruz , Lorenzo Menezes Machado Souza

12. DADOS PESSOAIS VERSUS DADOS SENSÍVEIS: QUANDO O VAZAMENTO DE DADOS PODE LEVAR AO DANO PRESUMIDO? ANÁLISE DA DECISÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA À LUZ DOS DIREITOS DA PERSONALIDADE - Tatiana Manna Bellasalma e Silva, Ivan Dias da Motta

13. BASES LEGAIS PARA A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS NA LEGISLAÇÃO ARGENTINA E URUGUAIA - Alexandre Weihrauch Pedro

14. A PUBLICIDADE COMO PRINCÍPIO CONSTITUCIONAL DA ADMINISTRAÇÃO PÚBLICA EM CONSONÂNCIA COM A PROTEÇÃO DE DADOS NOS CONTRATOS ADMINISTRATIVOS. - Sérgio Assis de Almeida, Zulmar Antonio Fachin

15. NO CONTROLE EFETIVO DO FLUXO INFORMACIONAL: OPERAÇÃO DE COMPENSAÇÃO COM A FAZENDA PÚBLICA POR CORRETORES DE DADOS NA VENDA DOS DADOS PESSOAIS PELO TITULAR - Valéria Fernandes de Medeiros, Ana Paula Basso

3 – Informação, Democracia, Negócios e Tecnologia

16. FAKE NEWS E DEEP FAKE - SEU EVENTUAL IMPACTO NO PROCESSO ELEITORAL DEMOCRÁTICO - Giullia Cordeiro Rebuá , Bruna Guesso Scarmagnan Pavelski , Mario Furlaneto Neto

17. OS GRUPOS DE INTERESSE NÃO PERSONALIZADOS E O COMBATE À DESINFORMAÇÃO NA ERA DA TECNOLOGIA PERMEADA PELAS FAKE NEWS: A PERSPECTIVA DE ATUAÇÃO DESSES ATORES NO AGRONEGÓCIO BRASILEIRO - Fabiane Velasquez Marafiga

18. A CRISE DA DEMOCRACIA NO REGIME DAS TECNOLOGIAS DE INFORMAÇÃO - Caroline Bianchi Cunha, Marina Witter Puss , Filipe Bianchi Cunha

19. O POLICENTRISMO (ESTADO E CIDADÃOS ATIVOS E RESPONSIVOS) E RADICALIZAÇÃO DEMOCRÁTICA - Cesar Marció , Clóvis Reis

20. GOVERNANÇA COMO INSTRUMENTO DE CONVERGÊNCIA DA RELAÇÃO ESTADO-SOCIEDADE - Vladimir Brega Filho, José Ricardo da Silva Baron, Ronaldo De Almeida Barretos

21. QUALIFICAÇÃO PROFISSIONAL NA ERA DIGITAL: A RESPONSABILIDADE SOCIAL DA EMPRESA COMO MEIO AUXILIAR NA TUTELA DE DIREITOS FUNDAMENTAIS - Nicole Schultz Della Giustina

22. SEGREDOS DE NEGÓCIO E ENGENHARIA REVERSA DE TESTES DO NOVO CORONAVÍRUS DURANTE A PANDEMIA DA COVID-19: UMA ANÁLISE SOB A ÓTICA DO DIREITO COMPARADO - Carlos Alberto Rohrmann , Ivan Luduvice Cunha , Sérgio Rubens Salema De Almeida Campos

4 – Saúde, Processo e Visual Law ante a tecnologia

23. NANOMEDICAMENTOS, SAÚDE HUMANA E RISCOS DO DESENVOLVIMENTO - Versalhes Enos Nunes Ferreira, Pastora Do Socorro Teixeira Leal

24. TUTELA DA TECNOLOGIA BLOCKCHAIN ÀS PESSOAS COM DUPLA DEFICIÊNCIA - Fabio Fernandes Neves Benfatti (Artigo integrante do Projeto contemplado pelo Edital 06/2021 - PROGRAMA DE BOLSAS DE PRODUTIVIDADE EM PESQUISA - PQ /UEMG, desenvolvido durante o ano de 2022)

25. O PRINCÍPIO DA INTEROPERABILIDADE E AS REPERCUSSÕES NO DIREITO PROCESSUAL BRASILEIRO - Solange Teresinha Carvalho Pissolato , Rogerio Mollica

26. VISUAL LAW: UMA ANÁLISE DA NECESSIDADE DE SIMPLIFICAÇÃO DA LINGUAGEM JURÍDICA DO MAGISTRADO ATRAVÉS DA NOÇÃO DE AUDITÓRIO DE CHAÏM PERELMAN - Priscila Vasconcelos Areal Cabral Farias Patriota, Samuel Meira Brasil Jr

Espera-se, então, que o leitor possa vivenciar parcela destas discussões por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Profa. Dr. Jonathan Barros Vita– UNIMAR

Prof. Dr. Yuri Nathan da Costa Lannes –FDF/ Mackenzie/Unicap

FAKE NEWS E DEEP FAKE - SEU EVENTUAL IMPACTO NO PROCESSO ELEITORAL DEMOCRÁTICO

FAKE NEWS, DEEP FAKE AND ITS EVENTUAL IMPACT IN DEMOCRATIC ELECTION PROCESS

Giullia Cordeiro Rebuá
Bruna Guesso Scarmagnan Pavelski
Mario Furlaneto Neto

Resumo

Sob a ótica do direito e da tecnologia, com emprego do método dedutivo e o procedimento metodológico de revisão doutrinária, busca-se enfrentar os impactos da disseminação das fake news e deepfakes no cenário do processo eleitoral democrático brasileiro, objetivando esclarecer se a manipulação da informação e a influência produzida no eleitorado seria cenário para a anulação do pleito eleitoral. Conclui-se, assim, que a disseminação massiva de notícias falsas através de bots e pela divulgação de vídeos deepfakes tem como principal objetivo influenciar e/ou modificar o resultado do pleito eleitoral por meio da manipulação da opinião pública na formação da sua intenção de voto, o que representa uma séria ameaça à democracia. Com efeito, essas ferramentas digitais devem ser combatidas de forma oficial e regulamentada para não ferir a liberdade de expressão ou de uso de redes sociais e apps de difusão de informações pessoais e gerais. Portanto, é importante destacar que a facilidade de compartilhamento de informações na internet aumenta os riscos da disseminação dessas notícias falsas, exigindo-se ação conjunta dos órgãos que compõem o sistema de justiça para prevenir e reprimir tais condutas.

Palavras-chave: Fake news, Direito eleitoral, Direito digital, Criminalização do deep fake, Combate às fake news

Abstract/Resumen/Résumé

From the perspective of law and technology, using deductive methods and a doctrinal review methodology, we seek to address the impacts of the dissemination of fake news and deepfakes in the Brazilian democratic electoral process, aiming to clarify whether the manipulation of information and the influence produced on the electorate would be grounds for the annulment of the election. Thus, it is concluded that the massive dissemination of fake news through bots and the publication of deepfake videos aims to influence and/or modify the outcome of the electoral process through the manipulation of public opinion in the formation of their voting intention, which represents a serious threat to democracy. Therefore, these digital tools must be officially and regulatedly combated so as not to infringe upon the freedom of expression or the use of social media and apps for the dissemination of personal and general information. It is important to note that the ease of sharing information on the internet increases the risks of the dissemination of this fake news,

requiring joint action from the organs that make up the justice system to prevent and repress such behavior.

