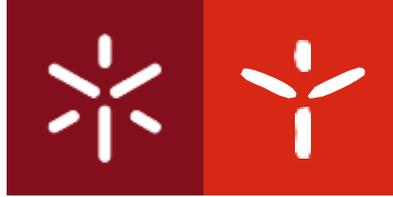


Universidade do Minho
Escola de Direito

José Ricardo Mansur

FAKE NEWS DIGITAIS NO BRASIL – Uma
Análise do Projeto de Lei 2.630/20 Sob a
Ótica de Um Crime Especial de
Responsabilidade



Universidade do Minho
Escola de Direito

José Ricardo Mansur

FAKE NEWS DIGITAIS NO BRASIL – Uma
Análise do Projeto de Lei 2.630/20 Sob a ótica
de Um Crime Especial de Responsabilidade

Dissertação de Mestrado
Direito e Informática

Trabalho realizado sob a orientação do
Prof. Doutor Pedro Miguel Dias Venâncio

e do
Prof. Doutor Paulo Jorge Freitas Oliveira Novais

Outubro de 2021

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição-SemDerivações
CC BY-ND

<https://creativecommons.org/licenses/by-nd/4.0/>

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

FAKE NEWS DIGITAIS NO BRASIL – UMA ANÁLISE DO PROJETO DE LEI 2.630/20 SOB A ÓTICA DE UM CRIME ESPECIAL DE RESPONSABILIDADE

RESUMO

O principal objetivo deste estudo foi analisar, sob a ótica da Informática e do Direito, a proposta apresentada no Projeto de Lei 2.630/20, quanto à necessidade de tipificar *Fake News* como um crime especial de responsabilidade, bem como analisar as medidas de combate apresentadas. A metodologia aplicada foi uma pesquisa bibliográfica, descritiva e qualitativa, numa análise crítica contemporânea, comparada e documental. A análise compreendeu o período em que o Projeto de Lei 2.630/20 (Lei das *Fake News*) tramitava na Câmara dos Deputados, desde o recebimento do texto original até a presente data. A realização desse estudo teve origem no fato de que, por estarmos inseridos num mundo onde as informações circulam numa quantidade excessiva, por vezes encontramos dificuldade para processá-las na sua totalidade. Muitas das informações veiculadas nas redes sociais, por não traduzir a realidade dos fatos, acabaram criando um baixo nível de confiabilidade para os usuários. Isso levou os provedores de redes sociais e de serviços de mensageria privada, que até então permitiam o livre fluxo de informações, a se preocupar com a perda de credibilidade das suas plataformas. Por esse motivo, começaram a tomar ações visando à coibição de *Fake News*. A informática foi fundamental para desenvolver e aplicar instrumentos, como algoritmos, inteligência artificial etc, para checar a veracidade dos conteúdos. A análise do PL 2.630/20 mostrou que o seu objeto não se enquadra como crime de responsabilidade, nem como crime especial. Mas apontou a necessidade de o legislador tipificar como crime comum *Fake News*, quando de forma coletiva afeta a honorabilidade das Instituições. Isto porque suas consequências podem colocar em risco o Estado Democrático de Direito. Quanto às medidas de combate a *Fake News*, o resultado da análise apontou que atendem aos objetivos e princípios definidos no referido Projeto de Lei.

Palavras-chave: *fake news*, internet, redes sociais, PL-2.630/20, algoritmos

***FAKE NEWS* DIGITAIS IN BRAZIL – AN ANALYSIS OF THE 2.630/20 BILL FROM THE
PERSPECTIVE OF A SPECIAL RESPONSABILITY CRIME**

ABSTRACT

The main objective of this study was to analyze, from the perspective of Information Technology and Law, the proposal presented in Bill 2,630/20, regarding the need to typify Fake News as a special liability crime, as well as analyze the combat measures presented. . The applied methodology was a bibliographical, descriptive and qualitative research, in a contemporary critical analysis, comparative and documentary. The analysis included the period in which the Bill 2630/20 (Law of Fake News) was processed in the Chamber of Deputies, from the receipt of the original text to the present date. This study was carried out due to the fact that, as we are in a world where information circulates in an excessive amount, we sometimes find it difficult to process it in its entirety. Many of the information conveyed on social networks, for not translating the reality of the facts, ended up creating a low level of reliability for users. This has led providers of social networks and private messaging services, which until then allowed the free flow of information, to worry about the loss of credibility of their platforms. For this reason, they began to take actions aimed at curbing Fake News. Information technology was essential to develop and apply instruments, such as algorithms, artificial intelligence, etc., to check the veracity of content. The analysis of PL 2,630/20 showed that its object does not qualify as a crime of responsibility, nor as a special crime. But he pointed out the need for the legislator to typify Fake News as a common crime, when collectively it affects the honorability of the Institutions. This is because its consequences can put the Democratic Rule of Law at risk. As for the measures to combat Fake News, the result of the analysis indicated that they meet the objectives and principles defined in the Bill.

Keywords: fake news, internet, social networks, PL-2,630/20, algorithms

ÍNDICE

INTRODUÇÃO	9
I – A PROBLEMÁTICA DAS <i>FAKE NEWS</i>	14
1. Histórico da Internet	14
2. Instrumentos teóricos aplicáveis à tecnologia	18
2.1 – Algoritimos	19
2.2 – Inteligência Artificial	21
2.3 – Aprendizado de Máquina	23
3. Combate as <i>fake news</i> digitais nas redes sociais	26
3.1 – Linkedin	28
3.2 – Facebook	29
3.3 – Instagram	32
3.4 – Whastapp	34
4. Ações para assegurar credibilidade nas informações	36
5. Questões pertinentes associadas às Redes Sociais Online	39
5.1 - O acesso e as contas inautênticas	42
5.2 - A rapidez e a disseminação das informações	43
5.3 - A Privacidade e o Anonimato	44
5.4 - A garantia da liberdade de expressão	45
6. Eficácia da tecnologia no combate as <i>fake news</i>	46
II – ENQUADRAMENTO JURÍDICO DAS <i>FAKE NEWS</i>	48
1. A Legislação Brasileira	49
1.1 - Constituição da República Federativa do Brasil	49
1.2 - Marco Civil da Internet	53
1.3 - LGPD – Lei Geral de Proteção de Dados	58
1.4 - Crimes de responsabilidade	61
1.5 - Liberdade de manifestação do pensamento e da informação	63
1.6 - Código Penal	64
III – O PROJETO DE LEI 2.630/20 – LEI DAS <i>FAKE NEWS</i>	67
IV – MEDIDAS PROCESSUAIS OU CAUTELARES DE COMBATE AS <i>FAKE NEWS</i>	75
CONSIDERAÇÕES FINAIS	82

REFERÊNCIAS BIBLIOGRÁFICAS	87
LEGISLAÇÕES	94
JURISPRUDÊNCIAS	96

LISTA DE ABREVIações E ACRÔNIMOS MAIS FREQUENTES

AI	ARTIFICIAL INTELLIGENCE (INTELIGÊNCIA ARTIFICIAL)
AL	ALGORITHMS (ALGORITIMOS)
CCB	CÓDIGO CIVIL BRASILEIRO
CJF	CONSELHO DA JUSTIÇA FEDERAL
CPDHED	CARTA PORTUGUESA DE DIREITOS HUMANOS NA ERA DIGITAL
CRFB	CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL
EOAB	ESTATUTO DA ORDEM DOS ADVOGADOS DO BRASIL
EUA	ESTADOS UNIDOS DA AMÉRICA
FB	FACEBOOK
GT	GRUPO DE TRABALHO
INSTA	INSTAGRAM
ISP	INTERNET SERVICE PROVIDER (PROVEDORES DE SERVIÇOS DE INTERNET)
LK	LINKEDIN
ML	MACHINE LEARNING (APRENDIZADO DE MÁQUINA)
OAB	ORDEM DOS ADVOGADOS DO BRASIL
PGR	PROCURADORIA GERAL DA REPÚBLICA
PL	PROJETO DE LEI
RICD	REGIMENTO INTERNO DA CÂMARA DOS DEPUTADOS
RISTF	REGIMENTO INTERNO DO SUPREMO TRIBUNAL FEDERAL
SSL	SECURE SOCKET LAYER
STF	SUPREMO TRIBUNAL FEDERAL
STJ	SUPERIOR TRIBUNAL DE JUSTIÇA
TCP/IP	TRANSFER CONTROL PROTOCOL para INTERNET PROTOCOL
TSE	TRIBUNAL SUPERIOR ELEITORAL
TW	TWITTER
WPP	WHATSAPP

INTRODUÇÃO

Motivação

Um dos motivos para realização deste trabalho se deveu ao fato de que, por estarmos inseridos num mundo onde as informações circulam numa quantidade excessiva, por vezes encontramos dificuldade para processá-las com confiabilidade e segurança.

É cediço que, por conta desse volume de informações, tem sido necessário escolher quais delas devem ser processadas, uma vez que são veiculadas informações de toda natureza e por vezes divergentes. Fica a dúvida em quais delas se fiar.

Na mídia tradicional, notícia falsa sempre esteve presente em suas manchetes como forma de engajar a audiência. Não se trata de um fenômeno novo, porém a proliferação de notícias falsas (*fake news*) ganhou destaque no mundo digital e virou um grande negócio, acima de valores éticos e morais.

A facilidade do acesso à internet e a criação das redes sociais ampliou o impacto das *fake news* digitais a nível global. Antes, notícias falsas diziam respeito à vida das pessoas de destaque. Entretanto, atualmente o que se observa é que as *fake news* influenciam a sociedade quanto ao comportamento, ao posicionamento político e à saúde da população.

Hoje impera um ambiente no qual não há qualquer autoridade estabelecida, onde qualquer pessoa diz qualquer coisa sobre qualquer assunto, da maneira que quiser. A informação vem de qualquer fonte, sem nenhum critério, com potencial de se espalhar, manipulando emoções, causando influência destrutiva na população e definindo rumos para a sociedade.

As redes sociais online têm sido invadidas por muitas *fake news*, fato que me instigou a desenvolver o trabalho sobre este tema.

Problema

Em plena era da sociedade da informação, o fenômeno das *fake news* tem sido uma preocupação mundial, cuja relevância merece ser analisada quanto a uma possível influência negativa nos meios de comunicação.

A sociedade brasileira, de maneira geral, tem se referido a *fake news* como:

- O termo é em inglês, mas se tornou popular em todo o mundo para denominar informações falsas que são publicadas, principalmente, em redes sociais¹.
- Em alguns casos, os autores criam manchetes absurdas com o claro intuito de atrair acessos

¹ <https://mundoeducacao.uol.com.br/curiosidades/fake-news.htm>, Publicado por: Rafael Batista, p.1 acessado em 26/08/20

- aos sites e, assim, faturar com a publicidade digital²;
- podem ser usadas apenas para criar boatos e reforçar um pensamento, por meio de mentiras e da disseminação de ódio. Dessa maneira, prejudicam-se pessoas comuns, celebridades, políticos e empresas³;
 - Informações noticiosas que não representam a realidade, mas que são compartilhadas na internet como se fossem verdadeiras, principalmente através das redes sociais⁴;
 - notícias falsas que pretendem distorcer o sentido de fatos verídicos⁵;
 - informações noticiosas que não dizem respeito à realidade, mas que mesmo assim acabam sendo compartilhadas pelas pessoas na internet, principalmente pelas redes sociais, como se fossem verdadeiras⁶;
 - notícias falsas são utilizadas com a meta de prejudicar a imagem e a reputação de um adversário político, um candidato, fazendo com que ele perca apoio em uma disputa eleitoral, por exemplo.⁷

Porém, no meio acadêmico, TEIXEIRA (2018, 21) entende que “*Fake News* é um termo inglês cujo significado corresponde a notícias falsas, são informações comprovadamente inverídicas e intencionalmente divulgadas”.

TEIXEIRA (2018, 21) complementa que, “usualmente, essa disseminação ocorre na internet e tem o intuito de influenciar as pessoas em várias dimensões, como a política, a social e a econômica. O fator crucial para a sua eficácia é a impressão de credibilidade de sua fonte.”.

Para CARNIELLI & RICHARD (2011, 325), *fake news* significa “notícias falsas, histórias inventadas para parecerem jornalismo crível e amplamente difundidas com a intenção de influenciar o público-alvo e fazer com que este divulgue a mensagem”.

Segundo GRECO (2020), no Brasil ainda não há uma definição legal sobre *fake news*, mas pessoalmente entende como sendo “notícias falsas, divulgadas através das redes sociais e internet, com o objetivo de desinformar e/ou macular reputações de pessoas físicas ou jurídicas”.

No Brasil são atribuídas diversas interpretações ao termo inglês *fake news* e ainda não há um conceito firmado sobre elas. Mas, para efeito desse estudo, concluindo sobre as várias interpretações de *fake news*, será considerado o seguinte conceito:

² <https://mundoeducacao.uol.com.br/curiosidades/fake-news.htm>, Publicado por: Rafael Batista, p.1 acessado em 26/08/20

³ <https://mundoeducacao.uol.com.br/curiosidades/fake-news.htm>, Publicado por: Rafael Batista, p.1 acessado em 26/08/20

⁴ <https://www.significados.com.br/fake-news/>, p.1 acessado em 26/08/20

⁵ <https://www.significados.com.br/fake-news/>, p.1 acessado em 26/08/20

⁶ <https://www.meusdicionarios.com.br/fake-news/>, p.1 acessado em 27/08/20

⁷ <https://www.meusdicionarios.com.br/fake-news/>, p.1 acessado em 27/08/20

São notícias falsas ou, se verdadeiras, dissociadas do contexto original, divulgadas nos meios tradicionais de comunicação e/ou pela internet nas redes sociais digitais, capazes de manipular o público, distorcendo a realidade com objetivo de desinformar, enganar ou até mesmo prejudicar alguém.

Na verdade, o fato de existir notícia falsa não é nenhum fenômeno novo, pois sempre esteve presente em muitas manchetes da mídia tradicional. Entretanto ganhou destaque no mundo digital, principalmente nas mensagens trocadas nas redes sociais, sendo conhecida como *fake news* digital. Assim, *fake news* digital são notícias falsas que veiculam no mundo virtual, através das redes sociais.

Além do grande volume de informações, vivemos uma comunicação digital onde as trocas ocorrem de forma célere, através de meios informáticos de acesso fácil e popular, como se observa nas redes sociais e nos aplicativos de mensageria.

Essa facilidade tem permitido às pessoas divulgar e discutir informações que, muitas vezes, não traduzem a realidade dos fatos. Isto pode levar a disseminação de falsas notícias entre os usuários e provocar prejuízos à imagem, a honra ou até mesmo financeiros a outrem.

É fato que as notícias veiculadas nas redes sociais têm apresentado baixo nível de confiabilidade em razão de pouca ou nenhuma filtragem pelos meios informáticos. E a sua disseminação, por ser muito rápida, é difícil de ser eliminada imediatamente e vem afetando a credibilidade das plataformas.

Nesse sentido, os provedores, que até então permitiam o livre fluxo das informações, passaram a utilizar mecanismos de checagem da veracidade das mesmas, confrontando-as com fontes oficiais confiáveis, a partir da relevância da notícia veiculada.

No Brasil, existem alguns sites, como “Aos fatos”⁸ e “Truco – Agência Pública”⁹, que realizam esse tipo de checagem a fim de validar as informações. Em Portugal, também existem sites que realizam essa checagem, como é o caso do poligrafo¹⁰ e do sicnoticias¹¹.

Observa-se que as *fake news* têm gerado consequências como a desinformação, dúvida quanto à realidade dos fatos e quanto à veracidade das informações.

Quanto à credibilidade da fonte da informação, o anonimato que tem sido permitido pela internet favorece condutas delitivas de agentes. Estes agentes, sem fronteiras, capturam mensagens, vídeos e imagens, para praticar crimes virtuais, como é o caso de *fake news*.

Desinformações podem, por vezes, afetar a reputação de cidadãos através das redes sociais, no

⁸ <https://www.aosfatos.org/>

⁹ <https://apublica.org/truco-antigo/>

¹⁰ <https://poligrafo.sapo.pt/>

¹¹ <https://sicnoticias.pt/programas/poligrafo>

cometimento de crimes de responsabilidade. O ordenamento jurídico brasileiro, pelo Código Penal, já prevê crimes contra a honra: injúria, difamação e calúnia. Entretanto, sua tipificação não distingue se o cometimento ocorre na forma escrita ou falada.

Atualmente no Brasil essa preocupação é ainda mais evidente, tendo em vista o enorme volume de mensagens veiculadas nas mídias sociais que divulgam informações enganosas com viés ideológico, com a intenção de macular a reputação de representantes dos três poderes: Executivo, Legislativo e Judiciário.

Não à toa, foi proposto o Projeto de Lei 2.630/20 com o objetivo de regulamentar esse assunto, como forma de se resguardar a democracia e a liberdade de expressão. No fundo, objetiva-se considerar as *fake news* como um crime virtual de responsabilidade.

Pelas razões expostas, mostra-se relevante que o Projeto de Lei das *fake news* seja exaustivamente discutido no Congresso Nacional a fim de avaliar a necessidade de tipificação de um novo crime e as medidas de bloqueio propostas para normatizar as ações que os provedores devam tomar para combater as *fake news*.

Conteúdo

Este trabalho analisará a versão do Projeto de Lei 2.630/20 durante todo o período de investigação, no qual ele estará em discussão no Congresso Nacional Brasileiro.

Dessa forma, com base na definição de *fake news*, torna-se necessário analisar se esse delito seria um novo tipo de crime, uma vez que praticado na modalidade virtual e, caso não enquadrado no ordenamento jurídico brasileiro, como deveria ser tipificado.

Acrescenta-se a necessidade de avaliar a pertinência das medidas de bloqueio propostas pelo Projeto de Lei visando à inibição de notícias falsas, frente às ações dos provedores das redes sociais e serviços de mensageria no combate às *fake news*, realizadas através do uso de recursos tecnológicos.

No final, com base nos resultados obtidos, pretende-se realizar um estudo comparativo com o ordenamento jurídico português sobre como é tratada a questão das *fake news*.

Assim, quanto à problemática das *fake news*, serão abordados os instrumentos teóricos aplicáveis à tecnologia no combate às *fake news*, a forma como vem sendo combatidas nas Redes Sociais online, as ações para assegurar a credibilidade das informações, as questões envolvendo as Redes Sociais online e a eficácia da tecnologia no combate às *fake news*.

Quanto ao enquadramento jurídico das *fake news*, serão abordadas as legislações brasileiras que tratam da liberdade de manifestação do pensamento e da informação, análise do Projeto de Lei

2.630/20 e as medidas processuais ou cautelares de combate às *fake news*.

Este trabalho tem caráter descritivo e utiliza grafia brasileira, com metodologia de análise crítica contemporânea, comparada e documental.

I – A PROBLEMÁTICA DAS *FAKE NEWS*

1. Histórico da Internet

É praticamente impossível definir o momento específico da origem da Internet, pois muitos indivíduos podem tê-la previsto, sendo que para várias dessas previsões não se tem registros acadêmicos.