Keywords/Palabras-claves/Mots-clés: Fake news, Elections laws, Digital law, Deep fake criminalization, Combat to fake news

1. INTRODUÇÃO

Desde que a sociedade passou a viver em um mundo inteiramente digital, todas as áreas da vida receberam diversas mudanças, sejam elas positivas ou negativas. Com o processo eleitoral, não foi diferente, muita coisa mudou, desde a campanha do pré-candidato até o fim de seu mandato, ou mesmo, depois de sua saída do mundo político.

As estratégias para se promover um candidato nos tempos modernos, são bem diferentes do que costumavam ser. Hoje, o candidato obrigatoriamente deve possuir uma rede social forte e frequentemente ativa, para alcançar seus eleitores já garantidos, assim como outros possíveis optantes, através de postagens que apresentem suas propostas, ideias e ideais. Esse tipo de serviço pode ser feito de maneira orgânica, ou simplesmente um conteúdo pago e patrocinado.

Acontece que, no processo eleitoral democrático, mesmo em seus primórdios, a autopropaganda não é o único recurso para angariar votos. Um dos mais eficazes e mais utilizados é, na verdade, macular de alguma forma a reputação de outros candidatos durante a época das eleições ou pouco antes de seu início, utilizando recursos que moldem a opinião do eleitor, e direcionem suas opiniões e, portanto, seu voto. Dessa forma, surgem as fake News e, posteriormente (e mais atualmente) os deep fakes. Estes são utilizados amplamente em época de campanha eleitoral e fora dela, durante o mandato do candidato eleito, para manipular de maneira subconsciente a opinião e o voto público à espera da chegada de um novo processo eleitoral.

Este artigo, portanto, trata-se de uma pesquisa científica que se aprofunda no significado de tais termos, como são utilizados e disseminados esses recursos midiáticos e tecnológicos e de que forma impactam no processo eleitoral democrático e no cotidiano do cidadão da República Democrática Brasileira. Assim sendo, o trabalho é dividido em quatro partes: conceito, definição e impacto das fake News; conceito, definição e impacto de deep fake; projetos de lei para combater a disseminação de fake News, deep fakes e manipulação de informações; e, por fim, as conclusões mais efetivas para combater a disseminação massiva destes através de bots e a produção de vídeos nocivos através de apps e programas de deep fake.

2. CONCEITO, DEFINIÇÃO E IMPACTO DAS FAKE NEWS

Um tópico amplamente utilizado, e frequentemente abordado em uma gama de nichos de influência, mas majoritariamente no político e eleitoral são as “Fake News”. A expressão começou a ganhar força com as eleições americanas de 2016, vencidas por Donald Trump, e

onde ocorreram esquemas envolvendo bancos de dados pessoais e manipulações de conteúdo, e que, aqui no Brasil, começou a se popularizar nas eleições de 2018.

> O fenômeno das fake news, disseminação de notícias falsas com fins políticos, atingiu uma dimensão global, tendo sido identificado como um dos principais desafios dos processos democráticos contemporâneos. No contexto eleitoral, as fake news podem distorcer o debate público, influenciar indevidamente a escolha do eleitorado e comprometer a legitimidade das eleições" (GONÇALVES, 2021, p. 18).

Com a ampla disseminação de “fake news”, os resultados do processo eleitoral se instabilizaram, havendo grande dúvida quanto à integridade das informações passadas pelos veículos de mídia, e principalmente aquelas encaminhadas através de mídias sociais e aplicativos como o “Whatsapp”.

Através desse cenário, as militâncias ganharam força, não mais importando a veracidade do conteúdo, mas sim se este era prejudicial ou não ao candidato apoiado, este atributo se tornando o meio de julgamento da credibilidade de cada notícia para um fiel eleitor de qual candidato fosse. Conforme o autor Klaus Schwab:

> Os governos devem também se adaptar ao fato de que o poder também está passando dos atores estatais para os não estatais e de instituições estabelecidas para redes mais abertas. As novas tecnologias e os agrupamentos sociais e interações que elas promovem permitem que praticamente qualquer pessoa exerça influência de maneira que teria sido inconcebível há apenas alguns anos. (SCHWAB, 2016, p. 70).

Sendo assim, utilizando-se desse poder oriundo da utilização das grandes mídias sociais exercido por essas vertentes de militância, seus líderes, e principalmente pelos chamados influenciadores digitais, isso torna-se um conteúdo prejudicial e questionável, que terá mais material disponibilizado para denegrir de alguma forma a imagem de indivíduos públicos, sejam candidatos ou não, através do novo software “Deep Fake”, que ganha cada vez mais força no mercado como um aplicativo utilizado para gerar conteúdo “escrachado” e humorístico, mas concorre como real ameaça para a máquina eleitoral e a democracia desta União.

Como tudo tem uma origem, a preocupação com a difusão de notícias inverídicas em massa através de meios digitais também, e provém das famosas “fake news”. O termo em inglês, traduzido livremente para o português, significa notícia falsa. Essa expressão é usada para mencionar qualquer informação fabricada, não só reportagens completas, devido à proporção de danos e desinformação infligidos e divulgados para a população. No Brasil, acabou se tornando uma gíria para falar sobre qualquer informação falsa que seja, que leve a opiniões e ideais errôneos, mesmo que seja um mínimo comentário.

Vale ressaltar, que o termo teve início nos meios mais tradicionais de comunicação, como o jornal impresso, rádios e televisão, atingindo seu auge após a popularização e

crescimento das redes sociais, através das quais foi amplamente propagado. A informação apresentada pode ser criada por qualquer pessoa, em qualquer lugar, desde perfis pessoais, pequenos blogs e tabloides sensacionalistas à grande mídia.

O interessante é saber que existem vários tipos de fake news, como classificado pela professora e Ph.D. na área de mentiras em redes sociais, Claire Wardle, que as define em sete tipos, que são: **as sátiras e paródias, falsas conexões, conteúdos enganosos, contexto falso, conteúdo impostor, conteúdo manipulado e conteúdo fabricado.**

A **sátira ou paródia** é geralmente ligada à ironia e humor, onde a falsidade não tem o intuito da maldade, mas tem o potencial para ludibriar o leitor, como no exemplo aqui do Brasil, onde temos o "Jornal Sensacionalista". A **falsa conexão** é derivada da mídia tradicional, quando temos um título de matéria em destaque, porém não tem conexão com o conteúdo do texto, uma grande artimanha de jornais e revistas para vender mais, prendendo a atenção e curiosidade do leitor, e nos mundos digitais, o termo é conhecido como "click bait", traduzido como isca para clicar.

O **conteúdo enganoso**, como o próprio nome já diz, é quando a informação é utilizada como ferramenta de iludir o leitor. Enquanto o **conteúdo falso** se dá quando informações irreais são adicionadas ao fato verdadeiro, com o objetivo de enganar, impressionar ou até confundir o leitor. Já **conteúdo impostor** é aquele em que não só a informação é falsa, mas principalmente as fontes são mentirosas, geralmente de grandes mídias para tentar uma maior credibilidade para o texto, por exemplo, vinculando um endereço do G1 a um texto particular, geralmente bastando ao leitor leigo a menção ao portal, este não se importando em aprofundar suas buscas.