Sabe-se que em 1908, Nikola Tesla previu uma tecnologia que possibilitaria uma comunicação instantânea para homens de negócio emitir instruções e fazê-las aparecer em outro local diferente de onde as originou, inclusive permitindo o acesso global. (KLEINROCK, 2010, 26)

Em 1938, H. G. Wells associou a ideia de um “Cérebro Mundial” como sendo um local onde conhecimento e ideias são recebidos, confrontados e classificados. Baseando-se nessa ideia, em 1945, Vannevar Bush previu uma máquina com memória comunitária que intitulou de memex, na qual “formas totalmente novas de enciclopédias aparecerão, prontas com uma malha de trilhas associativas passando por elas, pronto para ser inserido no memex e amplificado.”. (KLEINROCK, 2010, 26)

Em 1949, quando a União Soviética detonou a sua primeira arma nuclear num grande evento após confronto com os Estados Unidos, a defesa aérea passou a ser uma preocupação para os EUA que, já em 1948, a Força Aérea Americana previa a necessidade de desenvolver uma rede de radar de alerta de defesa aérea. Esse pode ter sido o início da jornada de desenvolvimento de uma rede de comunicação entre computadores.

Era o início de uma corrida espacial para o avanço armamentista, momento que levou os EUA a repensar quanto à política voltada para a ciência e tecnologia, passando a incrementar o apoio às pesquisas universitárias e à educação dos estudantes das áreas de ciência e engenharia.

A partir daí a Internet passou a ser fortemente desenvolvida e implantada principalmente nos Estados Unidos, através de um conjunto de invenções e inovações que envolveram o campo da computação, das comunicações e dos serviços públicos.

Em 1969, durante a guerra fria, a empresa americana ARPA - *Advanced Research Project Agency* desenvolveu uma rede de comunicação confiável onde não existia um comando central, chamada de ArpaNet, que utilizava protocolo de comutação de pacotes conhecido como *Network Control Protocol* (NPC).

Na visão de seus designers o objetivo da ARPANET era permitir que os pesquisadores da ARPA compartilhassem dados e programas residentes nos computadores de outros centros de pesquisa da ARPA, com vistas à produtividade intelectual e ao uso eficiente dos recursos.

Naquela época, havia dezenas de computadores diferentes e incompatíveis, o que tornava difícil vinculá-los. Como solução a equipe da BBN¹² - Bolt, Beranek e Newman (ALPERIN, BROWN, HUANG, & SHASTRI 2001, 4) desenvolveu o *Interface Message Processor* (IMP)¹³, um *switch*, que hoje chamaríamos de roteador. (MOWERY & SIMCOE 2002, 7)

Os IMPs eram pequenos computadores cujo único trabalho era codificar mensagens do computador *host* em pacotes para distribuição pela rede e decodificar pacotes de entrada para o computador *host*¹⁴. (NEUMAN, 2010, 144)

A ARPANET era composta de inúmeras redes de computadores, visando à interligação das bases militares americanas aos departamentos de pesquisas científicas e acadêmicas, para reduzir a vulnerabilidade no sistema de comunicação, através da utilização via subterrânea de *backbone*¹⁵, tornando difícil a interrupção do sistema. (CLAY, POLYZOS e BRAUN s.d., 3)

Segundo ALMEIDA (2005, 2), a rede utilizava o *batch processing* no qual os dados eram processados por lotes e num longo período de tempo.

E acrescentou que muito embora se mostrasse satisfatório para atender as necessidades de cálculos, o *batch processing* deixava a desejar quanto à possibilidade de viabilizar uma comunicação interativa entre os computadores e a própria troca de dados entre eles.

Entre 1970 e 1975, a ARPANET superou os 100 nós, em razão dos locais de acesso às pesquisas, utilizando o protocolo NPC, estarem ligados à rede em muitas universidades e áreas importantes de defesa. Isso acabou gerando preocupação de como poderia a comunicação ser mantida sem interrupção com o crescimento inesperado de utilizadores.

No final dos anos 70, diante da grande expansão do uso, o protocolo NPC apresentou-se insuficiente. Sua função era comutar os pacotes originais, dividindo os seus dados em partes menores, objetivando que estas pequenas partes identificassem a origem e o destino dos seus dados.

Na busca de solução a ARPANET, através de pesquisas realizadas pelos engenheiros Robert Kahn¹⁶ e Vinton Cerf, conseguiu modificar o NPC e desenvolver um protocolo de comunicação mais eficiente, que chamou de *Transfer Control Protocol* para *Internet Protocol* (TCP/IP). (ROSENZWEIG 1998, 1536)

¹² (ALPERIN, BROWN, HUANG, & SHASTRI 2001, 4) "BBN was created in 1948 in part by Beranek, who hired Licklider in 1957."

¹³ (MOWERY & SIMCOE 2002, 7) The switch was called an Interface Message Processor (IMP), and linked computers at several major computing facilities over what is now called a wide-area network. A computer with a dedicated connection to this network was referred to as a "host."

¹⁴ (NEUMAN, 2010, 144) Um host (também conhecido como "host de rede") é um computador ou outro dispositivo que se comunica com outros hosts em uma rede

¹⁵ (CLAY, POLYZOS e BRAUN s.d., 3) backbone: espinha dorsal da National Science Foundation – NS *fake news* ET. To maintain data regarding packets and bytes transmitted and received, erros, delay times, and down times, all NS *fake news* ET backbone nodes record statistics about the packets which traverse each of their interfaces.

¹⁶ (ROSENZWEIG 1998, 1536) *Review Essay* Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet ROY ROSENZWEIG. "In collaboration with Vinton Cerf, Kahn developed in 1974 a new and more independent packet-switching protocol-at first called Transmission Control Protocol

O protocolo TCP/IP, que substituiu o NPC, foi considerado altamente confiável, pois corrigiu vários problemas anteriormente apresentados pelo NPC. Ele foi disponibilizado e implementado de forma gratuita através de um padrão aberto.

Isso permitiu que a rede crescesse de forma ilimitada, dado que o protocolo era facilmente implantado em qualquer plataforma computacional e garantia a interoperacionalidade e interconexão das diversas redes de computadores.

Em 1979, pela internet, foram criadas as primeiras compras online, viabilizadas através da interligação de uma TV a um computador residencial, que processava a transação em tempo real, com uso de linha telefônica. Entretanto, após ter sido liberada para uso comercial em 1987, nos Estados Unidos, passou a ser utilizada para acesso à comunicação e informação, através de correio eletrônico, conhecido como *e-mail*.

Muitas instituições originavam suas mensagens através de um processo informal de correspondência intitulado Chamado Solicitação de Comentários (*Request for Comments – RFC*)¹⁷, criado pelo estudante de ciência da computação Steve Crocker, em 1969. A utilização de RFC disseminou rapidamente, tornando-se o espaço padrão para que a ARPANET se desenvolvesse tecnicamente, enviando comentários, ideias novas e refinando propostas de melhoria. (LEINER, et al. 1997, 12)

Nos anos 80, surgiu o *e-commerce*, conhecido como comércio eletrônico, com transações sempre por via telefônica voltadas para usuários com computadores domésticos, para os quais foram criadas ferramentas disponibilizadas num serviço que foi denominado *Electronic Mall*.

Assemelhava-se a um Shopping virtual, no qual os usuários tinham a oportunidade de realizar compra de produtos escolhidos em formulário de vários comerciantes online. Registra-se que esse foi um dos primeiros casos de comércio eletrônico que se tem conhecimento.

No ano de 1990, Tim Berners-Lee, pesquisador da CERN, apresentou um hipertexto que permitia usufruir as informações da internet de modo rápido e dinâmico, através de uma interface denominada navegador. A essa interface o pesquisador chamou de *www - World Wide Web*, ou simplesmente navegador *WEB*.

A internet passou a ser o meio mais utilizado para acesso aos sites remotos. Ocorre que os dados em formato de texto simples enviados e recebidos usando o protocolo de TCP/IP, podiam ser

or TCP and later TCP/IP, with IP standing for "Internet Protocol"-that would serve as a kind of lingua franca for this new Internet."

¹⁷ (LEINER, et al. 1997, 12) In 1969 a key step was taken by S. Crocker (then at UCLA) in establishing the Request for Comments (or RFC) series of notes. These memos were intended to be an informal fast distribution way to share ideas with other network researchers.

acessados e violados com bastante facilidade e, portanto, não garantia a segurança dos dados. (BHATT, SHULZE e HANCKE 2006, 793)

Em 1994 foi criado o Netscape 1.0 com um protocolo chamado de *Secure Socket Layer* (SSL) utilizado para assegurar através de criptografia a integridade das informações, no envio ou na recepção, das transações por via internet. (PORIYE e UPADHYAYA 2015, 810)

O SSL era o protocolo de segurança mais popular e apresentava três versões: 2, 3 e 3.1 sendo a versão 3 a mais popular. Por essa razão, serviços que exigiam confidencialidade e autenticação eram oferecidos por SSL. (PORIYE e UPADHYAYA 2015, 810)

A internet começou a se difundir mundialmente em 1995, atendendo aos mais variados fins, abrindo espaço para alguns tipos de negociações a nível comercial de produtos que podiam ser negociados exclusivamente na forma eletrônica.

Nesse referido ano, o sucesso da utilização do comércio eletrônico começou a ser sentido, contando com a participação de grandes empresas como a Amazon.com e a eBay. A partir daí, a internet transformou o mundo numa enorme aldeia global.

O crescimento acelerado do uso da internet nos últimos anos tem impulsionado a criação de aplicativos e sites que viabilizam a comunicação entre os usuários, na forma de comunidades ou grupos, por motivo profissional, negocial, afetivo, acadêmico, entre outros.

Segundo CUNHA (2016, 12), no período compreendido entre o ano 2000 e 2013 surgiram vários sites especializados em criar redes sociais. Nesse período, *Friendster* foi um dos primeiros grandes sites desse tipo criado em 2002, seguido por outros como *LinkedIn*, *Orkut*, *Facebook* e *Twitter*.

Após esse período, outros software e sites têm surgido, graças à Internet. Cita-se como exemplo, o Messenger, o Instagram, o Line e o Whatsapp. Este último chegou ao Brasil em 2009 e atualmente lidera a mensageria nas redes sociais do País.

Em 2010 no Brasil foi instituído pelo Decreto 7.175/10 o Programa Nacional de Banda Larga – PNBL, regulamentando o acesso à Internet de banda larga e a inclusão digital. (PLANALTO.gov.br, Decreto 7.175/10 2010)

Porém referido Decreto, foi revogado em 2018 pelo Decreto 9.612/18, que normatizou as políticas públicas de telecomunicações¹⁸. (PLANALTO.org.br, Decreto 9.612/18 2018)

¹⁸ (PLANALTO.org.br, 2018) Art. 2º São objetivos gerais das políticas públicas de telecomunicações:

I - promover:

a) o acesso às telecomunicações em condições econômicas que viabilizem o uso e a fruição dos serviços, especialmente para:

1. a expansão do acesso à internet em banda larga fixa e móvel, com qualidade e velocidade adequadas; e

2. a ampliação do acesso à internet em banda larga em áreas onde a oferta seja inadequada, tais como áreas urbanas desatendidas, rurais ou remotas;

b) a inclusão digital, para garantir à população o acesso às redes de telecomunicações, sistemas e serviços baseados em tecnologias da informação e comunicação - TIC, observadas as desigualdades sociais e regionais;

A inclusão digital favoreceu o acesso em massa dos brasileiros às redes sociais, ficando atualmente atrás somente dos EUA.

Para BHATT, SHULZE e HANCKE (2006, 793), “como a Internet pode ser vista como uma grande rede de computadores interconectados, quase todos os usuários da Internet correm o risco de um ataque à segurança. Mais em risco estão empresas que transmitem dados críticos pela Internet para seus sites corporativos em todo o mundo. A necessidade de comunicação segura e confiável pela Internet é tão predominante agora como sempre foi”¹⁹.

Para HARTMANN, a popularização da internet tornou-a o principal meio de comunicação disponível para as pessoas divulgarem as suas opiniões. Entretanto, essa tecnologia não permite a publicação generalizada dos conteúdos, pois controla proativamente a plataforma disponibilizada, através de decisões individuais quanto a não publicar ou excluir as mensagens. (FOLHA UOL 2020, 1)

As decisões individuais das Plataformas, de publicar ou excluir as mensagens dos usuários, deixa dúvida se esse controle próativo de alguma maneira estaria violando o direito de liberdade de expressão, questão esta que será abordada mais adiante.

Registram-se as boas intenções quando da criação da internet para democratizar de maneira generalizada o acesso às informações e ao conhecimento, que levou o mundo a se transformar numa verdadeira aldeia global. Percebe-se que nesse mundo globalizado, a internet é um caminho sem volta.

Entretanto, infelizmente a internet tem sido usada com finalidades criminosas das mais diversas, desde pedofilia, venda e consumo de drogas, discriminações em geral e também para disseminar *fake news*. Ações como essas devem ser combatidas com rigor para que essas práticas não venham a macular a importância da internet no mundo contemporâneo.

2. Instrumentos teóricos aplicáveis à tecnologia

No âmbito da tecnologia, muitos são os instrumentos teóricos utilizados pela informática para tratamento das informações no ambiente virtual.

Como base comparativa no tratamento dos dados informáticos que veiculam nas redes sociais e nas mensagerias podemos citar a utilização de algoritmos (*algorithms* - AL), aprendizagem de máquina (*machine learning* - ML) e inteligência artificial (*artificial intelligence* - AI).

¹⁹ BHATT, SHULZE e HANCKE (2006, 793) Since the Internet can be viewed as a large network of interconnected computers, almost every user on the Internet is at risk against a security attack. More at risk are companies that transmit critical data across the Internet to their corporate sites all over the world. The need for reliable secure communication over the Internet is as prevalent now as it ever was.

2.1 - ALGORITMOS

Algorithms são definidos no *Cambridge Dictionary*²⁰ como um conjunto de instruções ou regras matemáticas que, especialmente se fornecidas a um computador, ajudarão a calcular uma resposta para um problema. (CAMBRIDGE Dictionary s.d.) (DICIO s.d.)

AL é também um processo de cálculo matemático ou da descrição sistemática da resolução de um grupo de problemas semelhantes. Pode-se dizer também que são regras formais para obtenção de um resultado ou da solução de um problema englobando fórmulas de expressões aritméticas. Na área de desenvolvimento de software é muito comum relacionar a palavra algoritmo com diagrama de bloco.. (MANZANO e OLIVEIRA 2005, 6)

Conforme registrou VENÂNCIO (2013, 89)²¹, numa definição matemática, AL é «uma sucessão finita de passos (destinadas a servir de instruções), cada um dos quais definido e executável, que opera sobre os dados, produzindo resultados²²⁷⁻²²⁸.».

Segundo MARTINI e COSTA (2019, 149), “AL é uma sequência finita de instruções executadas mecanicamente ou eletronicamente em um espaço computacional. Os algoritmos precisam de programações manuais, mas podem ser executados automaticamente, conforme os comandos recebidos. Isto é, algoritmos são os passos necessários para executar as tarefas exigidas pelo navegador.”

Os autores explicam que existem diversos níveis de complexidade para a aplicação de AL, sobretudo, no desenvolvimento de programas para computadores até a coleta de informações pessoais para banco de dados. (MARTINI e COSTA 2019)

Para MANZANO e OLIVEIRA (2005, 3), AL é “um processo de cálculo matemático ou da descrição sistemática da resolução de um grupo de problemas semelhantes. Pode-se dizer também que são regras formais para obtenção de um resultado ou da solução de um problema englobando fórmulas de expressões aritméticas.”.

O pesquisador de direito digital e diretor do Instituto Beta: Internet e Democracia, PAULO RENÁ questiona o uso de sistemas automatizados (como AL) para monitorar conteúdos, recurso adotado por todas as plataformas.

PAULO RENÁ pondera que “a tecnologia não vai ser suficiente para nos salvar de nós mesmos. Para saber o que é informação e o que é desinformação, nós precisamos do contexto. Não será um

²⁰ Cambridge Dictionary . Algorithm is a set of mathematical instructions that must be followed in a fixed order, and that, especially if given to a computer, will help to calculate an answer to a mathematical problem. Algoritmo é definido como um “Conjunto de regras que fornecem uma sequência de operações capazes de resolver um problema específico.”

²¹ VENÂNCIO (2013, 89) ²²⁷BORRUSO;RUSSO ;TIBERI, Informatica per il giurista: dal bit a internet, p. 207 (Tradução da nossa responsabilidade). ²²⁸Outra definição similar usual é «Um algoritmo é um conjunto ordenado e não ambíguo de passos executáveis que define um processo completo e definitivo.» (tradução nossa), BROOKSHEAR, Computer science: an overview, p.169.

robô, não será uma máquina ou mesmo um jeito de fazer, uma ‘receita de bolo’, que vai saber o que é verdade.” (AGÊNCIABRASIL 2018, 4)

Quanto à sua aplicação, o AL pode ser projetado especificamente para redes estrela e satélite, também para programação linear, programação dinâmica, programação de metas, como algoritmo de ramificação e corte, entre outras.

Sabe-se que “algoritmos exatos, geralmente baseados em programação dinâmica e algoritmos de ramificação e corte, requer esforço computacional significativo e não são apropriados para a maioria das aplicações práticas, como roteamento multicast em redes”. (NOFERESTI e SHAH-HOSSEINI 2012, 2)

No caso da programação de metas, independentemente de serem as metas alcançáveis ou não, um objetivo será definido quando a otimização dá um resultado que se aproxima o mais possível das metas desejadas (solução satisfeita). (ORUMIE e EBONG 2014, 69)

Quando se trata de um problema de objetivo único, a formulação e solução são semelhantes à programação linear, com a exceção de que, se o cumprimento completo do objetivo não for possível, a programação de objetivo fornecerá uma solução e informações para os tomadores de decisão.

No entanto, um grande retrocesso na aplicação do método de programação de objetivo linear (LGP) tem sido a falta de um algoritmo capaz de atingir a otimização em tempo razoável. (ORUMIE e EBONG 2014, 59)

O uso de AL busca reduzir o tempo gasto pelo usuário quando acessa as redes sociais, filtrando as notícias de seu interesse, dado o excesso de informações produzidas, disponíveis na internet.

O resultado dessas e de outras ações ocorre por causa do AL, ou seja, de uma sequência de passos previamente programados que são executados para resolver alguma demanda. (EBC 2016, 1)

Relativamente à *fake news*, para melhorar a capacidade de rastreamento de notícias falsas, AL pode ser utilizado como algoritmo de classificação, nomeadamente, Regressão Logística, Multinomial Naives Bayes, SVC linear, Árvore de decisão e K-Nearest.

É certo que na tecnologia toda programação se dá através de um algoritmo, que nada mais é do que uma linguagem de programação com a qual se constrói uma série de comandos. Por sua vez, os algoritmos podem ser usados de várias formas.

Podemos citar seu uso para estimar a importância de um site, através da quantidade de acessos obtidos; filtrar o número de comentários do usuário nas postagens sobre determinado assunto; e filtrar quem fez as postagens (pessoas com as quais se deram as suas interações – compartilhando, comentando ou curtindo).

Também são usados para coletar dados, interpretá-los e principalmente criptografá-los, como é o caso da troca de assinaturas digitais, de chaves e *hashing* de mensagens, pela NSA – Agência Nacional de Segurança dos Estados Unidos. A aplicação mais simples de um algoritmo é quando é utilizado como uma bolha, onde contém gravadas as informações que o usuário mais pesquisa na internet.

Para o FB, AL representa uma série de fatores e variáveis traduzidos pela rede para mostrar ao usuário exatamente aquilo que interessa a ele em primeira mão. Exemplificando, o FB exibe na *timeline* do usuário os anúncios interpretados como sendo os de seu maior interesse.

Na visão dos utilizadores, Algoritmos são usados, por exemplo, quando se faz uma busca na internet, quando recebe uma notificação do Wpp ou, até mesmo, quando pede para o computador “ejetar” um pendrive.

Ocorre que, na realidade pouco se sabe quais AL os provedores utilizam. Como forma de combater a disseminação de *fake news* ou rumores nas principais redes sociais online, melhor seria que os algoritmos de propagação das informações utilizados pelos provedores se tornassem públicos.

Nas redes sociais, AL são utilizados como forma de filtrar informações sobre determinado tema que veicula nas mensagens trocadas pelos usuários. Os AL são a base de funcionamento da AI, que através de um conjunto significativo de dados, utiliza o *machine learning* como impulsionador.

2.2 – INTELIGÊNCIA ARTIFICIAL

Artificial Intelligence é definida como sendo o estudo de como produzir máquinas que tenham algumas das qualidades que a mente humana possui, como a capacidade de compreender a linguagem, reconhecer imagens, resolver problemas e aprender. (Cambridge Dictionary s.d.)

Em 1950, Alan Turing, em seu artigo “Computing Machinery and Intelligence”, projetou o “Teste de Turing”. Referia-se a ação de uma pessoa que, ouvindo uma conversa em linguagem natural entre um usuário e um computador com Inteligência Artificial – AI, sem visualizá-los, testasse a capacidade de distinguir qual dos dois era o humano. Caso o testador não conseguisse distinguir entre o computador e o usuário, a AI seria considerada inteligente.

O grande desafio da AI é desenvolver em computadores um comportamento que se assemelhe ao de um ser humano, quando este realiza tarefas do dia-a-dia como, por exemplo, reconhecer figuras, compreensão ou utilização de uma linguagem ou resolver um problema. Chama-se AI forte para a possibilidade de que o computador raciocine, aprenda, planeje e seja capaz até de mover objetos.

Quando questionado sobre a probabilidade das máquinas se tornarem mais inteligentes que os seres humanos, Jean-Gabriel Ganascia, cientista de computação, respondeu que não. E disse que se

trata de um mito inspirado na ficção científica. (UNESCO COURIER 2018, 7)

A MICROSOFT (2016, p.1-2)²² tem uma visão ousada de criação de sistemas com AI real entre agentes, aplicações, serviços e infraestrutura. Também se vê como inclusiva, pois busca o acesso generalizado da AI, de forma que todos possam usufruir dos benefícios. E essa visão vem ganhando vida com a criação do Chatbot Xo e com Kits de desenvolvimento e de recursos para dispositivos Cortana (Cortana Devices SDK and Skills Kit).

Para RIBEIRO (2010, 8), "A Inteligência Artificial é uma ciência multidisciplinar que busca desenvolver e aplicar técnicas computacionais que simulem o comportamento humano em atividades específicas".

Na concepção de RICH (1998, 17), "Inteligência Artificial é o estudo de como fazer computadores realizarem tarefas para as quais, até o momento, o homem faz melhor".

Para DELOITTE (s.d., 2)²³, AI representa teoria e desenvolvimento de sistemas computacionais com capacidade de realizar tarefas que necessitam de inteligência humana. E comenta que a inteligência pode ser artificial, mas suas aplicações são bem reais e tangíveis, pois a AI potencializa estratégias com insights, reduz custos com automação e velocidade de processamento com precisão.

Segundo NOVAIS et al (2016, 257) *data mining* (em português: mineração de dados) - DM tem grande importância para AI, pois através desse método é possível detectar conhecimento oculto nos dados. Muitas vezes é preciso enquadrar o objeto em análise, numa determinada classe pré-definida.

Esclarece que, após a classificação, as páginas são distribuídas por categorias e, se indesejáveis ou ofensivas, são automaticamente bloqueadas. Essa ação é extremamente útil para inibir sites com conteúdos impróprios ou mesmo impedir a disseminação de conteúdos indesejáveis.

Atualmente são muitas as abordagens de classificação de sites, porém a análise de conteúdos textuais que veiculam nas páginas da web tem sido amplamente utilizada e, embora eficiente, tem se mostrado muito difícil, quando comparada a outros tipos de abordagens.

Existem categorias de sites cujos conteúdos textuais são bem semelhantes, embora diferentes quanto às características estruturais. Nesses casos, a pesquisa se vale de outros métodos de classificação como, por exemplo, baseados em endereços de URL ou etiquetas de marcação HTML.

²² MICROSOFT (2016, p.1-2) Afirma Harry Shum, vice-presidente executivo do grupo de Inteligência Artificial (IA) e Pesquisa da Microsoft, descrevendo-se como um "cara de pesquisa transformado num cara de produtos", que "Sempre buscamos democratizar a tecnologia. Com a IA, faremos isso de duas formas – ao infundi-la em produtos como o Office 365, ao mesmo tempo em que criamos uma plataforma na qual outros podem construir e inovar". E complementa que, em outubro, a Microsoft se tornou a primeira empresa do setor a chegar à paridade com humanos em reconhecimento de voz.

²³ DELOITTE (s.d., 2) Algoritmos de machine learning, plataformas AI-powered e analytics estão cada vez mais disseminados e consolidados. Combinando isso com o atual poder de computação para processar enormes volumes de dados coletados de bilhões de dispositivos conectados estaremos a aumentar a capacidade de resolver problemas complexos a velocidades a que o cérebro humano nunca poderá atingir.

Essas abordagens verificam a presença ou ausência de etiquetas predefinidas. (NOVAIS et al 2016, 258)

Quanto ao emprego de métodos de identificação do autor de mensagens indesejáveis varia muito, sendo que o mais comum se baseia no conteúdo da mensagem, o qual é rastreado através da aplicação de AL que, com a utilização de ML, auxilia a AI na identificação do autor.

Entretanto, as soluções empregadas não levam em consideração fatores como a personalidade e o humor do autor, que são emoções traduzidas em palavras, contidas no texto, quando da escrita das mensagens.

Estudos com base nessa abordagem têm sido realizados, obtendo resultados favoráveis à aplicação dessa metodologia. Em um de seus artigos, NOVAIS et al (2018, 1) comenta que, “numa discussão online, na qual muitos recursos-chave não estão presentes (como gestos, expressões faciais, entonação etc) as palavras usadas e os estilos de escrita podem revelar informações sobre nossas preferências, pensamentos, emoções e comportamentos.”.

Para os utilizadores, AI é um sistema que analisa dados em grande escala, capaz de identificar tanto padrões, como tendências e com isto formular previsões com precisão e velocidade, de forma automática. E, de certo, tem um papel muito importante na identificação das *fake news*.

2.3 – APRENDIZADO DE MÁQUINA

Machine Learning é definido no *Cambridge Dictionary* como um processo nos computadores, que muda a maneira como realizam tarefas, aprendendo com novos dados, sem que um ser humano precise dar instruções na forma de um programa. Sua pesquisa ajuda a moldar o campo do aprendizado de máquina, aproximando os computadores do reino do pensamento humano. O caminho para o aprendizado de máquina genuíno e a inteligência artificial passa pela linguagem. (CAMBRIDGE Dictionary s.d.)

BISHOP (2006) define ML como sendo um ramo da AI que se baseia em estatística computacional e também em procedimentos de otimização, que utilizam técnicas de aprendizado auto aperfeiçoadas para solucionar problemas ou para executar tarefas específicas.

A área de ML é uma área de pesquisa dinâmica, na qual frequentemente são propostos novos métodos, onde a principal preocupação é com a qualidade dos dados a serem processados.

Vale registrar o conceito de dados que, segundo VENÂNCIO (2013, 15) trata-se de elementos ou valores discretos que isoladamente não têm qualquer significado ou utilidade. Por sua vez, a “informação” é o resultado de alguma forma de processamento de dados, quando estes são

relacionados ou interpretados.

VENÂNCIO (2013, 15-16) complementa que a apreciação intelectual realizada por um ser humano sobre uma informação disponível, resulta em um determinado “conhecimento”. E finaliza registrando que a partir do conhecimento é possível alcançar a “sabedoria”, que representa o estado mais elevado de abstração e complexidade.

Nesse contexto, no caso específico das *fake news*, a manipulação de dados transforma-se em informações errôneas, que por sua vez, acabam se transformando em conhecimento errôneo. Existem ferramentas que trabalham sobre dados, informações e conhecimento, cada uma aplicada em níveis diferentes de *fake news*.

Existem dois principais tipos de ML: aprendizagem supervisionada e não supervisionada.

Na aprendizagem supervisionada, um conjunto de dados é previamente inserido no computador e os algoritmos devem guardar semelhança com esses dados, de maneira que o resultado já será o previsto.

Na aprendizagem não supervisionada, nenhum resultado específico é esperado, isto é, não há possibilidade de se fazer uma previsão dos resultados após o processamento das informações.

A expectativa sobre o ML é que a máquina, a partir dos dados alimentados, aprenda com o mínimo de programação a chegar a um resultado de forma autônoma. O ML é o principal impulsionador da AI e sua base de funcionamento são os algoritmos. (CAMPOS 2017, 46)

Atualmente a mais recente ameaça distópica é o *deepfake*, que basicamente são falsas identidades criadas com o *deep learning* (aprendizagem mais profunda) com uso de uma técnica que sintetiza imagens humanas baseada em AI.

Com base nessa tecnologia existe a possibilidade de um “humano digital” ou uma “falsa pessoa” se tornar um *bot* na internet e influenciar os internautas em várias situações, inclusive com disseminação de *fake news*.

Essa técnica é um problema grave e se apresenta como um grande risco para os meios de comunicação digital, tendo em vista deturpar a realidade, difundindo *fake news* principalmente pelo convencimento de que os fatos são verdadeiros.

É possível também combinar e sobrepor vídeos e imagens reais transformando em vídeos e imagens “originais”, numa técnica chamada de GAN (*Generative Adversarial Network* - Redes Geradoras Adversariais), que é um conceito de ML que nasceu em 2014. Com ela podem ser criados eventos para uma pessoa que na realidade nunca existiram.

Philip Wang, engenheiro de software da Nvidia, criou um website demonstrando a potência da

técnica GAN, que gera imagens com base no método StyleGAN desenvolvido pela referida empresa, visando a construção de imagens artificiais de alta resolução e qualidade.

Acrescenta-se que a tecnologia chamada GPT-2 (sistema de previsão de linguagem) da OpenAI é capaz de, com habilidade, escrever textos de forma convincente e enganosa utilizando estilo de escrita de escritores famosos. Por tudo isso, há o risco da AI ser usada para criar perfis falsos, escrever *fake news* e enganar usuários das redes sociais. (REVISTA GALILEU 2019, 2)

Relativamente às *fake news*, com a potência do *Big data* e AI, o ML tem capacidade de processar uma gama de informações, em grande velocidade e detectar se as notícias são ou não verdadeiras, baseando-se em AL pré-determinados.

Para os utilizadores, o ML é uma programação usada nos computadores que permite à máquina aprender a retornar com respostas às consultas, baseadas em experiências adquiridas com os resultados no processamento de uma gama de informações (dados processados) prévias.

Quanto aos instrumentos teóricos, os algoritmos por sua vez, apresentam como vantagem para o utilizador, a redução do tempo gasto nas redes sociais para acessar assuntos de seu interesse, diante do grande volume de informações. E para os provedores se traduz na capacidade de rastreamento e filtragem de determinados temas que veiculam nas redes sociais, no combate às *fake news*.

A desvantagem para o utilizador é a interferência na vontade humana ou quando ocorre um resultado errôneo do algoritmo, que o leva a uma injusta punição como, por exemplo, uma suspensão temporária. Para o provedor, a desvantagem é o comprometimento do nível de credibilidade da sua plataforma, como reflexo dos erros de análise.

As limitações quanto ao uso dos algoritmos não são claras para os utilizadores. Este fato pode levar a erro do provedor por negligência e pelo utilizador por desconhecimento das regras, devido à falta de transparência no processo de captação e uso dos dados pelo provedor.

Quanto à inteligência artificial, tanto para os provedores, quanto para os utilizadores, a vantagem está na realização de tarefas de forma rápida, com custo reduzido de automação e qualidade próxima da inteligência humana. A questão ética é a grande desvantagem, pois ao estabelecer o que é certo e o que é errado, numa linha tênue entre o bem e o mal, o utilizador pode acabar sendo discriminado.

O aprendizado de máquina tem a vantagem de processar, com rapidez, uma gama de informações. A desvantagem é que quando o aprendizado ocorre sem supervisão, os resultados, após o processamento das informações, são imprevisíveis.

Atualmente, no aprendizado de máquina, o *deepfake* se mostra um alto risco para a credibilidade das plataformas de redes sociais, cujo desafio maior está em identificar e eliminar as imagens e vozes

por ele produzidas.

Por fim, será necessário desenvolver um Projeto de Lei que estabeleça um código de ética específico, que limite o uso de algoritmos pelas plataformas de redes sociais visando à privacidade e o direito de liberdade de expressão do usuário.

3. Combate às *fake news* digitais nas redes sociais

A Internet, sem dúvida, tem influenciado a crescente mudança de comportamento dos seus usuários, na medida em que favorece a interconexão entre eles, que interagem concordando ou discordando dos conteúdos veiculados, mas posicionando-se através do direito constitucional da liberdade de expressão.

Segundo NOVAIS et al (2014, 1), nas duas últimas décadas os avanços tecnológicos têm facilitado a comunicação instantânea entre as pessoas no mundo, porém de forma superficial e artificial. Entretanto, faltam elementos não verbais importantes numa comunicação humana, como por exemplo, o nível de estresse e traços de personalidade dos interlocutores.

Complementa o autor que, ao se comunicar, uma pessoa expressa a sua personalidade, a qual é resultante da percepção que ela tem do mundo e nesse sentido a comunicação pode se alterar conforme o nível de estresse ou mesmo variações de humor, no momento da escrita.

Assim, conseguir avaliar a relação entre os traços de personalidade e o nível de estresse da pessoa ao se comunicar pode ser um facilitador no processo de comunicação. Outro ponto a ser considerado é o estilo de escrita, que pode favorecer o reconhecimento e a identificação do autor da mensagem.

Atualmente, a interlocução em massa, associada ao *lockdown* (consequência do COVID-19) favoreceu o aumento no nível de conversação entre os usuários e a disseminação de notícias de todo tipo, inclusive falsas.

Tem-se a impressão de que vivemos uma era de desinformação inimaginável e por conta disso, preocupadas com a disseminação de *fake news*, as plataformas de redes sociais estão cada vez mais desenvolvendo controles para inibir ou conter o seu avanço.

Entretanto, há que se considerar, que as ações tomadas pelas plataformas sobre essas notícias, ainda que falsas, podem implicar em consequências graves para a sociedade, nomeadamente quanto à liberdade de expressão e a democracia.

É fato que o combate às *fake news* tem sido intenso, principalmente nas plataformas de redes sociais que têm contado com o auxílio de organizações de checagem de notícias, as quais verificam a veracidade das informações, confrontando-as com fontes oficiais confiáveis, a partir da relevância da

notícia veiculada nas redes sociais.

Como exemplo, citamos algumas organizações de checagem de fatos: “LUPA”, “Aos fatos”, “Truco – Agência Pública”, “Fato ou Fake” e “COMPROVA”, no Brasil; “Polígrafo” e “Sicnotícias”, em Portugal; “MALDITA.ES”, na Espanha; “LATAMCHEQUEA”, na Argentina; “Correctiv”, na Alemanha e “IFCN - International Fact-Checking Network” e “Lead Stories”, nos EUA.

Vale registrar que o Google, apesar de ser um motor de busca de simples acesso onde se localiza qualquer tipo de informação independente de ser verdadeira, ao nível de comunicação entre usuários disponibiliza a ferramenta Youtube que, embora seja direcionada para apresentação de vídeos, oportuniza a interação com o produtor do conteúdo.

Através dos seus mecanismos de busca no *Youtube* e nas redes sociais, o Google tem combatido as *fake news*. Recentemente o Google firmou parceria com a *First Draft*, (DRAFTNEWS s.d., 1) num projeto em fase de desenvolvimento na *Havard Kennedy School*, chamado *Desinfo Lab*, que visa à divulgação de informações erradas veiculadas em períodos de eleições e nos casos de notícias de rápida apuração. (CANALTECH 2018, 1)

A empresa tem trabalhado para treinar o sistema com o uso da ferramenta ML com o objetivo de identificar notícias falsas e ajustar o sistema para que aos seus usuários só sejam mostrados resultados mais precisos. (CANALTECH 2018, 1)

Um curso, voltado para jornalistas, foi disponibilizado pela Google para ensinar como usar o ML para criar as suas reportagens, com a ferramenta *Google Cloud AutoML Vision*, criada pela LSE – *The LONDON SCHOOL of ECONOMICS and POLITICAL SCIENCE*. (GOOGLE s.d., 16-20)

Nesse curso, o jornalista aprende como treinar um modelo de ML para identificar e classificar imagens em grandes conjuntos de dados. (GOOGLE s.d., 16)

O *Cloud AutoML* é um conjunto de produtos de ML criado para que desenvolvedores com conhecimento limitado nessa área treinem modelos de alta qualidade com base nas necessidades dos negócios. Ele usa a tecnologia de pesquisa de arquitetura neural e o aprendizado por transferência de última geração do Google.

Além disso, a Google está trabalhando com o *Poynter Institute*, a *Stanford University* e a *Local Media Association* para lançar um novo programa chamado *MediaWise* para jovens leitores, a fim de melhorar o conhecimento sobre mídia digital. (THEVERGE 2018, 2)

A empresa GOOGLE (2020, 2) tem investido²⁴ bastante no combate as *FAKE NEWS*²⁵, principalmente

²⁴ GOOGLE (2020, 2) O Google está oferecendo mais de US\$ 6,5 milhões em recursos para organizações de checagem de fatos e entidades sem fins lucrativos de todo o mundo, que trabalham no combate às informações falsas e enganosas sobre o coronavírus. E mais: estamos renovando nosso apoio à Rede Internacional de Checagem de Fatos (IFCN, na sigla em inglês), que continua colaborando com checadores de todo o mundo para defender as

em relação às informações enganosas que dizem respeito ao coronavírus, cuja disseminação tem gerado descrédito e pânico na sociedade. (GOOGLE 2021, 2)

As redes mais focadas no combate as *fake news* são Facebook, Instagram, WhatsApp e Twitter, por serem as redes mais importantes, visto que têm as maiores quantidades de utilizadores e, por consequência, estão mais propícias a grande quantidade de *fake news*.