O **conteúdo manipulado** é dado através da utilização principalmente de imagens para enganar o leitor, como por exemplo, as famosas montagens na internet, de maneira a manipulá-lo a crer que há provas daquele acontecimento. Por fim, temos o **conteúdo fabricado** que, diferente do conteúdo falso, não possui nenhuma verdade nos fatos, sendo criado um conteúdo completamente irreal, com o objetivo de atacar ou prejudicar uma pessoa, ou empresa.

Em se falando do impacto das fake news, para mensurá-los pode-se analisar o caso da Cambridge Analytica nos Estados Unidos e no Reino Unido durante as eleições de Donald Trump e a aprovação do Brexit. Com um banco de dados de cada usuário, coletados por redes sociais e outras formas, as notícias falsas eram direcionadas de forma específica. Se o usuário estivesse ligado a conteúdos sobre a economia, a empresa patrocinava publicações falsas sobre a taxa de desemprego nos Estados Unidos, ou no caso dos britânicos, fornecia informações de que o Reino Unido perdia milhões de dólares semanais, enquanto membro da União Europeia. Se a maioria dos conteúdos estivesse ligado com segurança nacional, a empresa patrocinava

conteúdos de notícias falsas, onde a candidata rival Hillary Clinton tinha alguma responsabilidade pela criação do Estado Islâmico.

Portanto, ficou mais do que provado que as fakes news conseguem influenciar diretamente em uma eleição, pois definiu o destino da maior economia do mundo, e conseguiu mudar a economia do Reino Unido. Devemos nos atentar como não cair e proliferar as fake news, principalmente em períodos eleitorais.

Decorrido disso, a IFLA (International Fact-Checking Network) publicou uma normativa que auxilia os usuários a diferirem uma notícia íntegra de fake news. Algumas assertivas podem soar básicas, porém, grande parte do público, principalmente de idade superior a 35 anos, não tinham o costume de colocá-las em prática durante a checagem de uma informação.

Além disso, fica claro como é mais difícil determinar uma fake news antes de muitas pessoas terem-na veiculado visto a rapidez com que o ciclo de informações funciona atualmente, e a disseminação de comentários, discussões e atualizações de redes sociais sobre determinados assuntos, conforme citado abaixo:

> Por causa do ritmo acelerado das mudanças desencadeadas pela quarta revolução industrial, os reguladores estão sendo desafiados a um grau sem precedentes. Atualmente, as autoridades políticas, legislativas e reguladoras são muitas vezes ultrapassadas pelos acontecimentos, incapazes de lidar com a velocidade da mudança tecnológica e a importância de suas implicações. O ciclo de notícias de 24 horas pressiona os líderes a comentar os eventos ou agir imediatamente, reduzindo o tempo disponível para obter respostas calculadas, valoradas e calibradas. Há um perigo real de perda de controle sobre os temas importantes, especialmente em um sistema global, com quase 200 Estados independentes e milhares de línguas e culturas diferentes (SCHWAB, 2016, p. 72).

As dicas incluem sempre considerar as fontes das publicações, verificar se a fonte tem mais temas que se assemelhem ao assunto abordado, se o autor ou veículo de postagem tem ligação positiva ou negativa (a depender do tipo de informação) com a pessoa/objeto ao redor do qual gira a informação, se outros veículos também estão citando essa situação sob as mesmas circunstâncias, e checar também os autores quanto às suas ideologias pessoais e seu histórico com relação à imparcialidade sobre o assunto em questão. Caso a matéria possua fontes externas, deve também checá-las, tanto sua credibilidade quanto a veracidade das informações utilizadas para tal dado.

Outra prática importante, é ler a informação/matéria/publicação por completo, e não apenas seu título ou “thumbnail”, visto que em sua maioria são sensacionalistas e, como são chamadas hoje “click bait”, que seria a informação de forma exagerada para chamar atenção do público e levar ao seu consumo. É importante levar em consideração a data de postagem, visto que a progressão da sociedade leva a mudanças e transforma costumes em atitudes imorais e

vice-versa. Seguindo essas dicas o usuário se torna menos propenso a ser pego pelas falsas informações ou compartilhá-las erroneamente com seus próximos.

Há ainda algumas ações tomadas mais recentemente por alguns aplicativos de redes sociais para combater esse tipo de conteúdo. Por exemplo, o selo "False Information" (Informação Falsa) do Instagram, que é um recurso lançado em dezembro de 2020 e visa combater a disseminação de informações falsas na plataforma. Quando um post é sinalizado como informação falsa por verificadores independentes de fatos, o Instagram adiciona um selo de aviso ao post, informando aos usuários que o conteúdo é contestado.

O selo exibe um ícone de ponto de exclamação dentro de um triângulo vermelho e inclui um texto informando que o conteúdo do post foi verificado por analistas independentes e considerado total ou parcialmente falso. Além disso, também é limitada a distribuição desses posts sinalizados, reduzindo seu alcance e impedindo que eles apareçam nas pesquisas de hashtags e na aba "Explore".

O objetivo do selo "False Information" é aumentar a conscientização dos usuários sobre a veracidade das informações que encontram na plataforma e incentivar a checagem de fatos antes de compartilhar conteúdo duvidoso. Ele é um dos esforços do Instagram para combater a disseminação de informações falsas e promover um ambiente mais seguro e confiável na rede social.

Mesmo tomando cuidado com todas essas pontuações supracitadas, ainda há constante desenvolvimento de novas ferramentas focadas na disseminação de falsas e tendenciosas informações, como é o caso do novo Deep Fake.

3. CONCEITO, DEFINIÇÃO E IMPACTO DE DEEP FAKE

O deep fake é a tecnologia mais atual, integrada com uma inteligência artificial focada em “machine learning” com o intuito de criar conteúdo falso e realista, utilizando a imagem de pessoas relevantes, como vídeos íntimos falsos de pessoas famosas, ou discursos fictícios de políticos influentes. Basicamente o algoritmo da inteligência artificial, através de um banco de dados, consegue manipular imagens, áudios, movimentos e expressões. Como o deep fake foi criado com o intuito de criar informações, vídeos e fotos falsas, pode-se considerar como uma subcategoria de fake News.

A expressão deriva de duas palavras em inglês *deep* (profundo), que é derivada de *deep learning* (aprendizado profundo), com *fake* (falso) já definido anteriormente. Essa linha da informática chamada *deep learning* é derivada do famoso *machine learning* (máquina

aprendendo). Desde a década de 50, os maiores pesquisadores da informática começaram os estudos da inteligência artificial, e começaram a estudar os algoritmos, e foram aprendendo como funcionam. A ideia do *machine learning* é literalmente colocar a máquina para aprender sozinha a partir de dados introduzidos em sua programação; um exemplo do uso de *Machine Learning* é "a identificação de spams, onde inicialmente é fornecido e-mails rotulados como spams e a partir disso o software AntiSpam deverá identificar, nos próximos e-mails que forem recebidos, padrões para que possa classificá-los como spam ou não spam". Basicamente, encontrar-se-á o *Deep Learning*, este é "um tipo de *Machine Learning* que capacita a máquina a realizar tarefas mais complexas, como reconhecimento de fala, identificação de imagens e realizar previsões" (DAMACENO, 2018, p. 13).