Apenas como exemplo, citamos outras redes como Messenger, WeChat, Qzone, Weibo, Pinterest, Snapchat e Vkontakte, porém se trata de redes com menor potencial de utilizadores, comparadas àquelas de maior importância.

Como já descrito, nas redes sociais para detectar e combater as *fake news* os provedores utilizam algoritmos, aprendizagem de máquina, inteligência artificial e contam inclusive com o auxílio de agências checadoras de fatos.

3.1 - LINKEDIN

LinkedIn é considerada a maior rede social profissional, tendo sido criada para viabilizar relacionamentos profissionais, podendo ser utilizada para procurar emprego, criar parcerias, anunciar vagas ou simplesmente como *network* (rede de relacionamento).

No LK é possível criar currículos, localizar empregos e contactar profissionais de todo mundo. As empresas, por sua vez, podem captar candidatos para suas vagas, como também localizar perfis de clientes em potencial.

Muitos usuários utilizam o LK para compartilhar experiências e publicar artigos. A rede é uma mina de ouro para as empresas e headhunters para captar talentos.

Embora o LK controle a qualidade do conteúdo do que é publicado pelos usuários quanto à relevância e valor, via de regra as publicações são estritamente profissionais, fato que por si só descarta a existência de conteúdos com caráter ofensivo.

Assim, sendo o LK um espaço aberto e democrático acessível a qualquer pessoa que deseja trocar experiência através de *network*, procurar emprego, publicar artigos ou qualquer contato profissional, não há espaço para disseminação de *fake news*.

melhores práticas na área da verificação de informações. Essa parceria vai permitir uma nova visualização da base de dados resultante da checagem publicada pela CoronavirusFacts Alliance. Já a [Science Feedback](#) vai realizar uma análise de rede a partir dessa base de dados, para rastrear a disseminação de informações falsas sobre a COVID-19 em plataformas e sites de todo o planeta.

²⁵ (GOOGLE 2021, 2) “Um mito comum, por exemplo, é achar que as empresas de tecnologia podem criar soluções que resolveriam o problema da desinformação de uma vez, mas não é bem assim. “Desinformação”, “fake news” ou “informação errada” são termos diferentes com significados diferentes para cada pessoa, e que ainda dependem de contexto e de uma compreensão sobre a intenção de seu autor. Como não estamos em posição de avaliar, de modo objetivo e em larga escala, a veracidade de um conteúdo ou a intenção dos seus criadores, enfrentamos o problema da desinformação destacando informações confiáveis e de alta qualidade, como já dissemos, e também combatendo agentes mal-intencionados e oferecendo mais contexto às pessoas, por meio do estímulo à educação midiática, da verificação de informações, ou do apoio à produção de notícias de qualidade.”

3.2 - FACEBOOK

O Facebook (FB) foi fundado²⁶ por Mark Zuckerberg e Eduardo Saverin em 2004, sendo que atualmente é proprietário do INSTAGRAM e do WHATSAPP. (Hei-man 2008, 1)

O objetivo foi viabilizar uma rede de conexão entre os alunos da University of Harvard. O FB acabou se expandindo para outros meios universitários do mundo e em pouco tempo, permitiu o acesso para pessoas com idade superior a 13 anos.

No início, as ferramentas de interação eram limitadas, tais como publicação de conteúdos em texto, fotos ou vídeos, comentários e caixas de conversas online. À medida que a rede social cresceu, novas funções foram atribuídas e as antigas melhoradas.

Um dos pontos mais pertinentes nas mudanças do FB foi o uso de AL que precisa o usuário em um ambiente onde existem milhões de pessoas com diferentes gostos e características intelectuais, culturais e socioeconômicas distintas. (MARTINI e COSTA 2019, 151). No FB o AL basicamente determina o que deve aparecer primeiro no (GOOGLE, Support 2020, 1) *feed*²⁷ dos usuários.

Conhecendo as preferências dos usuários, o FB, através de combinações algorítmicas determinadas pela própria rede social e por empresas comerciais atuantes, passou a oferecer em primeira mão e com maior frequência, conteúdos que vão ao encontro do gosto dos usuários.

Importante registrar que a data e a hora da publicação do conteúdo também influenciam nessa oferta, pois um dos principais algoritmos usados tem por função manter o conteúdo mais recente no topo das publicações. Segundo o estudo de JURNO e D'ANDREA (2017, 463-484) em junho de 2014, o FB passou a ordenar melhor os vídeos que são publicados diretamente na plataforma.

Para melhor captar o perfil e entender o comportamento dos usuários, a plataforma criou rápidas e simples pesquisas²⁸, com base nas reações aos vídeos acessados, passando a ranquear as publicações, inclusive informativas, entre usuários com afinidades sobre o tema acessado. (BOOKS GOOGLE 2018, 1)

²⁶ (Hei-man 2008, 1) Facebook was founded by Mark Zuckerberg in 2004 in a Harvard dorm room. At first it was originally designed only for students in Harvard to replace the printed directory. Later, it opened its door to college students all over the world as long as they had a validated college email address. Then in May, 2007, it decided to let everyone sign up and open the platform for third party mini programme developers. It has been very popular in the West since its change of policy.

²⁷ (GOOGLE, Support 2020, 1) "Feed é um fluxo de conteúdo que você pode percorrer. O conteúdo é exibido em blocos de aparência semelhante que se repetem um após o outro. Por exemplo, um feed pode ser editorial (lista de artigos ou notícias) ou informações do produto (lista de produtos, serviços etc.). Os feeds podem aparecer em qualquer lugar na página."

²⁸ (BOOKS GOOGLE 2018, 1) During the months that followed my visit to Google in may 2016, I started to see a new type of maths story in the newspapers. An uncertainty was spreading across Europe and the US. Google's search engine was making racist autocomplete suggestions; Twitterbots were spreading fake news; Stephen Hawking was worried about artificial intelligence; far-right groups were living in algorithmically created filter-bubbles; Facebook was measuring our personalities, and these were being exploited to target voters. On after another, the stories of the dangers or algorithms accumulated. Even the mathematicians' ability to make predictions was called into question as statistical models got both Brexit and Trump wrong.

Em 2009 o FB criou uma equipe²⁹ responsável pela moderação de conteúdos na plataforma, cujas regras, na época, cabiam numa única página e se respaldaram na mais importante lei dos EUA na proteção do discurso na internet, o CDA (*Communications Decency Act*). (KLONICK 2018, 1.620)

No CDA, Lei de Decência das Comunicações Americanas, o código 47 da Section 230 define como regra³⁰ para o editor ou locutor, a proteção para bloqueio privado e triagem de material ofensivo, relativos a conteúdos fornecidos por outro provedor de informação. (CORNELL LAW SCHOOL s.d., 1)

Ocorre que os bloqueios resultantes das triagens podem colocar em risco a liberdade de expressão e a cultura democrática, que são elementos essenciais da natureza das plataformas de redes sociais. Na realidade, muito pouco se sabe como se dá a curadoria do conteúdo das mensagens dos usuários.

Considerando que o ano de 2015 foi marcado por inúmeras *fake news* circulando nas redes sociais, o FB decidiu aplicar mudanças³¹ no AL para relações próximas, objetivando que as mensagens entre amigos passassem a ter mais prioridade. Paralelamente, começou a diminuir o alcance, avisando aos usuários quanto à incerteza dos conteúdos duvidosos. (MARTINI e COSTA 2019, 2)

Igualmente a outras plataformas, em razão da crescente quantidade de *fake news* circulando nas redes sociais, o FB passou a adotar medidas na tentativa de reduzir a disseminação desses conteúdos.

Nesse sentido, o FB criou um link que faculta aos usuários identificar *fake news* e a desconfiar de matérias sensacionalistas, com títulos em letras maiúsculas e/ou com muitos pontos de interrogação/exclamação. Orienta o usuário para:

- Ficar atento ao URL (Uniform Resource Locator, em português é conhecido como endereço do site ou localizador padrão de recursos), que pode estar simulando algum site conhecido, porém alterando/acrescentando apenas alguma letra/símbolo.

- Valorizar a investigação sobre a fonte, quem é o responsável pelo site, verificando se essa fonte possui algum endereço ou um meio físico para contato. Igualmente, investigar as imagens e fotos, que podem não corresponder ao conteúdo da mensagem, se tratar de algum tipo de montagem ou de

²⁹ (KLONICK 2018, 1.620) "It was not until November 2009, five years after the site was founded, that Facebook created a team of about twelve people to specialize in content moderation. Like YouTube, Facebook hired a lawyer, Jud Hoffman, to head their Online Operations team as Global Policy Manager. Hoffman recalled that, "when I got there, my role didn't exist." Hoffman was charged with creating a group separate from operations that would formalize and consolidate an ad hoc draft of rules and ensure that Facebook was transparent with users by publishing a set of "Community Standards."

³⁰ (CORNELL LAW SCHOOL s.d., 1) Código dos EUA § 230 c) Protection for "Good Samaritan" blocking and screening of offensive material.

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

³¹ (MARTINI e COSTA 2019, 2) "Desde 2014, a rede social digital Facebook começou a usar algoritmos bastante específicos para melhorar o consumo de vídeos e para atender empresas que possuem páginas comerciais no ambiente digital. As mudanças algorítmicas afetaram diretamente as empresas que produzem notícias, pois interferem diretamente nos mais variados tipos de conteúdos publicados diariamente na rede social. Essas modificações ocorreram gradualmente, ao passo que os produtores de conteúdo começaram a se esforçar para desvendar os segredos do Facebook. Para uma empresa de notícias alcançar bons resultados, por exemplo, tornou-se essencial desenvolver estratégias para usar os algoritmos em favor de seus objetivos."

momentos passados.

- Consultar outros sites, confiáveis, que tenham veiculado esse mesmo tipo de notícia. Caso não encontre, já seria um indício de que a informação pode não ser verdadeira. Neste caso, sugere registrar uma denúncia na plataforma para que esta, com auxílio das organizações de checagem de fatos, possa verificar se realmente se trata de uma notícia verdadeira ou falsa.

Nessa seara o FB, ao permitir ao usuário se reportar a notícia que considera falsa, disponibilizou uma ferramenta (denunciar publicação) na qual o usuário denuncia a notícia com simples cliques. A partir da denúncia, a notícia é direcionada para agências parceiras do FB, para verificar o fato e analisar quanto a sua veracidade.

Na verificação, a notícia tem seus dados históricos, seus números e tudo que é possível de ser analisado, contrastado com um banco de dados públicos e é com base nele que se afirma se a notícia é ou não uma *fake news*.

Comprovada a impropriedade da notícia, a sua publicação sofre uma redução no alcance, diminuindo a visibilidade, principalmente inibindo o acesso a impulsionar notícias dentro da plataforma e a usar os produtos de monetização.

Há casos em que os usuários criam notícias para ganhar dinheiro com a quantidade de visualizações. Esse processo é conhecido como monetização³². Muitas vezes são notícias que não espelham a realidade dos fatos. (CLAUSSEN, KRETSCHMER e MAYRHOFER 2011, 3)

Quando essas notícias são consideradas *fake news*, seus usuários têm os incentivos³³ econômicos cortados para que não tenham mais como fazer dinheiro com esse tipo de transação dentro da plataforma. (CLAUSSEN, KRETSCHMER e MAYRHOFER 2011, 2)

Entretanto, o FB decidiu não proibir o compartilhamento de mensagens, mas o usuário recebe um alerta de que as agências detectaram inverdade na informação por ele veiculada e, por conta disto, os seus leitores recebem um aviso de que se trata de uma postagem suspeita.

Em 2018, FB lançou o “botão de contexto”, com o objetivo de fornecer informações sobre as fontes dos artigos no Feed de notícias. Mais uma vez a intenção foi mostrar informações confiáveis para que usuário possa tomar da decisão correta e não disseminar *fake news*. (HEGEMAN 2020, 1)

³² (CLAUSSEN, KRETSCHMER e MAYRHOFER 2011, 3) “Managing a platform has the goal of maximizing its monetization opportunities. As revenues for platform owners are often generated through advertising or transaction-based charges, managing active user engagement (which in turn increases advertising effectiveness) is often at the core of platform management. This may be done through non-price instruments imposing rules and constraints, creating incentives and shaping demand and supply behavior (Boudreau and Hagiu 2009).”

³³ (CLAUSSEN, KRETSCHMER e MAYRHOFER 2011, 2) “The way firms interact with their consumers has changed significantly with the advent of social media channels. In particular, communication channels based on links among consumers, e.g. word-of-mouth or (active or automated) recommendations are supported through use of social media. In the empirical context of Facebook in-site applications (or pps), we study how firms and users transform their behavior in response to a change in the effectiveness of social media channels. More specifically, Facebook started rewarding apps that engage users more by enabling them to send out more notifications.”

No início de 2020 o FB lançou a “notificação de contexto”, com objetivo de informar ao usuário que a matéria que pretende compartilhar tem mais de 90 dias, ou seja, trata-se de uma notícia antiga, porém cabe ao usuário decidir se compartilha ou não a informação.

Na sequência, em 30/06/20, numa tentativa de conectar as pessoas diretamente a fontes seguras e exibir menos desinformações, principalmente sobre COVID-19, FB começou a utilizar perguntas para auxiliar o usuário a desmascarar *fake news*.

Aos usuários cabe responder três perguntas: “**de onde vem a publicação?** *Se não houver fonte, procure*”; “**o que está faltando?** *Leia toda a história e não apenas o título*”; e “**como a notícia faz você se sentir?**”.

Em 12/08/20, FB lançou uma campanha de “tela de notificação global”, com o objetivo de fornecer aos usuários, links com contextos adicionais sobre COVID-19, visando à inibição da disseminação de *fake news* sobre o conteúdo que compartilham.

No combate às notícias falsas, de forma geral, o FB vem atuando através das seguintes ações: removendo incentivos econômicos para os disseminadores de desinformação (*spammers*); construindo, testando e iterando novos produtos para identificar e limitar a disseminação de *fake news*; melhorando a classificação do Feed de notícias; utilizando parceria com organizações independentes de verificação de fatos; e ajudando o usuário a ficar mais bem informado para tomar decisões.

3.3 - INSTAGRAM

Lançado em outubro de 2010, pelos criadores Kevin Systrom e Mike Krieger, o INSTAGRAM pretendeu criar uma rede social na qual fosse possível compartilhar imagens e vídeos. Foi desenvolvido para ser utilizado em plataforma iOS, em sistema restrito de aparelhos criados pela Apple: celulares iPhone, reprodutores de músicas iPod Touch e Tablet iPad.

Em 2012 foi comprado pelo Facebook, continuando com a mesma sistematização, ou seja, compartilhamento de imagens e vídeos na rede social. Mas logo em seguida foi liberado para uso também na plataforma móvel do Google.

Em maio de 2019 o FB começou a utilizar a tecnologia de detecção de imagem no INSTA, expandindo seu programa de checagem de informações para o aplicativo. Com isso as notícias falsas resultantes das pesquisas na aba “Explorar” passaram a ser removidas do INSTA.

Nesse mesmo período, o INSTA buscando combater *fake news* em sua plataforma iniciou uma parceria com agências norte-americanas de checagem de notícias para identificar, revisar e rotular as informações falsas. Tratava-se de parceiros independentes que objetivavam reduzir disseminação de

fake news, sendo que o INSTA estaria expandindo essa parceria com outras agências de checagem de fatos ao redor do mundo para permitir classificar *fake news* na rede social. (CANALTECH 2019, 1)

Em agosto de 2019, segundo a revista Forbes Brasil, “O Instagram lançou hoje (15) um recurso que permite aos usuários denunciarem **publicações** que considerem falsas. A publicação de informação falsa não é proibida em todos os serviços do Facebook, mas a companhia está tomando medidas para limitar o alcance de publicações erradas e alertar os usuários.”. (FORBES 2019, 1)

Nessa mesma revista, a Forbes noticiou que o “Facebook começou a usar tecnologia de detecção de imagem no Instagram em maio e expandiu seu programa de checagem de informações para o aplicativo. Os resultados considerados como falsos são removidos de locais em que os usuários buscam conteúdo novo, como a aba “Explore”, do Instagram, e resultados de busca por **hashtags**.” (FORBES 2019, 1)

Em março de 2020³⁴, o INSTA divulgou medidas exclusivas para combater a disseminação de *fake news* sobre COVID-19 (coronavírus) e melhorar a qualidade das informações a respeito desse tema. Entre elas, mudanças no processo de busca, no qual a procura por termos ligados àquele tema resultará em mensagem educacional, embasada em informações da Organização Mundial da Saúde (OMS) e do Ministério da Saúde. (G1.GLOBO 2020, 2)



fonte: WhatsApp 18/01/21

Outras medidas que estão sendo adotadas são: remoção de perfis relacionados ao COVID-19 que tenham sido recomendados; retirada de conteúdos na aba “Explorar”, que não sejam de fontes confiáveis e redução do alcance dos conteúdos identificados por agências de checagem, no *feed* e nos stories, como falsos. (G1.GLOBO 2020, 1)

O FB, que é proprietário do INSTA, anunciou recentemente, em janeiro de 2021, que irá implantar uma central de notícias do coronavírus no topo do *feed* de notícias dos usuários.

³⁴ (G1.GLOBO 2020, 2) "Proibimos anúncios enganosos de produtos que se referem ao Covid-19 que tentam gerar pânico e urgência, prometem garantir curas ou impedir que as pessoas sejam contaminadas, e banimos temporariamente anúncios e conteúdo de marcas que promovem certos suprimentos médicos, incluindo máscaras faciais", disse o Instagram em comunicado. "Também não será mais possível procurar efeitos de realidade aumentada relacionados à doença, com exceção para os que foram desenvolvidos em parceria com uma organização de saúde reconhecida."

3.4 - WHATSAPP

Lançado em novembro de 2009, pelos criadores Brian Acton e Jan Koum, o *WhatsApp* pretendeu disponibilizar gratuitamente a veiculação de mensagens de texto, vídeos, imagens, documentos em PDF e chamadas de voz para aparelhos *smartphones*, através de conexão com internet.

Em 2012 as mensagens passaram a ser codificadas. O Wpp³⁵ foi adquirido em 2014 pelo FB e em 2016 passou a contar com sistema de criptografia, mudança que agregou muito mais segurança e privacidade para os usuários relativamente às mensagens trocadas no aplicativo. (PESSOA e FILHO 2017, 4-5)

As mensagens no Wpp têm sido compartilhadas numa proporção acentuada, se comparadas aos demais aplicativos das redes sociais. Mas, diante das mudanças nas políticas de privacidade anunciadas pela Wpp, uma gama de usuários começou a migrar para outras plataformas como, por exemplo, a Signal e a Telegram. (PESSOA e FILHO 2017, 2)

As mudanças do Wpp pretendem compartilhar dados com o FB sem a necessidade do consentimento dos usuários, que os comercializará com os seus clientes. Diante de muitos questionamentos, o Wpp revisou a sua proposta de mudança na política de privacidade e anunciou a implementação no Brasil para abril de 2021.

Como forma de combater a *fake news*, a organização de checagem de notícias, “Aos Fatos”, utiliza um robô chamado FactMa (abreviação de FactMachine), que atua no Wpp, no Twitter e no Messenger. O objetivo é informar aos usuários sobre checagens realizadas e dicas que visam à verificação autônoma da notícia e a segurança para utilizar a rede de forma independente e confiável³⁶.

³⁵ (PESSOA e FILHO 2017, 4-5) “Quase um mês após o WhatsApp ter sido vendido para o Facebook por US\$ 16 bilhões, o presidente-executivo do aplicativo, Jan Koum, afirmou que a negociação não vai alterar a privacidade dos usuários, que continuarão a não ter seus dados explorados para fins comerciais de qualquer forma”. E prosseguiu: “Se a parceria com o Facebook significasse que nós tivéssemos de mudar nossos valores, nós não a teríamos feito”, pontou Koum, para quem o WhatsApp fazer parte da família Facebook ajudará que o aplicativo continue a operar de forma independente.

³⁶ <https://www.aosfatos.org/fatima/> p.1 acessado em 10/01/21

O quadro a seguir apresenta de forma detalhada as ações de combate a *fake news* que, até o momento, foram implantadas pelo Facebook, atual proprietário das demais plataformas, Wpp e Insta.

Ações	FB	Insta	Wpp
1	X		X
2			X
3		X	
4		X	
5		X	
6		X	
7	X		
8	X		
9	X		
10	X		
11	X		
12	X	X	

Legenda (fontes: AGENCIABRASIL, 2018; TECHTUDO, 2018-2019):

- 1 - atuar em parceria com agências independentes de verificação de fatos (já descrito)
- 2 – usar robô FactMa - dicas para o usuário verificar automaticamente a notícia. (já descrito)
- 3 – remover perfis suspeitos ou falsos (p.e., desinformação sobre COVID-19) (AGENCIABRASIL, 2018)³⁷
- 4 – remover conteúdos de fontes não confiáveis (AGENCIABRASIL, 2018)
- 5 – reduzir alcance conteúdos identificados *fake news* pelas agências (AGENCIABRASIL, 2018)³⁸
- 6 – usar busca com “mensagem educacional” para usuário denunciar *FAKE NEWS* (TECHTUDO, 2018)
- 7 – remover notícias falsas resultantes da pesquisa na aba explorar (TECHTUDO, 2019)³⁹
- 8 – remover incentivos econômicos para spammers - disseminador de *FAKE NEWS*. (já descrito)
- 9 - botão de contexto (mostrar informações confiáveis – fonte de artigos no Feed) (TECHTUDO, 2018)⁴⁰
- 10- notificação de contexto (alerta de que a matéria a compartilhar é antiga) (TECHTUDO, 2019)⁴¹
- 11 - tela de notificação global (links com contextos adicionais sobre COVID-19) (já descrito)
- 12 – rotular notícia classificada como falsa (já descrito)

³⁷ AGENCIABRASIL. 2018. Outra frente de atuação do Facebook é o combate aos perfis falsos, identificados como um instrumento de difusão de *fake news*. A empresa anunciou em maio que derrubou neste ano, em média, 6 milhões de contas falsas por dia. A remoção ocorreu baseada nos “parâmetros da comunidade”, regras que, quando violadas, geram a exclusão da publicação.

³⁸ AGENCIABRASIL. 2018. Em 2017, o Facebook anunciou que as checagens apareceriam como uma informação adicional. Contudo, em 2018 elas passaram a ter consequências para os autores. Aquelas mensagens consideradas falsas têm o alcance reduzido, e os usuários que as compartilharam recebem uma notificação.

³⁹ TECHTUDO. 2019. O Instagram anunciou, nesta segunda-feira (16), uma expansão em seu programa de checagem de fatos. A partir de agora, publicações que contenham fake news (notícias falsas) terão sua distribuição filtrada da aba Explorar e da pesquisa por hashtags, e exibirão um aviso de que aquele conteúdo é falso. A identificação dessas fotos e vídeos será feita usando tecnologia de aprendizado de máquina, com ajuda de empresas independentes de checagem de fatos.

⁴⁰ TECHTUDO, 2018. No começo de outubro, o Facebook lançou um botão de contexto que oferece mais detalhes sobre notícias compartilhadas no feed. A função ativa um painel que mostra a descrição do site e outros links sobre o mesmo assunto para efeito de comparação. O objetivo é ajudar ao usuário a identificar o nível de confiabilidade do material por conta própria.

⁴¹ TECHTUDO. 2019. O Instagram utilizará tecnologia de aprendizado de máquina (*machine learning*) para encontrar as fake news na rede social e para aplicar a tela de aviso. O alerta será exibido para todos os usuários que encontrarem o post, seja no feed, no perfil, nos Stories ou em mensagens do Direct. Além do alerta, um link externo disponibilizará artigos e matérias de fontes confiáveis para refutar as informações contidas no post falso.

Os provedores das redes sociais, na intenção de combater as *fake news* digitais, implantaram nas plataformas diversas funcionalidades, através da criação de facilitadores para que os usuários possam identificar e alertar sobre notícias falsas e receber informações e notificações de fontes confiáveis sobre *fake news*. Com auxílio de agências de verificação passaram a limitar com mais celeridade o alcance das publicações erradas e a alertar os usuários sobre conteúdos considerados falsos.

Criaram pesquisas simples e rápidas para captar o perfil do usuário e entender o seu comportamento a fim de identificar as suas preferências. Entretanto essa funcionalidade, de certa forma prejudicou o usuário, porquanto a partir dessa identificação, passou a só poder interagir com temas ligados às suas preferências, limitando o seu acesso a informações das mais diversas.

Nessa seara, o uso da aprendizagem de máquina para identificar *fake news* vem sendo fundamental para ajustar o sistema, de modo a disponibilizar resultados mais precisos e confiáveis.

O quadro a seguir, apresenta de forma detalhada as ações de combate a *fake news* que, até o momento, foram implantadas pelo Facebook, atual proprietário das demais plataformas, Wpp e Insta.

4. Ações para assegurar credibilidade nas informações

É fato que o que mantém o nível de credibilidade e, em consequência, a reputação dos provedores de redes sociais é a qualidade das suas informações. A veiculação de informações falsas compromete sobremaneira a credibilidade e, por isso, deve ser constantemente combatida.

Embora o uso da técnica de criptografia, que visa à garantia das propriedades de segurança, como integridade dos dados e autenticidade da origem da mensagem, seja de suma importância num sistema de comunicação, não garante a qualidade das informações, no sentido de inibir a disseminação de *fake news*.

Como forma de garantir a credibilidade, as redes sociais têm contado com o auxílio das organizações independentes de verificação de fatos e das informações veiculadas pelos órgãos oficiais do governo, inclusive a nível internacional, para combater as notícias falsas, no sentido de manter a qualidade das informações.

O usuário observa que a credibilidade das plataformas das redes sociais tem sido objeto de preocupação das mesmas para com a qualidade das informações, resultado de medidas de combate as notícias falsas já explicitadas anteriormente.

Segundo JUNIOR e SANTOS (2018, 1), a “reputação on-line dos meios de hospedagem é um fator de decisão na escolha dos clientes da Hotelaria” e “a maioria dos usuários de hotéis utilizam as

plataformas digitais para verificarem os comentários dos lugares que ficarão hospedados”. E, “que as notas atribuídas pelos clientes e os rankings que os hotéis estão posicionados nestes portais influenciam nas escolhas de qual lugar se hospedar.”.

O uso massivo das redes sociais na internet tem incentivado as empresas a investirem fortemente em marketing digital⁴² nas plataformas. Para atender a essa demanda, surgem novas formas de emprego como, por exemplo, os *influencers* digitais. (HOTMART 2019, 2)

Influencer digital (em português, blogueiro ou influenciador digital) é aquele que usa redes sociais para publicar vídeos online ou textos, com suas análises, para um público específico e que tem a capacidade de influenciar a opinião dos seus seguidores⁴³. (ALVES 2019, 1)

Nesse sentido, vem ocorrendo um aumento exponencial do marketing digital nas redes sociais, oportunidade na qual os *influencers* na busca de maior ganho com as propagandas que veiculam não se preocupam com a qualidade da informação.

Entretanto, há casos em que *fake news* são criadas com a intenção de impulsionar o acesso dos seus seguidores e, em consequência, rentabilizar com a visualização das propagandas. Para que produzam o efeito desejado, essas *fake news* são criadas de forma a obter uma identificação com os leitores, envolvendo temas que os atraiam.

Esse crescimento tem gerado uma grande preocupação com a disseminação de notícias falsas, pois na essência, coloca em cheque a credibilidade das informações e pode refletir em consequências ruins para a sociedade e para a reputação dos provedores das redes sociais.

Nesse sentido as plataformas de redes sociais têm adotado ações para assegurar a credibilidade das informações que veiculam, inclusive, em alguns casos, com a colaboração dos usuários. Buscam inibir as *fake news* ou retirar sites, que veiculam notícias falsas com o intuito de monetizar com a visibilidade dos seus seguidores ou de realmente provocar a disseminação de *fake news*.

O FB vem utilizando um sistema de verificação no qual os próprios leitores ajudam a detectar possíveis notícias falsas. Através de cliques na mensagem o leitor é capaz de denunciar uma notícia e classificar como sendo *spam*, desinteressante, indevida ou falsa.

Posteriormente essas denúncias são apuradas por agências parceiras do FB, através levantamento diário nas postagens suspeitas, para verificar a veracidade dos fatos. O FB também, através de

⁴² (HOTMART 2019, 2) “De acordo com um estudo feito pela SocialChorus, campanhas com influenciadores podem ter um engajamento até 16 vezes maior do que a publicidade em outros meios de comunicação. Outra pesquisa feita pela Nielsen, empresa especializada no comportamento dos consumidores, mostrou que 90% dos clientes confiam na recomendação de outras pessoas para comprar um produto, enquanto apenas 33% se dizem influenciados por anúncios.”

⁴³ (ALVES 2019, 1) “Veja que ser *influencer digital* é prestar o serviço de divulgação para que chegue aos seus seguidores sua vida, o que usa de roupa, de produtos, o que come, o que bebe, os lugares que frequenta, tudo de forma a demonstrar que se trata de uma publicidade confiável, agradável, de qualidade e, em contrapartida, receber uma remuneração por isso, seja por dinheiro, por permuta ou outras formas combinadas.”

verificação nas contas dos usuários, tem cancelado contas identificadas como falsas, no sentido de conter a disseminação de *fake news*.

Por sua vez, o INSTA⁴⁴ em agosto de 2019 passou a rotular, de forma automática, todo conteúdo idêntico publicado no FACE, que tenha sido classificado como falso. A intenção é marcar o conteúdo e fornecer links de artigos cujas fontes são confiáveis e desmintam a publicação do conteúdo rotulado como falso.

Nessa seara, conforme informação do Instagram Press, no início de 2020 o INSTA incorporou a opção de informar ao leitor que determinada publicação contém informações falsas. Apontamentos como esse (na figura abaixo), agregados a outros sinais, auxiliam a empresa a agir com celeridade uma vez identificado o problema e assegurar a credibilidade das informações. (CANALTECH 2019, 2)



fonte: Instagram Press

O WhatsApp e o Twitter, vêm utilizando a robô FactMa, responsável pelos projetos de Inteligência Artificial e automação da agência checadora “Aos Fatos”. O objetivo é passar informações e dicas para os usuários a fim de autonomamente, checarem a notícia, sentindo segurança e confiabilidade para tráfegar na rede, sem intermediários.⁴⁵ (AOS FATOS 2021, 1)

As plataformas de redes sociais, de uma forma geral, utilizam ferramentas tecnológicas como ML integrada a AI, através da aplicação de AL, para identificação das *fake news*. Parte significativa dessas ferramentas utiliza robôs digitais com técnicas de *deep learning*, impulsionada pelos AL de “filtro bolha”⁴⁶. (SASTRE, CORREIO e CORREIO 2018, 2)

⁴⁴ (CANALTECH 2019, 2) “Quando o conteúdo é classificado como falso (ou parcialmente falso) por um parceiro de checagem de fatos, o Instagram reduz sua distribuição e o remove das páginas Pesquisar e Hashtags. Além disso, o conteúdo também é marcado para que as pessoas saibam que não devem confiar naquela informação em questão. Quando esses marcadores são aplicados, eles aparecem para todos os usuários que visualizam esse conteúdo, não apenas no feed em si, como também no perfil, nos stories e até no direct.”

⁴⁵ (AOS FATOS 2021, 1) A Fátima – que vem de “FactMa” é uma abreviação de “FactMachine”

⁴⁶. (SASTRE, CORREIO e CORREIO 2018, 2) “De acordo com Pariser (2011), o “filtro bolha” é um conceito utilizado para denominar a ação dos algoritmos como filtros no ambiente virtual, que atuam como motores de previsão que influenciam e direcionam o acesso de conteúdo baseado no perfil e hábitos de consumo do usuário dando a sensação de eficiência na busca de ideias e informações, mas restringindo a maneira com a qual é realizada a pesquisa, ou mesmo, a definição de conteúdo. Esse mecanismo é muito utilizado, por exemplo, por buscadores como Google ou mídias sociais como o Facebook.”

O aprendizado de máquina vem sendo usado pelos provedores na identificação de mensagens contendo *fake news*, veiculadas por *influencers* para, tempestivamente, poder excluí-las e cancelar suas contas. O objetivo principal é garantir a credibilidade das informações veiculadas nas redes sociais, para não colocar em risco o grau de confiabilidade dos usuários nas plataformas.

A função “botão de contexto” foi implantada pelo FB para que o usuário possa acessar a fonte confiável de domínio sobre o assunto e, com isto, assegurar a credibilidade da informação recebida e coibir *fake news*.

O FB tem utilizado o modelo SimSearchNet, que se baseia em rede neural convolucional, destinado especificamente para detectar cópias quase exatas de imagens que contêm conteúdos enganosos ou falsos sobre coronavírus, a fim de aplicar rótulos de advertência. (SUMBALY et al, 2019)⁴⁷

Para enfrentar desafios como esse, o Facebook fez investimentos de longo prazo na pesquisa de sistemas de raciocínio visual e compreensão multimodal, desenvolvendo novas técnicas de aprendizagem auto-supervisionada e construindo plataformas de aprendizagem profunda.

Todas essas ações demonstram como é grande a preocupação que os provedores de redes sociais estão tendo para manter o nível de credibilidade e, conseqüentemente, a reputação perante os seus usuários.

5. Questões pertinentes associadas às Redes Sociais Online

Há aproximadamente cinco décadas, havia outra cultura de comunicação. A forma mais tradicional era realizada através de carta e, quando havia necessidade de ser rápida, era usado um sistema de telecomunicação (telefone, telegrama e telex).

A forma de troca de mensagens através de carta, de algum modo dificultava a formação de extensos grupos sociais que, talvez por isso, na maioria das vezes se restringia aos familiares.

Uma característica importante nas cartas escritas pelas próprias mãos do autor é a capacidade de transmitir emoções, condição mais difícil de ser observada quando são escritas de outra forma.

Antes mesmo da existência do FB, Arthur Finkelstein, que atuava no meio político dos EUA, aplicava o método *microtargeting*, que se baseava em análises demográficas sofisticadas. Esse método permitia identificar grupos, para os quais deveriam ser dirigidas cartas com mensagens segmentadas, a fim de

⁴⁷ (SUMBALY et al, 2019) Depois que verificadores de fatos independentes determinaram que uma imagem contém declarações enganosas ou falsas sobre coronavírus, o SimSearchNet, como parte de nosso sistema de indexação e correspondência de imagem de ponta a ponta, é capaz de reconhecer correspondências quase duplicadas para que possamos aplicar rótulos de advertência.

mapear os potenciais partidários. (EMPOLI 2019, 38)

Numa entrevista realizada em Praga, Finkelstein afirmou que “a coisa mais importante é que ninguém sabe nada” e que na política a verdade é o que se percebe como verdade.

Finkelstein é discípulo de Carl Schmitt, para quem na política primeiramente é necessário identificar o inimigo. E essa ação é de fundamental importância para se agrupar pessoas na luta por um mesmo objetivo.

Assim, tal qual um político, um *influencer* pode dizer uma série de verdades antes de começar a dizer uma série de mentiras e dessa forma o seu seguidor acreditará em tudo que ele dirá, sendo verdade ou *fake news*. (EMPOLI 2019, 41)

Na Itália, a partir de 2014, devido a questão migratória, foi elaborado um manual de conduta para os eleitos do M5S (Movimento 5 Estrelas)⁴⁸ que participariam de programas de TV, sugerindo a adoção de uma estratégia. (ADINOLF 2016, 3)

Como na questão da imigração afloram muitas emoções, dentre elas primeiramente o medo e a cólera, seria inútil propor soluções mais ou menos realistas, pois as famílias, tomadas por suas emoções, se sentem ameaçadas.

Logo, como pretender que essas pessoas acompanhassem um discurso puramente racional? Então a estratégia a ser utilizada pelo M5S deveria ser a transferência emocional, sugerindo: “Nós somos uma saída para a raiva e o medo”. (EMPOLI 2019, 43)

Se a raiva acumulada estimula a vontade de participar de um movimento popular, aqueles que vivem isolados e passivos diante da história tendem a aderir, principalmente num ambiente virtual, pois significa em certo sentido fazer parte de uma comunidade. Nesse ambiente, algoritmos são desenvolvidos e instaurados para dar ao indivíduo a sensação de protagonizar uma história, que achava estar condenado a ser um simples expectador. (EMPOLI 2019, 52)

Infere-se que mais importante que o significado das palavras num determinado contexto, é a influência que elas exercem sobre as emoções daqueles que nelas acreditam. Assim, usar palavras para mexer com as emoções sempre foi uma estratégia para tentar controlar as pessoas.

Segundo Jaron Lanier, “Para manter seus usuários conectados, uma empresa de redes sociais deve, sobretudo, fazer as coisas de maneira que eles se enervem, sintam-se em perigo ou tenham medo. A situação mais eficaz é aquela em que os usuários entram em estranhas espirais de um

⁴⁸ (ADINOLF 2016, 3) “AS TRÊS FASES DO M5S A evolução do M5S pode ser resumida essencialmente em três fases: a que precede o seu nascimento, durante a qual, através da notoriedade e da capacidade de entretenimento, o blogue de Beppe Grillo se impõe como uma referência política; o nascimento do Movimento, visto como megafone e coletor de instâncias provenientes de baixo, sobretudo ligadas às temáticas do ambientalismo; e, por fim, a fase de verticalização do Movimento que sucede à vitória das eleições legislativas de 2013 e que levará à constituição do grupo parlamentar europeu Europa para a Liberdade e a Democracia Direta (efd) com partidos antieuropeístas e nacionalistas e a formação de um diretório político decididamente mais profissionalizado.”

consenso muito poderoso ou, ao contrário, de sério conflito com outros usuários. Isso não acaba jamais, e é esse, exatamente, o alvo. As empresas não planejam nem organizam nenhum desses modelos de utilização. São os outros que são incitados a fazer o trabalho sujo.”.