O supracitado trata-se de um software de inteligência artificial cuja utilização por um programador facilmente pode resultar em uma cópia exata do rosto e voz de um indivíduo (no nosso caso em questão, de um candidato) atestando qualquer tipo de informação ou comportamento desejado pelo desenvolvedor do conteúdo. Para que esse conteúdo seja descredibilizado e os fatos desmentidos, há a necessidade de uma perícia técnica especializada, que demanda tempo e gastos. Além disso, com o imediatismo e a praticidade que a tecnologia e as redes sociais nos proporcionam, o conteúdo já haveria sido divulgado amplamente de uma forma que a perícia e o esclarecimento da situação não poderiam ser, resultando em grandes e quase inevitáveis riscos de dano irreversível à imagem do candidato em questão e ao resultado das eleições.

> As deepfakes têm um enorme potencial para disseminar desinformação, manipular a opinião pública e desestabilizar a democracia. Além disso, as deepfakes podem ser usadas como ferramentas para difamação, perseguição, chantagem e extorsão. A sociedade precisa estar ciente dos riscos associados às deepfakes e trabalhar para desenvolver ferramentas e estratégias que possam detectar e neutralizar essas ameaças (SANTOS, LIMA, BORGES e DIAS, 2020).

Um bom exemplo popular do uso de deep fake, mesmo que seja *masterizado* pela obra em questão, é o arco dramático da nova novela das 22h "Travessia", do canal Globo, onde crianças brincando com o aplicativo de deep fake trocaram o rosto de uma sequestradora de crianças pelo rosto de uma das personagens da trama, causando sua acusação e linchamento virtual após a viralização do conteúdo criado a partir do aplicativo. Além disso, houve outros exemplos, como o caso do vídeo manipulado onde Barack Obama ofende Donald Trump, ou Luiz Inácio Lula da Silva diz que gosta de uma "paçoca" específica de uma fazenda, além do vídeo que mostraria Mark Zuckerberg admitindo um roubo e tráfico ilegal de informações de todos os usuários de suas mídias sociais.

Em uma maior escala danosa, há, por exemplo, a possibilidade da criação de um vídeo dos atuais presidentes da Ucrânia ou Rússia anunciando rendição de suas tropas e aceite de quaisquer demandas do inimigo. Estando em uma situação precária e com acesso limitado à internet e informações, os militares poderiam acatar essas ordens, causando grandes perdas e danos irreversíveis à estratégia e posição no conflito para a potência em questão, gerando várias baixas ou até mesmo perda de territórios resguardados pelas tropas.

Antigamente eram comuns montagens grotescas de rostos de pessoas substituindo o de celebridades, era nítida e perceptível a diferença. Acontece que, em 2017, em um dos fóruns mais famosos da internet, o Reddit, um usuário com esse nome "deep fake" começou a postar vídeos íntimos de celebridades.

Logo o *post* chamou a atenção, pois como as pessoas eram famosas, rapidamente os vídeos rodaram o mundo, e começaram os questionamentos. Foi averiguado que eram vídeos já antigos, da indústria adulta, porém o rosto das atrizes foi substituído pelo rosto das outras celebridades, de uma maneira nunca vista e quase imperceptível, sendo reconhecida como montagem apenas quando alguém reconheceu o ambiente, ou qualquer outra coisa na montagem, e comparou com o vídeo original.

Mesmo sabendo que esse recurso de montagem em vídeo já não é mais uma novidade, já que a indústria cinematográfica de Hollywood já utiliza esse artifício a muito tempo, o fator preocupante do deep fake é que, diferente do cinema, que possui um custo de milhões, e demanda uma grande quantidade de tempo, o usuário até então apresentou o uso de uma tecnologia "caseira", que possuía a mesma eficácia da indústria do cinema, só que com o custo infinitamente menor, e melhor autonomia de tempo.

Quanto a sua criação, é feita a partir de uma técnica criada a partir de programação de inteligência artificial, o aplicativo procura em bancos de dados imagens suficientes do indivíduo para criar um tipo de modelo 3D de suas feições que possibilite a movimentação e atuação de forma livre, a ser inserido num vídeo já feito ou a ser feito já com a manutenção do aplicativo durante sua gravação, buscando também o timbre de voz da pessoa sempre que possível (visto que também há possibilidade de utilizar imagens até mesmo de pessoas como William Shakespeare, por exemplo, cuja voz é desconhecida).

Quando houver arquivos de gravação de áudio e vídeo originais do indivíduo a ser falsificado, a IA também se encarrega de copiar o timbre da maneira mais exata possível, usando o resultado para sobrepor a voz original da pessoa gravada no vídeo, resultando em um material assustadoramente realista e extremamente difícil de ser reconhecido como fraude por pessoas comuns/leigas, havendo algumas alternativas para a sua descredibilização: análise

técnica, um pronunciamento do próprio autor e/ou disseminador do conteúdo atestando sua inveracidade ou a análise atenciosa do usuário, visto que normalmente a IA não consegue devidamente reproduzir devidamente os movimentos das pálpebras - não piscando com tanta frequência, ou piscando mais que o normal e de maneira estranha, ou apenas deixando de piscar os olhos – e o movimento da respiração, natural do ser humano, ambos podendo ser notado pelos olhos humanos quando analisado com atenção devida.

4. PROJETOS DE LEI PARA COMBATER DISSEMINAÇÃO DE FAKE NEWS, DEEP FAKES E MANIPULAÇÃO DE INFORMAÇÕES.

Como todo instrumento prejudicial ao bem individual e/ou coletivo, essas ferramentas digitais devem ser combatidas de forma oficial, porém de maneira regulamentada buscando não ferir a liberdade de expressão ou de uso de redes sociais e apps de difusão de informações pessoais e gerais.

Isto porque, o desenvolvimento tecnológico está atrelado a liberdade e, é visto um fenômeno por si só positivo, pois, significa o progresso e este é sempre intrinsecamente bom (DE CARVALHO, 1997, p. 2). Todavia, devem ser observados os preceitos já elencados por Bobbio (2004, p. 96) em referência aos direitos da nova geração que "nascem todos dos perigos à vida, à liberdade e à segurança, provenientes do aumento do progresso tecnológico, haja vista que "entramos na era que é chamada de pós-moderna e é caracterizada pelo enorme progresso, vertiginoso e irreversível, da transformação tecnológica e, consequentemente, também tecnocrática do mundo".

Com efeito, houve a alteração do Código Eleitoral através da lei 13.834/2019, em que incluiu o art. 326-A para tipificar a denunciação caluniosa eleitoral, no caput, e a divulgação de fake news, no parágrafo terceiro, não sanando completamente o problema, visto que, por mais que tenha facilitado o trabalho do judiciário que se ocupou na maior parte das eleições ocorridas em 2018 de derrubar diversas postagens caluniosas e danosas à reputação e posição na competição eleitoral, nem de longe cobriu todas as categorias de disseminação de tais informações pervertidas ou delimitou claramente a proibição e sanção de certos atos danosos que se encaixam na mesma seara.