SANTOS e SANTOS (2014, 310) afirmam, sem equívoco, que “neste período técnico-científico-informacional, a internet, através das tecnologias da informação e comunicação (computador, celulares, smartphones, tablets), enquanto possibilidade de comunicação e informação está modificando a maneira como as pessoas se relacionam, aprendem e se comunicam.

Nesse sentido, uma “convergência dos momentos” se configura no substrato socioespacial em que se conjugam, num mesmo direcionamento, mídia e tecnologias de informação e comunicação configurando, em grande medida, o aumento das redes sociais digitais que se tornam cada dia mais latentes na cultura e sociedade contemporâneas.”. (M. SANTOS 2009, 196)

Os textos veiculados nas redes sociais, em geral, têm sido analisados em função da polaridade (positiva, neutra, negativa), do volume de mensagens e das palavras mais usadas, sem a pretensão de identificar emoções expressas nas mensagens.

Segundo NOVAIS (2020, 6), “a análise de sentimento está se tornando uma ferramenta poderosa, rápida e relativamente barata que é extremamente útil para analisar muitos tipos diferentes de cenários e prever resultados futuros”.

As mensagens trocadas nas redes sociais, especialmente no FB e no TW, são essenciais para servir como base de dados para qualquer tipo de análise, na qual as opiniões pessoais têm fundamental importância, como é o caso, por exemplo, das campanhas eleitorais.

Para tratamento desses dados, tecnicamente é utilizado o processamento de linguagem natural (PNL) conjugado com o ML. Ao PNL compete expandir um conjunto original de dados, que contém informações emocionais, fomentando o ML para processar e analisar essas informações.

O tratamento dos dados prevê o uso de um *pipeline* para estruturar um conjunto de dados que atenda aos objetivos da análise. É comum utilizar algoritmo com base em dicionário (léxico) a fim de identificar nos textos palavras que exprimem emoções.

A sistemática de analisar o sentimento (emoção) evidenciado nas mensagens de textos das mídias sociais apresenta etapas como o pré-processamento. Nela o *pipeline* inicia com a tokenização realizando a conversão dos textos em uma lista de palavras simples ou tokens.

A lista de palavras é processada e comparada com um dicionário base (léxico), sendo marcados os adjetivos, verbos, advérbios e substantivos, ao tempo em que são removidas as palavras irrelevantes. Resulta num novo léxico que contém categorias gramaticais que carregam informações emocionais.

O utilizador de uma rede social, a fim de se proteger das influências dos disseminadores de *fake news*, deve preventivamente criticar as mensagens recebidas, principalmente antes de repassar. É necessário checar as notícias junto a sites oficiais e também consultar as Agências de checagem de fatos sobre a veracidade.

Tanto o Wpp quanto o TW, vem utilizando a robô FactMa, responsável pelos projetos de Inteligência Artificial e automação da agência checadora “Aos Fatos”. O objetivo é passar informações e dicas para os usuários para que de forma autônoma, possa checar a notícia, sentindo segurança e confiabilidade para trafegar na rede, sem intermediários. (AosFATOS 2021, 1)

5.1 - O acesso e as contas inautênticas

A facilidade de utilização gratuita⁴⁹, sem fins comerciais, das plataformas de redes sociais tem estimulado o acesso cada vez maior de usuários. Como consequência natural, os usuários trocam uma gama de informações, as quais nem sempre contêm notícias verdadeiras. (RAPOSO 2017, 20)

Nessa seara, perfis falsos, também conhecidos como contas inautênticas, têm sido utilizados com objetivo de disseminar *fake news*, fato que gerou um problema de ordem mundial, colocando em dúvida até as informações verídicas.

Para complicar ainda mais essa situação, o *deepfake*, criado pelo *deep learning*, através de técnica que sintetiza imagens humanas baseada em AI, possibilita que uma “falsa pessoa”, ou seja, uma conta inautêntica também se torne um *bot* com acesso livre nas redes sociais.

Os bots sociais ou contas sybil são contas de usuários controladas por algoritmos ao invés de usuários humanos, os quais têm sido usados com fins dissimulados, que variam desde influências políticas até opiniões para propagar fraudes.

Os bots sociais têm um grau de sofisticação tão elevado, que chega ter a capacidade de interagir com usuários humanos, aumentando sobremaneira a preocupação das plataformas em combatê-los quando disseminam *fake news*.

As plataformas, preventivamente, têm utilizado mecanismos de identificação de falsos perfis, inclusive *bots*, aplicando-se-lhes suspensão do uso da conta até que o usuário se identifique. Confirmada a falsidade da conta, a mesma é excluída.

Segundo os provedores das plataformas, esses procedimentos têm o objetivo de inibir a disseminação de *fake news*. Entretanto, essa proatividade das plataformas coloca em dúvida se o direito de liberdade de expressão dos usuários está sendo violado.

⁴⁹ (RAPOSO 2017, 20) “Precisas das redes sociais porque são ótimas ferramentas de comunicação, são gratuitas e obténs uma comunicação instantânea com todo o mundo.”

5.2 - A rapidez e a disseminação das informações

Segundo SILVA e SANTOS (2019, 20) “A facilidade da comunicação advinda dos meios eletrônicos a disposição dos usuários, reflete a rapidez de disseminação de conteúdo, o qual mesmo que compartilhado com as pessoas mais próximas, com o efeito cascata, possuem o condão de disseminar para um número bastante significativo de pessoas a informação.”.

O poder de disseminação se refere à visibilidade das ações de um utilizador numa rede social. A visibilidade é afetada por diversos fatores e estes em conjunto com modelos matemáticos epidemiológicos faz com que seja possível calcular o poder de disseminação de um utilizador.

O objetivo dos modelos matemáticos epidemiológicos é compreender melhor todo o processo de transmissão e propagação da doença, quer em pequenas comunidades, assim como em regiões ou países, para que se possam propor medidas que levem a um decréscimo na transmissão da doença.

Os utilizadores do tipo *youtuber* que possuem grande quantidade de seguidores, têm a possibilidade de influenciar os seus leitores, para o bem ou para o mal, através das informações que veiculam nas redes sociais, cujo poder de disseminação pode, muitas vezes, ser devastador.

Um estudo feito pelo Instituto de Tecnologia de Massachusetts (MIT) mostrou que essas notícias falsas se espalham 70% mais rápido do que as verdadeiras. (DIZIKES 2018, 6)

A disseminação massiva de desinformação digital foi identificada como uma grande ameaça. O uso de *bots*⁵⁰, principalmente os *bots* sociais, tem potencializado a velocidade de disseminação das informações de baixa credibilidade, fato que tem levado as plataformas a tentar identificar e inibir o uso dessa ferramenta destinada a espalhar *fake news*. (QUEIROZ 2018, 6)

No caso específico de PDF, o Google é um dos únicos que consegue estender seus robôs para efetuar a leitura do arquivo formatado, contudo, ler e interpretar multimídia como os arquivos de vídeo (*Flash*, *Shockwave* e outros) não é tarefa tecnologicamente fácil. (MONTEIRO e FIDENCIO 2013, 6)

Muitos utilizadores (como p.e. políticos, jornalistas, *youtuber*) têm se transformado em verdadeiros ícones da comunicação, pelas postagens e comentários que veiculam nas redes sociais através do contato digital direto com seus seguidores.

Utilizando esse canal e com uma quantidade massiva de informações é possível mapear as opiniões

⁵⁰ (QUEIROZ 2018, 6) “Um exemplo de manipulação de mídia social é o uso de bots (também conhecidos como bots sociais, ou contas sybil), contas de usuários controladas por algoritmos em vez de usuários humanos. Os bots têm sido extensivamente usados para fins dissimulados, variando de influências políticas a opiniões para perpetuar fraudes. Os bots de mídia social existentes variam em sofisticação. Alguns bots são muito simples e meramente retuitam posts de interesse, enquanto outros são mais sofisticados e têm a capacidade de interagir com usuários humanos.”

desses seguidores sobre assuntos que eles consideram importantes e, com isso, identificar, através das suas palavras, características emocionais que qualificam o perfil emocional sobre o autor das mensagens.

Nesse sentido, segundo NOVAIS et al (2018, 1) “esse é um fenômeno que está cada vez mais transformando os políticos em influenciadores digitais” e a maneira como eles se comunicam na mídia social pode ser considerada sua “assinatura pessoal”.

É fato que a cada dia vem sendo disponibilizada nas redes sociais uma grande quantidade de informações, nem sempre precisas, dificultando os usuários de confiar nas fontes das notícias recebidas e nas orientações constantes nas mensagens.

Atualmente, esse tipo de ocorrência tem gerado pânico na população brasileira no que tange a notícias e informações a respeito do COVID-19, colocando em dúvida as orientações recebidas, ainda que de fontes ditas confiáveis.

As plataformas têm implantado medidas para combater as *fake news* e disponibilizar informações confiáveis sobre o COVID-19, originadas na OMS e no Ministério da Saúde no Brasil.

5.3 - A Privacidade e o Anonimato

Diferentemente da privacidade, o anonimato é vedado pela Constituição Federal do Brasil, porém agentes inescrupulosos usando de perfis falsos acessam as redes sociais para espalhar *fake news*. Em razão disso as plataformas têm usado contra-medidas para inibir ou excluir esses falsos perfis.

Entretanto, na internet, o anonimato é muito relativizado e tem grande importância como propulsor de conteúdos considerados relevantes, atendendo dessa forma ao princípio da natureza participativa, como ocorre no *yahoo groups*. Nele, o usuário faz questionamentos que acabam assumindo uma característica pessoal.

Já a privacidade no Brasil é garantida pela Constituição Federal e pela Lei Geral de Proteção de Dados Pessoais – LGPD, sendo garantida também pela Lei de Proteção de Dados Pessoais, em Portugal.⁵¹

Especificamente em relação ao Wpp, este vem utilizando a encriptação total visando ao aumento da privacidade dos usuários, em que pese o usuário para se registrar tenha que fornecer o número do telefone.

Porém, com isso o Wpp acaba identificando todos os usuários entre os contatos existentes no

⁵¹ Vide notas 57 e 74; DRE.pt - artigo 8º da CPDHED 27/2021 e artigo 2º da LPDP 67/98.

telefone fornecido e automaticamente tem acesso aos dados dos contatos de todos os usuários, condição que gera questionamentos sobre a privacidade.

Entretanto, o risco real para a privacidade digital do utilizador normalmente está associado à informação que o mesmo partilha, consciente ou inconscientemente e à rede que ele utiliza para veiculação da mensagem.

Em razão disso, o utilizador deve analisar com a devida atenção o poder de disseminação da rede social utilizada, para que possa determinar o risco real da sua privacidade digital.

5.4 - A garantia da liberdade de expressão

Antes da internet⁵², um editor decidia se restringia ou não o impacto e o poder da palavra nos meios de comunicação. Entretanto a internet mudou essa condição, permitindo que o autor compartilhe suas mensagens sem o crivo do editor. (KLONICK 2018, 1603)

Mas as grandes plataformas das redes sociais têm arquitetado regras de tratamento dos conteúdos veiculados em suas redes, na intenção de inibir as *fake news*. Esse fato criou um campo de batalha pela liberdade de expressão na era digital.

Para garantir tecnologicamente a liberdade de expressão, é preciso utilizar ferramentas de credibilidade e criptografia a fim de garantir a segurança e a integridade dos dados.

Mas a garantia da plena liberdade de expressão, embora prevista constitucionalmente no Brasil, tem sido, de certa forma, ignorada pelas redes sociais que, no intuito de inibir as *fake news*, suspendem ou eliminam mensagens dos usuários que, na visão delas, não devem transitar na rede.

Essas ações das plataformas têm trazido questionamentos na área jurídica, porquanto ofende o direito de liberdade de expressão dos usuários, ainda que por uma causa justa (inibir as *fake news*), mas sem respaldo jurídico para adotá-las.

Como a tecnologia é controlada por pessoas, difícil imaginar como ela sozinha possa garantir essa liberdade de expressão para todos e igualmente. Para coexistirem, tecnologia e liberdade de expressão, cabe à comunidade definir quais são as regras, termos e leis, a fim de não ferir a liberdade dos outros. Este assunto será abordado juridicamente mais adiante.

⁵² (KLONICK 2018, 1603) "1. SECTION 230, THE FIRST AMENDMENT, AND THE BEGINNINGS OF INTERMEDIARY SELF-REGULATION Before the internet, the most significant constraint on the impact and power of speech was the publisher. The internet ended the speaker's reliance on the publisher by allowing the speaker to reach his or her audience directly. Over the last fifteen years, three American companies — YouTube, Facebook, and Twitter — have established themselves as dominant platforms in global content sharing. These platforms are both the architecture for publishing new speech and the architects of the institutional design that governs it. This private architecture is the "central battleground over free speech in the digital era."

6. Eficácia da tecnologia no combate as *fake news*

As plataformas de redes sociais têm implantado cada vez mais medidas para combater as *fake news* em busca da eficácia, entretanto esse é um trabalho árduo e oneroso, que requer contínuo incremento de estratégias de reconhecimento das informações falsas.

Atualmente apresentam uma eficácia parcial porque, apesar de precários, os modelos de validação e checagem das informações conseguem filtrar primariamente as *fake news* de grande engajamento ou sinalizar se a informação foi replicada diversas vezes.

O uso de instrumentos como algoritmos, aprendizado de máquina e inteligência artificial pelas plataformas de redes sociais tem sido de grande importância no combate às *fake news*.

Os algoritmos, por sua vez, têm apresentado excelentes resultados quando utilizados para filtrar informações sobre determinado tema constante nas mensagens veiculadas nas redes sociais, na identificação de notícias falsas. Atuam na prevenção de bolhas de informações com potencial nocivo.

Entretanto, questiona-se a utilização indiscriminada de algoritmos, por conta dos prejuízos causados aos usuários, quando estes são indevidamente rotulados como disseminadores de *fake news*, pois acabam tendo a imagem maculada nas redes sociais, devido à demora na retratação do provedor.

Inclusive, apesar de ser apontada como notícia falsa, muitas vezes foi causada somente pelo uso do algoritmo, objeto da pesquisa, que não considerou a totalidade do contexto da notícia.

Também têm sido utilizados modelos de identificação de bots, tornando possível traçar e banir as principais fontes de *fake news*, ação esta de grande importância, pois é imensurável a capacidade de disseminação, engajamento e reverberação de *fake news* através do uso de bots.

Por isso, para se proteger da influência dos disseminadores de *fake news*, o utilizador deve pesquisar e validar as informações recebidas, realizando consulta prévia a fontes de credibilidade e confiança.

Entendo que devido à falta de regulamentação jurídica sobre a questão das *fake news*, os provedores é que têm decidido quais mensagens se apresentam como falsas notícias. A forma para detectar e controlar as *fake news*, é a utilização das tecnologias disponíveis (Algoritmos, Aprendizado de máquina, Inteligência Artificial etc), que se mostram necessárias e eficientes.

No entanto, é preciso que o ordenamento jurídico defina limites na utilização desses instrumentos teóricos, de forma que seja evitada a censura prévia e que não viole o direito da liberdade de expressão.

No que tange à detecção de *fake news*, os provedores, além de usar os instrumentos teóricos já citados, podem contar também com o auxílio dos utilizadores nas denúncias sobre notícias falsas.

Para efeito de controle, ao definirem mensagens como *fake news*, os provedores antes de aplicar qualquer punição, deveriam primeiramente notificar o usuário sobre a fundamentação do processo de análise e da aplicação da medida.

Finalmente, os provedores deveriam estabelecer prazo e os procedimentos necessários para contestação, dando a oportunidade do contraditório e da ampla defesa.

II – ENQUADRAMENTO JURÍDICO DAS *FAKE NEWS*

Como se percebe, em plena era da sociedade da informação, as redes sociais digitais apresentam altíssimo volume de troca de mensagens entre os usuários, interagindo com notícias e informações, principalmente em consequência do confinamento provocado pelo COVID-19.

Nada tão inesperado quanto à veiculação de mensagens ou desinformações, consideradas como *fake news*, que coloca em dúvida a origem e a confiabilidade do seu conteúdo.

Notícia falsa não é novidade para a nossa sociedade porque a mídia escrita e a televisiva sempre se utilizaram de manchetes tendenciosas para conseguir incrementar a venda de seus produtos ou aumentar o índice de audiência, no caso das redes de televisão. Com advento da internet, passou a se chamar de *fake news*.

A questão é que a facilidade de acesso à internet e de utilização das redes sociais favoreceu sobremaneira a interação dos usuários. E, postando ou repassando mensagens que muitas vezes não traduzem a realidade dos fatos, acabam disseminando-as rapidamente nas redes sociais e, por vezes, causando estragos irreparáveis. A questão é como ficam os prejudicados.

Por conta disso, os provedores de aplicação têm criado mecanismos para coibir esses tipos de mensagens que seus parceiros, checadores de informações, definem como *fake news*. Mecanismos que parecem não ter respaldo jurídico e podem estar ferindo o direito à privacidade e à liberdade de expressão dos usuários.

Diante desse cenário, o Senador Alessandro Vieira apresentou ao Senado Federal o Projeto de Lei 2.630/20, intitulado “Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet”, mais conhecido como PL das *Fake News*, que visa ao tratamento legal para os casos de *fake news*.

Esse PL visa ao estabelecimento de normas relativas à transparência de redes sociais e de serviços de mensagens privadas, em especial para a responsabilidade dos provedores pelo combate à desinformação, a transparência dos conteúdos patrocinados e a atuação do poder público, estabelecendo sanções pelo descumprimento. (SENADO FEDERAL 2020)

Referido Projeto de Lei foi discutido no Senado Federal e, após várias alterações no texto original, foi aprovado e encaminhado em 03/07/20 para apreciação da Câmara dos Deputados. Atualmente o PL encontra-se em tramitação na Câmara dos Deputados, em Brasília.

É fato que a liberdade de expressão e de pensamento são direitos basilares numa sociedade democrática. As manifestações desses direitos nas redes sociais permitem uma interação sem precedentes entre os usuários de internet.

Porém, considerando a máxima de que “um direito termina onde outro começa” essas liberdades,

não são direitos absolutos, por isso muitas vezes acabam conflitando com o direito a intimidade e a honra de outrem.

Todos esses direitos mencionados estão previstos na Constituição da República Federativa do Brasil e serão abordados adiante, sob a ótica exclusiva das consequências provocadas pelas *fake news* nas comunicações veiculadas nas redes sociais digitais.

1. A Legislação Brasileira

1.1 - Constituição da República Federativa do Brasil

A atual Constituição da República Federativa do Brasil, carta magna de 1988, assegura direitos e garantias fundamentais de um Estado Democrático, elencados nos direitos individuais e coletivos. (PLANALTO.gov.br, CRFB/88 1988)

Dentre eles, vale ressaltar a livre manifestação do pensamento⁵³, sendo vedado o anonimato. Dessa forma, mensagens trocadas nas redes sociais digitais, para as quais não é possível identificar a autoria, violam essa cláusula constitucional e, portanto, é uma condicionante ao direito de liberdade do pensamento. (PLANALTO.gov.br, CRFB/88 1988, 3)

A CRFB não distingue o meio, físico ou virtual, pelo qual é livre a manifestação do pensamento. Consequentemente também não o faz em relação ao anonimato. Por essa razão, o anonimato na internet não é permitido.

Entretanto, a vedação do anonimato não é absoluta. Para determinados profissionais, como por exemplo, jornalistas, que precisam se comprometer com o sigilo⁵⁴ da fonte como forma de obter informações, o anonimato da fonte é assegurado pelo artigo 5º, inciso XIV da CRFB/88. (PLANALTO.gov.br, CRFB/88 1988, 3)

Os jornalistas, quando no exercício da profissão, são responsáveis pela veracidade da informação divulgada. Mas, caso utilizem da prerrogativa do sigilo da fonte para cometer ilícitos, não serão amparados pelo referido artigo. Assim, não se trata de um privilégio, mas garantir o direito à prestação de informação verdadeira.

Mas, ainda que o profissional jornalista utilize de um pseudônimo⁵⁵ para referenciar a fonte da sua

⁵³ (PLANALTO.gov.br, CRFB/88 1988, 3) artigo 5º, inciso IV - é livre a manifestação do pensamento, sendo vedado o anonimato.

⁵⁴ (PLANALTO.gov.br, CRFB/88 1988, 3) **Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: **XIV** - e assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.

⁵⁵ (PLANALTO.gov.br, CCB/02 2002, 3) Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome.

informação, esta estará protegida pelo artigo 19 do Código Civil Brasileiro, desde que se refira à atividade lícita. (PLANALTO.gov.br, CCB/02 2002, 3)

Nessa seara, relativamente à internet, ao usuário comum não é permitido o anonimato, embora possa usar de pseudônimo nos seus acessos às plataformas de redes sociais. Entretanto, nem sempre é fácil a sua identificação quando do cometimento de ilícitos, como no caso de *fake news* que violam direitos constitucionais.

O PL-2.630/20 que tramita em discussão na Câmara dos Deputados, prevê que os provedores de acesso armazenem por determinado tempo os acessos do usuário. Busca-se uma forma de facilitar a identificação do mesmo, quando objeto de ordem judicial para julgar atos ilícitos.

Não obstante, a argumentação de que o endereço IP do utilizador seria suficiente para identificá-lo não é válida, porque referido endereço não identifica pessoa, mas sim dispositivo e além do mais com uma precisão relativa.

Para dificultar, muitas ações ocorrem na internet através do nível *DeepWeb*⁵⁶, no qual o rastreamento é muito difícil, uma vez que são usadas ferramentas que escondem a real localização e identidade do utilizador. (HIGA 2015, 1)

Tais ações tornam o anonimato ainda mais perigoso. Em razão da dificuldade de acesso e rastreamento a *deepweb* é usada para compartilhar conteúdos ilegais, principalmente sobre venda de drogas, pedofilia e violência.

O próprio STF (2021, 4) já se pronunciou positivamente em vários julgados quanto à vedação ao anonimato, preceito fundamental da CRFB, entre eles, no julgado do RE – Recurso Especial n° 1193343⁵⁷ AgR e no da ADI – Ação Direta de Inconstitucionalidade n° 5418⁵⁸.

Apesar da restrição ao anonimato, é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença⁵⁹. Em quaisquer dos casos a manifestação do pensamento não deverá violar a intimidade, a vida privada, a honra e a imagem das pessoas⁶⁰.

⁵⁶ (HIGA 2015, 1) A deepweb, também conhecida como *deepnet* ou *undernet*, é uma parte da web que não é indexada pelos mecanismos de busca, como o Google, ficando oculta ao grande público. É um termo geral para classificar diversas redes de sites distintas que não se comunicam e cada uma tem o seu próprio método de acesso.

⁵⁷ (STF RE 1193343 2019) RE 1193343 AgR Órgão julgador: Segunda Turma Relator(a): Min. CELSO DE MELLO
Julgamento: 29/11/2019 Publicação: 12/12/2019 Ementa: [... As autoridades públicas não podem iniciar qualquer medida de persecução administrativo-disciplinar (ou mesmo de natureza penal) cujo único suporte informativo apoie-se em peças apócrifas ou em escritos anônimos.]

⁵⁸ (STF ADI 5418 2021) ADI 5418 Órgão julgador: Tribunal Pleno Relator(a): Min. DIAS TOFFOLI
Julgamento: 11/03/2021 Publicação: 25/05/2021 Ementa:
As liberdades de imprensa e de comunicação social devem ser exercidas em harmonia com os demais preceitos constitucionais, tais como a vedação ao *anonimato*, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, o sigilo da fonte e a vedação à discriminação e ao discurso de ódio.

⁵⁹ (CRFB 2021, 3) artigo 5º, inciso IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.

⁶⁰ (CRFB/88 1988, 3) artigo 5º, inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

(CRFB/88 1988, 3)

Caso ocorra essa violação, é assegurado ao ofendido o direito à indenização pelo dano material ou moral que decorrer dessa violação. Acrescente-se que ao ofendido é assegurado o direito de resposta, proporcional ao agravo sofrido⁶¹. (CRFB/88 1988, 3)

Nesse contexto todo cidadão que se sinta ofendido com palavras incluídas nas mensagens veiculadas nas redes sociais digitais que violam a sua intimidade, sua vida privada, sua honra ou imagem, tem o direito de resposta e, por via judicial, a ser indenizado.

Entretanto, não obstante esses direitos, considerando a velocidade com que as mensagens transitam nas redes sociais, torna-se inevitável seu prejuízo moral. Isto porque ao demandar tempo para recorrer à via judicial visando à retirada da mensagem, ela já deve ter disseminado na rede e efetuado o estrago.

Talvez uma solução seja a possibilidade de um pronto atendimento ao ofendido para retirada da mensagem, através de solicitação dirigida diretamente aos responsáveis pela plataforma da qual o autor se utilizou.

A liberdade do pensamento, como registrada na carta magna (CRFB/88 1988, 3), tem um sentido muito mais amplo do que uma simples manifestação. É um direito a crença religiosa⁶² ou a convicção filosófica ou política⁶³. É uma garantia implícita ao pleno exercício do direito de acesso à internet, conforme artigo 8º da Lei 12.965/14⁶⁴.

Para CANOTILHO (2014, 132)⁶⁵, há uma série de direitos que são protegidos pela liberdade de expressão do pensamento. Em sentido amplo essa liberdade é um direito multifuncional que se desdobra num conjunto de direitos comunicativos fundamentais.

Segundo o STF, em julgamento da ADI – Ação Direta de Inconstitucionalidade nº 4451⁶⁶, a liberdade do pensamento é condição essencial para o exercício da democracia. Não à toa, com o risco

⁶¹ (CRFB/88 1988, 3) artigo 5º, inciso V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem.

⁶² (CRFB/88 1988, 3) artigo 5º, inciso VIII - ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei;

⁶³ (CRFB/88 1988, 3) artigo 5º, inciso VI - é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias.

⁶⁴ (PLANALTO.gov.br, Lei 12.965/14 2014, 3) Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet

⁶⁵ CANOTILHO (2014, 132) [... que dele decorrem naturalmente, como seja, por exemplo, a liberdade de expressão *stricto sensu*, de informação, de investigação acadêmica, de criação artística, de edição de jornalismo, de imprensa, de radiodifusão, de programação, de comunicação individual, de telecomunicação e comunicação em rede. As liberdades comunicativas encontram-se ainda associadas a outras liberdades, como a liberdade de profissão, a livre iniciativa econômica, de prestação de serviços e o direito de propriedade].

⁶⁶ (STF ADI 4451 2019, 1) ADI 4451 Órgão julgador: Tribunal Pleno Relator(a): Min. ALEXANDRE DE MORAES
Julgamento: 21/06/2018 Publicação: 06/03/2019

[... Democracia não existirá e a livre participação política não florescerá onde a liberdade de expressão for ceifada, pois esta constitui condição essencial ao pluralismo de ideias, que por sua vez é um valor estruturante para o salutar funcionamento do sistema democrático. ...]

da proliferação de *fake news*, os maiores interessados no PL das *fake news* são os que ocupam cargo nos três poderes, principalmente no Legislativo. (STF, ADI 4451 2019, 1)

Reação até compreensível haja vista que, na grande maioria das vezes, as mensagens que têm veiculado nas redes sociais dizem respeito a ações provenientes de integrantes de órgãos dos três poderes, que as interpretam como um ataque à democracia.

Entretanto, para o cidadão comum esses ataques se traduzem em crimes contra a honra⁶⁷, como é o caso da calúnia, difamação ou injúria, atingindo a dignidade da pessoa humana, direito fundamental da nossa Constituição. Esse direito também está amparado no Código Penal Brasileiro, o qual será abordado mais adiante.

Vale ressaltar que o Brasil é signatário (CÂMARA DOS DEPUTADOS 1992,1) do Pacto de San José da Costa Rica, objeto da Convenção Americana sobre Direitos Humanos ocorrida em 1969, que estabeleceu proteção para as liberdades individuais e respeito aos direitos humanos. Nele, a liberdade de expressão⁶⁸ merece destaque para este trabalho. (PLANALTO.gov.br, Decreto 678/92 1992)

Por sua vez, a Constituição Federal da República do Brasil, em seu artigo 220⁶⁹, trata da comunicação social visando à garantia da liberdade de pensamento e informação, numa forma livre de qualquer tipo de restrição. E essa liberdade de informação implica numa comunicação completa, verdadeira e imparcial, essencial na construção da percepção que o indivíduo terá do mundo. (PLANALTO.gov.br, CRFB/88 1988)

Não obstante, a forma livre de comunicação sem restrições já foi objeto de punição por abuso no

⁶⁷ (CRFB 2021, 3) art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

⁶⁸ (PLANALTO.gov.br, Decreto 678/92 1992) Pacto São José da Costa Rica. Artigo 13 - Liberdade de Pensamento e de Expressão

1. Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e idéias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha.

O exercício do direito previsto no inciso precedente não pode estar sujeito à censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei a ser necessária para assegurar:

a) o respeito aos direitos ou à reputação das demais pessoas; ou
b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral pública.
3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de freqüências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de idéias e opiniões.
4. A lei pode submeter os espetáculos públicos à censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2º.
5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade, ao crime ou à violência.

⁶⁹ (PLANALTO.gov.br, CRFB/88 1988), art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística. [...].

exercício da liberdade de imprensa, mediante regulamentação dos artigos 9º e 10 da Lei 2.083/53⁷⁰ e artigo 11 do Decreto 24.776/34⁷¹, ambos não recepcionados pela Constituição Federal da República do Brasil em 1988.

Em razão de tudo isso, há uma grande expectativa da população para que o PL 2.630/20 das *fake news* possa permitir minimizar a proliferação de *fake news* e seus efeitos sem, entretanto, prejudicar a garantia da liberdade de expressão e da livre manifestação do pensamento do cidadão brasileiro.

1.2 - Marco Civil da Internet

As primeiras discussões sobre a criação de um Marco regulatório da internet para o Brasil surgiram em função de Projeto de Lei de crimes virtuais, proposto ao Senado Federal, pelo senador Eduardo Azeredo em 2007⁷². O PL não prosperou, devido ao entendimento de que, antes de se definir regras criminais, o tema deveria ser tratado ao nível de regulamentação civil. (SENADO FEDERAL PLC 89/03 2003)

Muitas críticas⁷³ foram dirigidas ao referido Projeto de Lei. A principal delas se baseava no fato de que era necessário definir regras e as responsabilidades das operadoras, das empresas e dos usuários,

⁷⁰ (PLANALTO.gov.br, Lei 2.083/53 1953, 3) art 9º Constituem abusos no exercício da liberdade de imprensa, sujeitos às penas que vão ser indicadas, os seguintes fatos:

- b) publicar notícias falsas ou divulgar fatos verdadeiros, truncados ou deturpados, que provoquem alarma social ou perturbação da ordem pública
- e) ofender a moral pública e os bons costumes
- f) caluniar alguém, imputando-lhe falsamente fato definido como crime
- g) difamar alguém imputando-lhe fato ofensivo à sua reputação
- h) injuriar alguém, ofendendo-lhe a dignidade ou o decôro
- i) obter favor ou provento indevidos, mediante a publicação ou a ameaça de publicação de escrito ou representação figurativa desabonadoras da honra ou da conduta de alguém

art 10. São também puníveis a calúnia, a difamação e a injúria contra a memória de alguém, na forma das letras *f*, *g* e *h* do art. 9º http://www.planalto.gov.br/ccivil_03/leis/L2083.htm p.1 acessado em 07/05/21

⁷¹ Decreto 24.776/34 REVOGADO - Liberdade de Imprensa, Art. 11 - Publicar notícias falsas, ou noticiar fatos verdadeiros, umas e outros, porém, tendenciosamente, por forma a provocar alarme social, ou perturbação da ordem pública; — penas de multa de 500\$ a 2.000\$ ou prisão por um a seis meses.

⁷² (SENADO FEDERAL PLC-89/03 2003) 8ª versão do PLC 89 de 2003 do Senador Eduardo Azeredo.

⁷³ (CONJUR 2013, 1) O advogado e professor do Instituto Internacional de Ciências Sociais Marcos Bitelli destacou pontos que, na sua visão, deveriam ser melhorados no substitutivo ao projeto do Marco Civil da Internet. “Se o projeto defende a liberdade de expressão tem que deixar bem claro que é vedado o anonimato”, defendeu. “A internet hoje é terra do anonimato.”

O diretor de relações governamentais da Cisco — empresa fabricante de equipamentos de internet —, Giuseppe Marrara, também afirmou que o conceito de neutralidade de rede não pode ser absoluto. “Não se trata de permitir condutas anticoncorrenciais”, salientou. Na visão dele, o marco civil, por ser uma espécie de Constituição da internet, deve se atrelar a princípios básicos e ser flexível, “para não congelar” a rede.

Favorável ao princípio da neutralidade proposto, a advogada do Instituto Brasileiro de Defesa do Consumidor (Idec) Veridiana Alimonti afirmou que o texto “garante tratamento isonômico aos usuários”. Veridiana esclareceu que o princípio não impede a oferta de pacotes com velocidades de conexão diferentes e preços equivalentes. A advogada criticou a oferta de pacotes diferenciados de acordo com os valores pagos: “Acesso digno à rede é aquele em que o usuário não fique preso ao seu e-mail e ao seu perfil na rede social. Não é verdade que, de acordo com o modelo defendido pelas empresas, o consumidor vai escolher o que contratar. Assim, é o seu bolso que definirá e não há democracia”, alertou.

Eduardo Cunha, no entanto, alertou que o texto atual do relator da proposta, Alessandro Molon (PT-RJ) vai proibir a venda de pacotes com velocidades diferentes para acesso a toda a web. “Não tem nenhum artigo do substitutivo que diga que possa haver velocidade diferenciada. Do jeito que está o projeto, proíbe sim”, garantiu.

De acordo com João Vianey Xavier Filho, representante da Polícia Federal, um dispositivo no projeto pode prejudicar a investigação policial. Trata-se da parte que prevê que o provedor de internet responsável pela guarda de dados pessoais do usuário e do registro de acesso a aplicações de internet só será obrigado a disponibilizar essas informações mediante ordem judicial.

antes de definir regras criminais. (CONJUR 2013, 1)

Em 23/04/2014, foi criada a Lei nº 12.965, conhecida como Marco Civil da Internet, estabelecendo princípios, garantias e direitos e deveres para o uso da internet no Brasil. A lei disciplina o uso da internet com destaque no fundamento do respeito à liberdade de expressão. (PLANALTO.gov.br, Lei 12.965/14 2014)

Referida Lei também considera como fundamentais, entre outros, os direitos humanos, desenvolvimento da personalidade, exercício da cidadania em meios digitais, pluralidade, diversidade, livre iniciativa e a livre concorrência. O objetivo é promover maior transparência e garantir confiança no uso da internet.

A liberdade de expressão diz respeito a um direito oponível ao Estado, onde deste é exigida uma abstenção no sentido de não impedir a livre expressão do pensamento do cidadão. Ao contrário da censura que leva a uma estagnação cultural, a liberdade de expressão influencia no progresso da raça humana.

Vale esclarecer que, segundo o Enunciado 613, da VIII Jornada de Direito Civil realizada pelo Conselho da Justiça Federal em 24/05/18, “art. 12: A liberdade de expressão não goza de posição preferencial em relação aos direitos da personalidade no ordenamento jurídico brasileiro.”. (CJF 2018, 1)

A tese⁷⁴ de que a liberdade de expressão tem preferência sobre os demais direitos da personalidade tem sido difundida em decorrência da estreita conexão com o princípio democrático. Entretanto, os demais direitos da personalidade também possuem elevado peso abstrato, tendo em vista conexão direta com a dignidade da pessoa humana. (STF, RCL 22.328 MC/RJ 2015, 1)

Independentemente da preferência ou não do direito à liberdade de expressão em relação aos demais direitos da personalidade, a liberdade de expressão⁷⁵ e a privacidade são condições essenciais para o pleno exercício do direito de acesso nas comunicações via internet.

Segundo LAURENTIIS & THOMAZINI (2020, 2266), “Enfim, na realidade da troca de informações eletrônicas, há sempre indivíduos interessados em sustentar o seu próprio ponto de vista, para quem a

⁷⁴ (STF, RCL 22.328 MC/RJ 2015, 1) RCL 22.328 MC / RJ – STF Ministro Luis Roberto Barroso

A Carta de 88 incorporou um sistema de proteção reforçado às liberdades de expressão, informação e imprensa, reconhecendo uma prioridade prima facie destas liberdades públicas na colisão com outros interesses juridicamente tutelados, inclusive com os direitos da personalidade. Assim, embora não haja hierarquia entre direitos fundamentais, tais liberdades possuem uma posição preferencial (preferred position), o que significa dizer que seu afastamento é excepcional, e o ônus argumentativo é de quem sustenta o direito oposto.

⁷⁵ (PLANALTO.gov.br, Lei 12.965/14 2014) art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:

I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias /14decorrentes de serviços prestados no Brasil.

busca da verdade não passa de um interesse entre outros que devem ser atropelados”. E acrescenta que “[...] ideias são reguladas e combatidas por meio de outras ideias, não com poder ou força. Essa é a origem da liberdade de expressão.”.

Registra-se que, na sua concepção, a Lei do Marco Civil da Internet trata de assuntos ligados a questão da neutralidade da rede, a retenção de dados, a privacidade dos usuários e as obrigações dos provedores responsáveis pela disponibilização dos serviços de internet.

Como forma de garantir a livre manifestação do pensamento, o sistema adotado é da responsabilidade subjetiva. Dessa forma, torna-se necessário demonstrar a culpa de quem deu causa ao dano para que eventual condenação possa ocorrer. Na prática, esse sistema dificulta a defesa do cidadão que tem a reputação (honra objetiva) ou a auto-estima (honra subjetiva) ofendida por outrem na internet.

Referida Lei⁷⁶, em seus artigos 18 e 19, isenta os provedores de redes sociais digitais da responsabilidade civil por danos causados em razão de conteúdos produzidos por terceiros, exceto se, após recebimento de ordem judicial específica, não tomarem as devidas providências no prazo estipulado pelo Juízo. Percebe-se que essa isenção se assemelha à proteção dada aos ISPs, na CDA, Section 230.