Nesse sentido, foram submetidas as PLs 413/2017 e 2630/2020, que encontram-se em trâmite legislativo para serem aprovadas e vigoradas de forma a não atropelar ou restringir os direitos e deveres dos cidadãos a liberdade de imprensa, mas ainda assim procurando impedir a disseminação de tais informações prejudiciais ao acesso à verdadeira informação, ao processo

eleitoral justo e a uma escolha livre de candidatos no momento da votação, que seja baseada em seus projetos, conduta e trabalho, não em informações enganosas, sejam completamente falsas ou manipuladas de forma a impactar negativamente sua campanha e o julgamento pessoal do público eleitoral.

Além disso, em esforço ao combate às fake news, o TSE realizou diversas ações como a criação do Conselho Consultivo sobre Internet e Eleições (portaria 949/2017), Seminário Internacional Fake News: Experiências e Desafios, bots com o objetivo de tirar dúvidas de eleitores, que funcionam como assistentes virtuais.

Aprofundando-se um pouco sobre o PL 407/2017, ele busca barrar o uso de ferramentas automatizadas para disseminação de tais notícias enganosas e danosas, cujo número dentre os demais usuários disseminadores de informações e comentários na cena virtual de debate político informal era de aproximadamente 20% segundo pesquisa realizada pela Fundação Getúlio Vargas na época de proposição do projeto. Mas o que seriam essas ferramentas enganosas?

5. BOTS: COMO FUNCIONAM, SUA UTILIZAÇÃO NA PROPAGAÇÃO DA DESINFORMAÇÃO E AS MEDIDAS DE REGULARIZAÇÃO NO MERCADO E NA LEI

Inobstante, se trata de “bots”, perfis falsos automatizados por meio de projetos de linguagens de programação específica escolhida pelo programador, que automatiza o processo de encaminhamento para diversos números de WhatsApp, ou em comentários de redes sociais como Facebook e Instagram.

Importante mencionar que o termo "robot" surgiu pela primeira vez na “peça teatral R.U.R. (*Rossum’s Universal Robots*) publicada em 1920 pelo dramaturgo checo Karel Čapek, cujo significado advém da palavra checa robota, ´trabalho forçado´”, e foi utilizado para descrever um “ser autômato de aparência humana capaz de realizar todo tipo de tarefa no lugar do homem” (DE PAULA; MICHALSKI, 2019, p. 3).

O *robot* da vida real ou *bot* como é popularmente conhecido, “não possui forma física e vive nos recônditos da internet executando tarefas e procedimentos longe da visão do usuário comum” (DE PAULA; MICHALSKI, 2019, p. 3).

Deveras, os bots podem ainda funcionar a partir de disseminação de notícias prontas, mensagens inflamadas e apelativas, listagem de informações enganosas e etc.; ou a partir de filtragens de palavras específicas em comentários aleatórios, para onde o “bot” será direcionado a responder de forma padronizada, pré-programada pelo criador do código automatizador, refutando com informações enganosas e respostas apelativas o autor do comentário.

Na maioria das vezes, a conta terá fotos aleatórias de objetos generalizados como flores, por exemplo, ou uma foto de um elemento que identifique o candidato, partido, grupo ou ideologia em questão, ou do próprio candidato, com nomes também aleatórios e generalizados.

A ideia é que haja um bom número de bots automatizados para disseminar aquele conteúdo de forma quantitativa, buscando generalizar a informação para que não haja mais a possibilidade de identificar a origem, e que muitas pessoas cujo ideal se encaixe na informação se agradem e concordem com o conteúdo, disseminando-o cada vez mais e tomando-o como uma verdade indiscutível, muitas vezes um argumento em discussões que mesmo refutado continue tendo credibilidade entre o grupo a ser atingido. Corrobora com tais afirmações o autor:

> Os bots piratas podem ser programados para realizar várias atividades em redes sociais, como enviar mensagens automatizadas, curtir postagens, compartilhar informações falsas e influenciar a opinião pública. Essas táticas podem ser usadas em campanhas políticas para manipular as discussões online, espalhar desinformação e influenciar o resultado das eleições (HOWARD, 2019, p. 339).

Isso traz mais e mais pessoas à legião de "odiadores" de uma ideologia ou um candidato, assim como mais pessoas que preguem a ideologia e o candidato cuja equipe está por trás da contratação desse método de disseminação, que passam a acreditar que o candidato A ou B é a melhor opção, ou que este é um mal a ser combatido. Isso é reforçado pelos seguintes dados colhidos na obra de Francisco Brito Cruz:

> Segundo estudo desenvolvido pela FGV-SP em 2017, "bots" foram responsáveis Por mais de 10% das interações no twitter durante as eleições presidenciais de 2014, 20% de debate entre os vários favoráveis a Dilma no contexto do impeachment e quase 20% das interações no debate entre os apoiadores de Aécio Neves no segundo turno das eleições 2014. A Symantec, empresa multinacional que atua no setor de cibersegurança, destacou, em relatório lançado em 2016, que o Brasil hospeda o oitavo maior número de "bots" no mundo. (CRUZ, 2018, p. 151).

Todavia, o bot não é de "todo mal", visto que existem vários tipos como os chat bots, que aceleram o atendimento online de empresas e até mesmo de órgãos da máquina pública como o ganha-tempo e o site da delegacia, e os social bots, que fazem postagens de forma automática e interagem com seguidores ou público eventual nas contas de redes sociais, movimentando de forma mais efetiva o usuário na mídia e mantendo sua frequência alta para evitar diminuição na entrega de conteúdos e "publis", como para seus acompanhadores.

> Assim, o uso de bots é relativamente comum e disseminado: eles já desempenham uma série de tarefas básicas para nossa navegação na internet. A operação de **mecanismos de busca** – como o google – é baseada em grande parte no funcionamento de bots que processam e organizam a informação que é objeto de pesquisa. Em verdade, 61,5% de todo o tráfego na internet é realizado por programas automatizados, fato que também ocorre nas redes sociais (CRUZ, 2018, p. 153).

O serviço de bot de atendimento, também conhecido como chatbot, é um programa de computador projetado para realizar conversas com usuário sem linguagem natural. Eles podem ser usados em diversas áreas, como atendimento ao cliente, suporte técnico, vendas, entre outras. Reforça essa definição o autor:

> Os chatbots são programas de computador que utilizam técnicas de processamento de linguagem natural para simular conversas humanas. Eles podem ser usados em diversas aplicações, como atendimento ao cliente, vendas, suporte técnico, entre outras.(BARRIOS, 2019, p. 10).

Existem basicamente dois tipos de chatbots: os baseados em regras e os baseados em inteligência artificial. Aqueles baseados em regras são programados para seguir um conjunto específico de instruções, geralmente por meio de uma árvore de decisão. Eles podem responder a perguntas simples e fornecer informações básicas. No entanto, têm limitações quando se trata de conversas mais complexas ou com usuários que fazem perguntas fora do padrão.

Já os chatbots baseados em inteligência artificial são capazes de aprender com as conversas e melhorar suas respostas ao longo do tempo. Eles usam algoritmos de processamento de linguagem natural (NLP) para entender as intenções dos usuários e gerar respostas mais precisas e personalizadas. Estes são mais sofisticados e eficazes para lidar com uma ampla variedade de perguntas e situações.

Os chatbots de atendimento podem ser integrados a diversos canais de comunicação, como sites, redes sociais e aplicativos de mensagens. Eles são capazes de lidar com grande volume de solicitações simultaneamente e podem ajudar a reduzir os custos e o tempo de espera para atendimento ao cliente. No entanto, é importante lembrar que, embora possam ser muito úteis, eles não substituem completamente o atendimento humano, principalmente em situações mais complexas e sensíveis.

Claro, existem vários exemplos de chatbots úteis e inovadores que podem ser citados em um artigo acadêmico. Alguns exemplos são:

I. **Chatbot de atendimento ao cliente:** muitas empresas utilizam chatbots para oferecer suporte e atendimento aos clientes. O chatbot pode ser programado para responder às perguntas mais frequentes dos clientes, coletar informações de contato e encaminhar o cliente para um atendente humano, se necessário.
II. **Chatbot de agendamento:** alguns consultórios médicos e serviços de beleza, por exemplo, usam chatbots para permitir que os clientes agendem seus compromissos online. O chatbot pode coletar informações sobre o serviço desejado, horários disponíveis e confirmar o agendamento com o cliente.

III. **Chatbot de notícias:** alguns veículos de comunicação utilizam chatbots para fornecer notícias e informações atualizadas aos seus leitores. O chatbot pode ser programado para enviar notícias em tempo real, permitir que o leitor selecione o tipo de notícia que deseja receber e até mesmo personalizar o conteúdo com base nos interesses do leitor.

IV. **Chatbot educacional:** algumas instituições educacionais usam chatbots para fornecer informações sobre cursos e programas de graduação, responder às perguntas dos alunos e ajudar os estudantes a escolher suas disciplinas eletivas.

V. **Chatbot de suporte técnico:** muitas empresas de tecnologia usam chatbots para oferecer suporte técnico aos usuários. O chatbot pode coletar informações sobre o problema do usuário e oferecer soluções possíveis, ou encaminhar o usuário para um atendente humano se o problema for mais complexo.

Nota-se que o uso de *Chatbots* no aprendizado de línguas estrangeiras são "de grande valia no processo de ensino, uma vez que permitem aos alunos a possibilidade de imersão mais intensa na prática dos conceitos adquiridos"; além disso a aplicação do *Chatbot, "*no contexto de promover hábitos saudáveis, demonstra-se um aliado em potencial para alcançar uma parcela significativa de adolescentes, fornecendo respostas satisfatórias para suas dúvidas sobre sexo, drogas e álcool" (SÔNEGO; BERNARDINI; POZZEBON, 2018, p. 7).

Portanto, o *Chatbot "*funciona a partir da inserção, por parte do usuário, de uma pergunta ou comentário, sendo que a partir deste momento, o programa responde a pergunta, faz um comentário ou inicia um novo tópico". Esta ferramenta, como dito alhures, pode ser "aplicada em sistemas de navegação para automóveis, informações meteorológicas, orientações na programação de canais de televisão (...)" (SÔNEGO; BERNARDINI; POZZEBON, 2018, p. 3-7).

E estes são apenas alguns exemplos de como os chatbots podem ser usados para fornecer benefícios úteis e éticos para a sociedade. É importante lembrar que a criação de chatbots deve sempre levar em consideração as necessidades do usuário e seguir práticas éticas e responsáveis.

A programação é fundamental para o desenvolvimento de bots piratas usados para disseminar fake news. Para criar esses programas, é necessário utilizar linguagens de programação como Python, Ruby, Java, entre outras. Essas linguagens permitem aos desenvolvedores criar bots que podem interagir com as APIs (Application Programming Interfaces) das redes sociais, como Twitter, Facebook, Instagram, Whatsapp etc. Essa foi uma prática comum em meio a pandemia para disseminação de desinformação, conforme citado:

> De fato, a pandemia do coronavírus ocorre na era da informação, onde vive-se em um contexto digital, não-linear, globalizado, informatizado, conectado, tecnológico e acelerado, e onde a informação é compartilhada e disseminada mundialmente em fração de segundos. Assim, com o aumento do uso da Internet, de ferramentas colaborativas e de comunicação, além de uma maior utilização de redes sociais, tornou-se mais perceptível a ocorrência de alguns fenômenos informacionais, como a disseminação de informações falsas (muitas vezes potencializadas pela utilização de agentes autônomos computacionais), a chamada desinformação, que, em meio ao turbilhão informacional, aumentam a proporção dos sentimentos de incerteza em meio à pandemia (LIMA, 2022, p. 124).

Uma das principais técnicas utilizadas na programação de bots piratas é a automação. Isso significa que os desenvolvedores criam scripts que executam tarefas repetitivas em grande escala, como enviar mensagens, curtir e compartilhar conteúdo automaticamente, como já foi citado anteriormente. Isso permite que os bots se comportem como usuários reais, interagindo com outras contas e ampliando a disseminação de informações falsas.

Outra técnica importante é o uso de algoritmos de aprendizado de máquina[1]. Esses algoritmos permitem que eles aprendam a se comportar de maneira mais eficiente, melhorando a precisão na identificação de contas de usuários reais e na disseminação de fake news. Por exemplo, um bot pode aprender a identificar as melhores horas do dia para enviar mensagens, ou quais palavras-chave usar para aumentar a probabilidade de que uma mensagem seja compartilhada.

É importante ressaltar que a programação de bots piratas para disseminação de informações falsas é ilegal e antiética. Conforme preceituam Waldman; Lima e Uelze (2023, p.19) o que parece inegável é as *fake news* "importam em prejuízo a comunicação social, as primeiras através da deturpação dos fatos ou realidade objetivamente considerada, enquanto no caso da pós-verdade o vício decorre da distorção trazida pela sua interpretação tendenciosa e, mesmo, antiética".

As redes sociais têm políticas rigorosas de uso e detecção de bots, e o uso de suas versões piratas para disseminar fake news pode levar a punições severas, como a suspensão de contas ou até mesmo processos criminais. Além disso, a disseminação de informações falsas prejudica a credibilidade das redes sociais e é uma ameaça à democracia, comprometendo a capacidade dos eleitores de tomar decisões informadas com base em informações precisas e confiáveis.

Nesse ínterim, as notícias falsas proporcionam prejuízos à democracia, cujas consequências negativas não se restringem à divulgação do conteúdo em si, mas face à sua

1 Modo de Aprendizado Sempre que todo o conjunto de treinamento deva estar presente para o aprendizado, o modo de aprendizado de um algoritmo é não-incremental, também conhecido como modo *batch*. Por outro lado, se o indutor não necessita construir a hipótese a partir do início, quando novos exemplos são adicionados ao conjunto de treinamento, o modo de aprendizado é incremental. Portanto, no modo incremental o indutor apenas tenta atualizar a hipótese antiga sempre que novos exemplos são adicionados ao conjunto de treinamento (MONARD; BARANAUSKAS, 2003, p. 45).

amplificação (WALDMAN; LIMA e UELZE, 2023, p. 20) . Brites, Amaral e Catarino (2018, p. 86) enfatizam que, a partir daí, se estabelece um bloqueio emocional ou de crença, que prejudica o restabelecimento da verdade, ditada pela indignação causada pela notícia falsa, em especial aquelas aviltantes, a promover novo ciclo de desordem da informação (*information disorder*).

Para criar chatbots de WhatsApp, os programadores geralmente utilizam plataformas de desenvolvimento específicas, como a ManyChat, Chatfuel, a Azure que fornece um serviço completamente personalizável para o cliente utilizador, entre outras. Essas plataformas permitem que os desenvolvedores criem chatbots sem a necessidade de conhecimentos avançados em programação, utilizando interfaces gráficas e modelos pré-prontos.

No entanto, não permitem a utilização para esse tipo de atividade ilícita, levando ao serviço de programadores que fornecem bots maliciosos e sem regularização para disseminação de informações e doutrinação velada de eleitores e seguidores ideológicos de ambos os lados.

Por esta razão, o WhatsApp tem trabalhado em várias frentes para detectar e eliminar chatbots piratas. Uma das principais medidas adotadas foi a limitação do número de mensagens que um usuário pode enviar para outros usuários em um curto período. Essa medida visa impedir que esses mecanismos enviem uma grande quantidade de mensagens de uma só vez, o que pode indicar comportamento suspeito.

Outra medida importante foi a implementação de um sistema de detecção de contas de usuários que utilizam números de telefone falsos ou inválidos. Dessa forma, buscando impedir que os desenvolvedores de chatbots criem contas falsas para disseminar spam e fake news.

O WhatsApp também tem trabalhado em estreita colaboração com as autoridades de vários países para identificar e eliminar essas ferramentas clandestinas. Em agosto de 2021, por exemplo, fez uma parceria com a Agência Nacional de Telecomunicações (Anatel) no Brasil para identificar e eliminar contas de usuários que estavam-nas utilizando para enviar mensagens em massa.

No entanto, é importante ressaltar que a detecção e eliminação de chatbots piratas é um desafio constante para o WhatsApp e outras plataformas de mensagens. Os desenvolvedores estão sempre procurando maneiras de contornar as medidas de segurança e evitar a detecção, o que torna necessário um trabalho contínuo de aprimoramento das políticas e tecnologias de segurança.

O funcionamento pode variar dependendo do seu objetivo e da plataforma em que é utilizado. No entanto, em geral, segue um fluxo básico de interação com o usuário. Abaixo, segue um exemplo de fluxograma de um chatbot de atendimento ao cliente: **início:** o chatbot

cumprimenta o usuário e oferece ajuda; **identificação:** então, solicita que o usuário informe seu nome e outras informações relevantes, como número de pedido ou CPF, para identificá-lo; **tratamento:** ele verifica o problema ou solicitação do usuário e oferece soluções possíveis. Se necessário, encaminha o usuário para um atendente humano; **resposta:** aqui, ele fornece informações e responde às perguntas do usuário, de acordo com as opções oferecidas; **encerramento:** por fim, agradece ao usuário e finaliza a conversa, oferecendo-se para ajudar em caso de necessidade futura.

O fluxograma pode ser mais complexo dependendo da finalidade do chatbot. Por exemplo, um que seja utilizado para vendas pode incluir uma etapa de recomendação de produtos e uma etapa de finalização de compra, enquanto um focado em suporte técnico pode incluir uma etapa de triagem de problemas e uma etapa de encaminhamento para um técnico especializado.

Mas, em geral, o fluxograma é criado com base em uma análise das possíveis interações que o usuário pode ter com o chatbot e nas informações que o este precisa coletar para responder adequadamente às solicitações dele. Portanto, é programado para seguir esse fluxo de interação e oferecer respostas automatizadas de acordo com as informações fornecidas pelo usuário.

Por isso, as PLs citadas não podem incluir uma erradicação ou proibição dos bots, visto como são efetivamente positivos e úteis para a sociedade. Além disso, outras formas de enfrentar tal problemática, visto que são insuficientes estas para combater completa e efetivamente a divulgação de tais notícias falsas, sobretudo passando por tais transformações para formas mais evoluídas e tecnológicas, são a Lei nº 13.488, de 6 de outubro de 2017 (BRASIL, 2017a), alteradora dos dispositivos da Lei das Eleições e do Código Eleitoral com promovendo a reforma do ordenamento político eleitoral, e a Resolução TSE nº 23.551, de 18 de dezembro de 2017, esta que versa sobre a propaganda eleitoral, ambas sendo mais efetivas se usadas em conjunto.

Destarte, a erradicação da inteligência artificial no âmbito das eleições seria prejudicial ao desenvolvimento de um pleno debate nas redes sociais e na sociedade e no pleito eleitoral, visto que, conforme Francisco Brito Cruz:

> Restringir a utilização de instrumentos de inteligência artificial significa proibir a exploração da tecnologia a ser utilizada potencialmente para conferir transparência à campanha eleitoral ou colaborar na checagem de fatos. Além de experiências relevantes como o bot Fátima (elaborado pela agência Aos Fatos que atuará na disseminação de checagem de fatos no Facebook) ou a Operação Serenata de amor (que utiliza inteligência artificial para controle social da Administração Pública), essa tecnologia pode ser empregada pelas campanhas de diversas formas em benefício do debate político eleitoral e sem atentar contra a isonomia, a legalidade ou a legitimidade do pleito (CRUZ, 2018, p. 155).

Em relação às medidas legislativas contra o Deep Fake especificamente, há propostas de projetos de lei em tramitação no Congresso Nacional, como o PL 4060/2019, que visa tipificar o crime de manipulação digital de imagem ou som para alterar a verdade dos fatos, e o PL 4666/2020, que estabelece a responsabilidade civil e penal dos provedores de aplicativos e redes sociais que permitam a disseminação de deep fakes.

Além disso, algumas iniciativas tecnológicas têm sido desenvolvidas para combatê-los, como a criação de algoritmos e softwares capazes de detectar a manipulação de imagens e sons. No entanto, ainda há muitos desafios a serem enfrentados, como a velocidade com que novas técnicas de deep fake são criadas e a disseminação rápida desses conteúdos pelas redes sociais.

É importante ressaltar que o combate ao deep fake é um desafio global, que envolve não apenas as questões legais e tecnológicas, mas também a conscientização e educação dos usuários para identificar e não compartilhar conteúdos falsos e manipulados.

Isso sem contar a forma como a inteligência artificial e o algoritmo podem manipular informações conforme os interesses demonstrados pelo usuários das redes sociais, o que acaba levando ao oferecimento de informações específicas, sendo elas relevantes ou não, de acordo com a vontade e o interesse do internauta. Assim sendo:

> No novo mundo, como dizia o ex-presidente do Google, Eric Schmidt, é cada vez mais raro ter acesso a conteúdos que não sejam feitos sob medida. Os algoritmos da Apple, do Facebook ou do próprio Google fazem com que cada um de nós receba informações que nos interessam. E se, como diz [Mark] Zuckerberg, nos interessarmos mais por um esquilo agarrado na árvore em frente à nossa casa do que pela fome na África, o algoritmo dará um jeito de nos bombardear com as últimas notícias sobre roedores do bairro, eliminando assim toda interferência sobre o que se passa do outro lado do Mediterrâneo (DA EMPOLI, 2019).

Há, por fim, diversos outros meios, que não são tão efetivos, para combater as fake news e o deep fake, mas qual seria uma maneira mais eficaz de fazê-lo?

6. CONSIDERAÇÕES FINAIS

Algo mandatório para o momento seria a criminalização de aplicativos e sites usados para a produção livre e gratuita ou taxada de deep fake, visto que não há objetivo concreto ou qualquer necessidade para criação de tais vídeos, além da proibição de veiculação desse tipo de material claramente nocivo para o processo eleitoral e outros âmbitos da sociedade. Um vídeo veiculado durante as eleições próximo a data de votação já seria suficiente para manipular a escolha de voto da população e causar uma virada radical no resultado final, gerando, quando localizada e comprovada sua influência no processo, uma nulidade ou anulação no resultado

final, abrindo margem para novas eleições. Isso já é motivo suficiente para crer que há apenas objetivos e proposições nocivas para este sistema.

Quanto ao método mais efetivo para combater o resultado de falsas notícias veiculadas pela grande mídia ou por bots de redes sociais, a melhor proposição possível e mais rapidamente aplicável, seria combater "o mal com o mal", ou seja, utilizando bots automatizados para disseminar na mesma mensura a retratação da notícia em questão. Com o devido processo legal e profissionais capacitados, mesmo que contratados em serviço avulso de empresas especializadas em tecnologia, pode haver o uso desse tipo de ferramenta para corrigir a informação de forma ágil.

Essa função seria ainda mais facilitada pelo acesso ao sistema de informações da Receita Federal, criando um canal de comunicação simples com os eleitores e cidadãos no geral através de mensagens automáticas como as que já são enviadas em casos de previsão de clima perigoso, possíveis desastres naturais ou educação contra fake news disseminadas nas redes sociais.

Outros métodos que podem ser eficazes e foram aplicados anteriormente nas eleições dos Estados Unidos da América em 2020, são a remoção de vídeos com "mídia sintética manipulada" conforme atuação e anúncio do Youtube, que tomou essas medidas nesse momento como forma de assegurar que os cidadãos votantes não consumissem conteúdo inverídico, ou a rotulação de vídeos que contenham esse tipo de mídia, como foi feito pelo twitter, assim mantendo a possibilidade de consumir o conteúdo, mas dando ao internauta a ciência de que se trata de uma manipulação de imagem.

REFERÊNCIAS

BARRIOS, Daniel. **Chatbots**: Fundamentos, Desenvolvimento e Monetização. Novatec Editora, 2019.

BOBBIO, Norberto. **A era dos direitos.** Tradução Carlos Nelson Coutinho; apresentação de Celso Lafer. Nova ed. Rio de Janeiro: Elsevier, 2004. 7ª reimpressão.

BRASIL. PL 2630/2020 - Senado Federal. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/141944 Acesso em: 04 mar. 2023.

BRASIL. PLS 413/2017 - Senado Federal. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/131368. Acesso em: 04 mar. 2023.

BRITES, Maria José; AMARAL, Inês; CATARINO, Fernando. A era das "fake news": o digital storytelling como promotor do pensamento crítico**. Journal of Digital Media &**

Interaction. Vol. 1, N.º. 1, (2018), p. 85-98. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/55530/1/2018_Brites_Amaral_Catarino_AEraDasFakeNews.pdf. Acesso em: 11 abr. 2023.

DE CARVALHO, Marília Gomes. Tecnologia, desenvolvimento social e educação tecnológica. **Revista Educação & Tecnologia**, n. 1, p. 70-87, 1997. Disponível em: http://revistas.utfpr.edu.br/pb/index.php/revedutec-ct/article/view/1011/603. Acesso em: 10 abr. 2023.

CRUZ, Francisco Brito. **Direito eleitoral na era digital**. Belo Horizonte (MG): Letramento: Casa do Direito, 2018.

DAMACENO, Siuari Santos et al. Inteligência artificial: uma breve abordagem sobre seu conceito real e o conhecimento popular. **Caderno de Graduação-Ciências Exatas e Tecnológicas-UNIT-SERGIPE**, v. 5, n. 1, p. 11-11, 2018. Disponível em: https://periodicos.set.edu.br/cadernoexatas/article/view/5729Acesso em: 10 abr. 2023.

DE PAULA, Lorena Tavares; MICHALSKI, Rafael. Os bots de disseminação de informação na conjuntura das campanhas presidenciais de 2018 no Brasil. **Múltiplos Olhares em Ciência da Informação**, v. 9, n. 1, 2019. Disponível em: https://periodicos.ufmg.br/index.php/moci/article/view/17048/13818. Acesso em: 09 abr. 2023.

DA EMPOLI, Giuliano. **Os engenheiros do caos**: Como as fake news, as teorias da conspiração e os algoritmos estão sendo utilizados para disseminar ódio, medo e influenciar eleições. São Paulo, SP. Brasil. Vestígio Editora. 2019.

GONÇALVES, V. A. L. A difusão das fake news no contexto das eleições presidenciais de 2018: reflexões sobre o direito à informação e a liberdade de expressão. **Revista de Informação Legislativa**, Brasília, v. 58, n. 229, p. 11-32, jan./mar. 2021.

HOWARD, Philip N. **The internet and campaigns and elections**. In: Handbook of Research on Campaigns, Elections, and Voting Behavior in the Information Age, ed. R. Ling. IGI Global, 2019, p. 339-357.

LIMA, Camila Oliveira de Almeida. **A influência dos bots em processos informacionais**: limitações, benefícios e desdobramentos. Recife, 2022.

MONARD, Maria Carolina; BARANAUSKAS, José Augusto. Conceitos sobre aprendizado de máquina. **Sistemas inteligentes-Fundamentos e aplicações**, v. 1, n. 1, p. 32, 2003. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dcm.ffclrp.usp.br/~augusto/publications/2003-sistemas-inteligentes-cap4.pdf. Acesso em: 09 abr. 2023.

O que é deepfake? Inteligência artificial é usada para fazer vídeo falso. TECHTUDO. 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: 23 mar. 2023.

SANTOS, Carolina; LIMA, Jéssica; BORGES, Marcos; DIAS, Luana. "Deepfakes e o impacto nas eleições: desafios e estratégias para enfrentar a disseminação de notícias falsas no Brasil". **Revista Brasileira de Política e Segurança**, vol. 2, n. 1, 2020, p. 135-154.

Saiba o que é um deepfake e como identificar os vídeos falsos. ISTOÉ. Disponível em https://www.istoedinheiro.com.br/saiba-o-que-e-um-deepfake-e-como-identificar-os-videos-falsos/. Acesso em: 23 mar. 2023.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução Daniel Moreira Miranda – São Paulo: Edipro, 2016.

SÔNEGO, Arildo Antônio; BERNARDINI, Andréia Ana; POZZEBON, Eliane. Chatbots: Uma análise bibliográfica do estado da arte da literatura. **ARTEFACTUM-Revista de estudos em Linguagens e Tecnologia** , v. 16, n. 1, 2018. Disponível em: http://www.artefactum.rafrom.com.br/index.php/artefactum/article/view/1579/777. Acesso em 13 abr. 2023.

WALDMAN, Ricardo Libel; LIMA, Fernando Rister de Souza; UELZE, Hugo Barroso. As fake news e os limites ético-políticos da comunicação democrática. **Revista Pensamento Jurídico**, v. 16, n. 3, 2023. Disponível em: https://fadisp.com.br/revista/ojs/index.php/pensamentojuridico/article/view/389. Acesso em 11 abr. 2023.

WARDLE, Claire. **Fake News. It's complicated. First Draft News***,* 16 fev. 2017. Disponível em: https://firstdraftnews.org/articles/fake-news-complicated/ acesso em: 04 mar. 2023.