Quanto aos direitos e garantias dos usuários, destaca-se o direito a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei. Na realidade, trata-se do sigilo do fluxo de dados na internet, cujo direito já estava estabelecido no artigo 5º, inciso XII, da Constituição Federal⁷⁷.

Para FRANÇA (1996, 939-940), enquanto direito de personalidade, o direito à integridade moral protege a liberdade política e civil, a honra, ao recato, ao segredo, a imagem e a identidade pessoal, familiar e social.

Essa é uma questão polêmica, pois dependendo dos fatores fáticos a comunidade jurídica se divide nas suas decisões relativamente a esse direito fundamental. Afinal, torna-se difícil definir quais seriam as limitações da privacidade da pessoa humana.

No caso de colisão entre direitos de personalidade, a IV Jornada de Direito Civil do CJF – Conselho da Justiça Federal, em seu enunciado nº 274, previu que se deve adotar a técnica de ponderação. A

⁷⁶ (PLANALTO.gov.br, Lei 12.965/14 2014) art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

⁷⁷ (CRFB 2021, 3) art. 5º, inciso XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

fim de se buscar a melhor solução, deve o aplicador do Direito sopesar os princípios e direitos fundamentais no caso concreto. (CJF 2006, 35)

O desenvolvimento dessa técnica, no direito comparado, foi atribuído ao jurista alemão ALEXY (2008, 116-118). Para ilustrar a incidência dessa técnica de ponderação, apontamos o julgado do TST em 2005 que, ao contrário do que se esperava, legitimou um empregador a fiscalizar o e-mail corporativo do seu empregado utilizado no ambiente de trabalho. (TST RR613 2005)

No que concerne ao direito de propriedade e ao direito à privacidade, ambos são protegidos pela Constituição Federal no Brasil. Normalmente, o e-mail de um usuário é privativo, entretanto neste caso específico, aplicada a técnica da ponderação, o julgado foi decidido em favor do empregador.

Os dados pessoais dos usuários também são objeto de proteção na Lei 12.965/14, nomeadamente nos incisos VII e seguintes⁷⁸ do artigo 7º, não permitindo o fornecimento a terceiros, exceto quando houver consentimento livre, expresso e informado ou previsão legal.

Vale registrar que tanto a autoridade administrativa, a autoridade policial, quanto o Ministério Público poderá, cautelarmente, requerer que qualquer provedor de conexão (ou provedor de acesso) guarde os registros de conexão, por um prazo superior ao período de manutenção obrigatória por 1 ano.⁷⁹

Referidas autoridades também poderão, cautelarmente, requerer que qualquer provedor de aplicações de internet guarde os registros de acesso, inclusive por um prazo superior ao período de manutenção obrigatória de 6 meses.⁸⁰

Fica evidente o grande poder de controle que tem o provedor de conexão, tendo em vista que é responsável pela ponte entre usuário e internet.

Notório que a Lei 12.965/14 foi um grande avanço no ordenamento jurídico brasileiro quanto à criação de um Marco regulatório para a internet, mas referida Lei deixa a desejar quando se trata de

⁷⁸ (PLANALTO.gov.br, Lei 12.965/14 2014, 3) art. 7º, incisos VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

⁷⁹ (PLANALTO.gov.br, Lei 12.965/14 2014, 5) art. 13, § 2º - A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

⁸⁰ (PLANALTO.gov.br, Lei 12.965/14 2014, 5) art. 15, § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

fake news, que afeta a honra de alguém, uma vez que exige ação judicial para supressão do conteúdo ilícito.

Isso porque, a demora numa decisão judicial é altamente prejudicial, tendo em vista que o fator tempo é determinante para que maiores consequências possam ser evitadas.

De acordo com o artigo 18, da Lei 12.965/14, Marco Civil da Internet, o provedor de conexão não pode se responsabilizar civilmente em razão de danos causados por conteúdos gerados por terceiros, uma vez que a sua atividade se restringe à promoção da conexão entre os usuários.

Em seu artigo 19, referida Lei define que o provedor de aplicações só poderá se responsabilizar civilmente em razão de danos causados por conteúdos gerados por terceiros se, havendo ordem judicial específica, não tornar indisponível o conteúdo dentro do prazo estabelecido judicialmente.

Ocorre que, como a internet é uma rede mundial, ao estabelecer normativos restritos ao Brasil, não consegue aplicação efetiva da Lei, como no caso da ação movida pela atriz Daniela Cicarelli, cuja decisão judicial prejudicou, ainda que temporariamente, todos os usuários do Youtube.com no Brasil. (FILHO 2016, 5)

Conforme Enunciado 554 do STJ, na IV JORNADA DE DIREITO CIVIL, independe de indicação do local específico da informação na ordem judicial para que o provedor de hospedagem bloqueie determinado conteúdo ofensivo na internet. (CJF Enunciado 554, 2006)

Portanto, a solução dada pela Lei 12.965/14, Marco Civil da Internet, apresenta-se totalmente contrária à jurisprudência do STJ – Superior Tribunal de Justiça brasileiro.

Cita-se como exemplo de graves implicações na área de saúde pública, a disseminação de *fake news* sobre COVID-19, como é o caso de movimentos questionando a eficácia da vacinação no combate ao coronavírus.

Não à toa, o Ministério da Saúde preocupado com os problemas advindos dessas desinformações, criou um portal específico para prestar esclarecimentos à população a respeito desse tema. Fica claro que, se não fosse dessa forma, seria desastrosos aguardar por decisões judiciais para retirada desse tipo de conteúdo.

Nesse contexto, percebe-se a necessidade de incluir outras formas de combate a *fake news*, que não somente através do meio judicial, para que seu conteúdo possa ser suprimido com a devida celeridade e evitar danos à vítima, decorrentes da propagação nos meios virtuais.

1.3 – LGPD - Lei Geral de Proteção de Dados

A Lei Brasileira nº 13.709, criada em 14/08/18, intitulada Lei Geral de Proteção de Dados Pessoais – LGPD⁸¹ estabelece tratamento de dados pessoais, inclusive nos meios digitais, com objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (PLANALTO.gov.br, Lei 13.709/18 2018, 1)

Questiona-se na literatura sobre a adaptabilidade da tecnologia da informação à LGPD, fato que traz insegurança jurídica sobre a aplicabilidade da lei e das pertinentes ações a serem tomadas visando ao *compliance*. (PLANALTO.gov.br, Lei 13.709/18 2018)

Não resta dúvida de que a TI – Tecnologia da Informação é um poderoso recurso estratégico que pode auxiliar as empresas no monitoramento dos seus processos, especificamente em relação ao tratamento de dados.

Entretanto, na Europa, segundo CARVALHO et al (2019,21-30), escândalos de espionagem com divulgação de dados pessoais de clientes que envolveram a Cambridge Analytica e o Facebook foram objeto de discussão, que resultou na regulamentação da GDPR – *General Data Protection Regulation* quanto à segurança de dados no âmbito da União Europeia.

No Brasil, em 2014, a empresa VELOX foi acusada de ilegalmente vender dados pessoais de clientes para terceiros. E em 2015, empresa britânica de consultoria teve acesso aos dados pessoais de milhões de usuários do Facebook com a intenção de promover análise comportamental de eleitores dos EUA, segundo ZANATTA (2015, 447).

No que diz respeito à privacidade, a sistemática tecnológica utilizada para analisar sentimentos através das emoções evidenciadas nos textos das mensagens veiculadas nas redes sociais visando à identificação do autor, parece colocar em risco a proteção da LGPD relativamente a dados sensíveis do usuário.

Os resultados dessa análise podem apontar comportamentos como homofobia, xenofobia, racismo, intolerância religiosa etc, condição que, uma vez rotulada pelos provedores, particulariza o usuário, expõe a sua privacidade e, em consequência, fere princípios da LGPD.

Vale ressaltar que as redes sociais utilizam as preferências explicitadas pelos usuários nos conteúdos das suas mensagens, para personalizar recursos e produtos com base nessas preferências.

⁸¹ (PLANALTO.gov.br, Lei 13.709/18 2018, 1) art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Esses dados, embora considerados sensíveis, sendo disponibilizados publicamente pelos seus titulares, não gozam da proteção da LGPD.

Essa poderosa ferramenta tecnológica de análise de sentimentos, é aplicada sobre palavras e estilos presentes nos textos veiculados nas redes sociais. Tem a capacidade de revelar informações sobre preferências, pensamentos, emoções e comportamentos do usuário.

Tais revelações acabam identificando dados sensíveis do usuário, os quais são protegidos pela LGPD e permitem que sejam tiradas conclusões a respeito de uma pessoa. Quanto ao seu tratamento, só pode ser realizado mediante consentimento⁸² específico e destacado pelo titular. (PLANALTO.gov.br, Lei 13.709/18 2018, 5)

Embora se reconheça o avanço tecnológico com o desenvolvimento dessa ferramenta, tal identificação coloca em risco a privacidade do usuário. Isto porque, ao que parece, não há consentimento do usuário para realização do tratamento dos seus dados sensíveis, podendo expor, p.e., a sua opinião política ou religiosa.

Nessa seara, diante dos princípios e direitos previstos na LGPD, é questionável a licitude do tratamento desses dados pelos provedores quando utilizam a referida ferramenta sem o específico e destacado consentimento do titular, exigido por Lei.

Por outro lado, em relação à proteção dos dados pessoais, a LGPD admite como exceção⁸³ a dispensa da exigência do consentimento, quando o titular manifestamente torna público os seus dados pessoais. (PLANALTO.gov.br, Lei 13.709/18 2018, 3)

Sem dúvida, uma das preocupações do usuário é o possível vazamento de seus dados pessoais, objeto de proteção da LGPD. Mas há um receio quanto à violação do direito de liberdade de expressão porque, em razão do fenômeno das *fake news*, todas as mensagens são tratadas pelos provedores.

Nesses tratamentos, quando o provedor rotula a mensagem como *fake news*, são geradas consequências como, a retirada da mensagem nas redes sociais, a emissão de alerta sobre a mesma e até o cancelamento da conta do usuário junto ao provedor. Ações que, à primeira vista, não parecem garantir a liberdade de expressão.

É fato que existe uma relação muito próxima entre o poder do provedor sobre a informação e a proteção da liberdade de expressão, tanto que quando àquele interessa, ela é admitida, mas quando representa uma ameaça, ela é descartada.

⁸² (PLANALTO.gov.br, Lei 13.709/18 2018, 5) art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

⁸³ (PLANALTO.gov.br, Lei 13.709/18 2018, 3) art 7º, §4º - *É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta lei.*

O artigo 19⁸⁴ da Declaração Universal de Direitos Humanos prevê que todo indivíduo tem direito à liberdade de opinião e de expressão. Nos EUA, por exemplo, a proteção dessa liberdade impede que o Congresso lhe imponha muitas restrições. (MDH.gov.br 2018, 1)

O combate aos abusos no exercício da liberdade de manifestação do pensamento e informação iniciou-se no Brasil com a criação da Lei 5.250/67, conhecida como Lei de Imprensa. Em seu artigo 16, a publicação ou divulgação de *fake news* era penalizada com detenção e multa. Registra-se que referida Lei não foi recepcionada pela Carta Magna de 1988.

A CRFB em seu artigo 220⁸⁵ garante a isenção de qualquer tipo de restrição sobre manifestações do pensamento, criações, expressões e informações, veiculadas sob qualquer forma. E veda qualquer censura de natureza política, ideológica e artística. (PLANALTO.gov.br, CRFB/88 1988)

Por sua vez, o provedor de conexão tem o dever de tratar de forma isonômica as comunicações eletrônicas pela internet, sem qualquer tipo de restrição, garantindo a não discriminação das publicações.⁸⁶ (PLANALTO.gov.br, Lei 12.965/14 2014)

De certo, tanto aquele que implantou ou repassou uma notícia falsa, quanto o veículo de comunicação que divulgou a mensagem, deveria ser responsabilizado. Entretanto, o artigo 18, da Lei 12.965/14⁸⁷ isenta os ISPs dessa responsabilidade. (PLANALTO.gov.br, Lei 12.965/14 2014)

A rigor, a LGDP aplicada no combate às *fake news* auxilia na questão da liberdade⁸⁸ de expressão e opinião, da privacidade⁸⁹ e da proteção dos dados pessoais. Não obstante, estes podem ser liberados por ordem judicial para identificação dos usuários que postam notícias falsas, as quais tenham repercutido negativamente em relação à honra, imagem ou prejuízo financeiro a outrem. (PLANALTO.gov.br, Lei 13.709/18 2018) (PLANALTO.gov.br, Lei 12.965/14 2014)

Quem sabe, no Brasil, uma solução que garanta a liberdade de expressão, com uma mínima intervenção jurídica quanto às restrições adotadas, seja implantar um modelo similar ao EUA.

⁸⁴ (MDH.gov.br 2018, 1) [...] que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão.

⁸⁵ (PLANALTO.gov.br, CRFB/88 1988) art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

⁸⁶ (PLANALTO.gov.br, Lei 12.965/14 2014) artigo 9º - O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

⁸⁷ (PLANALTO.gov.br, Lei 12.965/14 2014) art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

⁸⁸ (PLANALTO.gov.br, Lei 13.709/18 2018) art 2º, inciso III - A disciplina da proteção de dados pessoais tem como fundamentos: a liberdade de expressão, de informação, de comunicação e de opinião;

⁸⁹ (PLANALTO.gov.br, Lei 12.965/14 2014) art 7º, inciso VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

1.4 - Crimes de responsabilidade

No ordenamento jurídico brasileiro a classificação doutrinária de crime de responsabilidade diz respeito a ações ilícitas cometidas por agentes políticos. A Lei 1.079/50, em seu artigo 2º, define que, ainda que tentados, os crimes são passíveis da pena de perda do cargo, com inabilitação até cinco anos para exercício de qualquer função pública. (PLANALTO.gov.br, Lei 1.079/50 1950)

Segundo SILVA (2014, 497-498)⁹⁰, a simples eleição não garante o pleno exercício da democracia, pois os governantes precisam responder pelo uso dos seus poderes, sob pena de cometer crime de responsabilidade, definidos na CRFB/88.

Os crimes comumente cometidos através das mídias, tradicionais e nas redes sociais, são crimes contra a honra de outra pessoa: calúnia, difamação e injúria.

Esses crimes, na doutrina brasileira, são classificados como “crime comum”, uma vez que o tipo penal não exige qualquer qualidade ou condição especial tanto para o sujeito ativo quanto para o sujeito passivo, segundo GRECO (2015, 417).

Para GRECO (2015, 1054), a classificação doutrinária de crime próprio diz respeito ao sujeito ativo, pois que somente o funcionário público pode praticá-lo. E o crime comum ao sujeito passivo, uma vez que não somente a Administração Pública pode figurar nessa condição, como qualquer pessoa que tenha sido prejudicada com o comportamento praticado pelo sujeito ativo.

Os crimes de responsabilidade são aqueles cometidos por agentes públicos, no exercício do cargo, assim definidos no ordenamento jurídico brasileiro, distintamente como crime de improbidade administrativa e *impeachment*.

Segundo GRECO (2015, 48), crimes de responsabilidade correspondem a infrações político-administrativas cujas sanções importam a vacância do cargo, a desinvestidura do agente e sua inabilitação por período de tempo certo para o exercício de funções públicas.

Crimes dessa natureza consistem em sanções não penais, conforme preconiza o artigo 52, parágrafo único da CRFB/88 e podem ser aplicadas sem prejuízo destas.

Prevista na Lei 8.429/92⁹¹, nos seus artigos 1º, 2º e 3º, a ação de improbidade abarca todo

⁹⁰ SILVA (2014, 497-498) Nos regimes democráticos não existe governante irresponsável. Não há democracia representativa sem eleição. “Mas a só eleição, ainda que isenta, periódica e lisamente apurada, não esgota a realidade democrática, pois, além de mediata ou imediatamente resultante de sufrágio popular, as autoridades designadas para exercer o governo devem responder pelo uso que dele fizerem, uma vez que ‘governo irresponsável, embora originário de eleição popular, pode ser tudo, menos governo democrático.’”

⁹¹ (PLANALTO.gov.br, Lei 8.429/92 1992) Art. 1º Os atos de improbidade praticados por qualquer agente público, servidor ou não, contra a administração direta, indireta ou fundacional de qualquer dos Poderes da União, dos Estados, do Distrito Federal, dos Municípios, de Território, de empresa incorporada ao patrimônio público ou de entidade para cuja criação ou custeio o erário haja concorrido ou concorra com mais de cinquenta por

agente público vinculado à Administração Pública, inclusive os não servidores. Já o *impeachment* se refere a crime de improbidade praticado por agentes públicos, desde que no pleno exercício do cargo.

O *impeachment* se fundamenta na Lei 1.079/50 (PLANALTO.gov.br, Lei 1.079/50 1950) em combinação com o artigo 52, inciso I da CRFB/88⁹² e se aplica aos agentes públicos ativos definidos no artigo 85, incisos I a VII da CRFB/88⁹³. (PLANALTO.gov.br, CRFB/88 1988)

Os agentes políticos que a Lei se refere, são os que ocupam cargo de Presidente da República, Ministros de Estado, Ministros do Supremo Tribunal Federal e Procurador Geral da República.

Os crimes de responsabilidade são específicos para cada agente, em função do cargo ocupado, seja de Presidente da República⁹⁴, Ministros de Estado⁹⁵, Ministros do Supremo Tribunal Federal⁹⁶ ou

cento do patrimônio ou da receita anual, serão punidos na forma desta lei.

Parágrafo único. Estão também sujeitos às penalidades desta lei os atos de improbidade praticados contra o patrimônio de entidade que receba subvenção, benefício ou incentivo, fiscal ou creditício, de órgão público bem como daquelas para cuja criação ou custeio o erário haja concorrido ou concorra com menos de cinquenta por cento do patrimônio ou da receita anual, limitando-se, nestes casos, a sanção patrimonial à repercussão do ilícito sobre a contribuição dos cofres públicos.

Art. 2º Reputa-se agente público, para os efeitos desta lei, todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nas entidades mencionadas no artigo anterior.

Art. 3º As disposições desta lei são aplicáveis, no que couber, àquele que, mesmo não sendo agente público, induza ou concorra para a prática do ato de improbidade ou dele se beneficie sob qualquer forma direta ou indireta.

⁹² (PLANALTO.gov.br, CRFB/88 1988)

Art. 52. Compete privativamente ao Senado Federal:

I - processar e julgar o Presidente e o Vice-Presidente da República nos crimes de responsabilidade, bem como os Ministros de Estado e os Comandantes da Marinha, do Exército e da Aeronáutica nos crimes da mesma natureza conexos com aqueles;

⁹³ (PLANALTO.gov.br, CRFB/88 1988)

Art. 85. São crimes de responsabilidade os atos do Presidente da República que atentem contra a Constituição Federal e, especialmente, contra:

- I - a existência da União;
- II - o livre exercício do Poder Legislativo, do Poder Judiciário, do Ministério Público e dos Poderes constitucionais das unidades da Federação;
- III - o exercício dos direitos políticos, individuais e sociais;
- IV - a segurança interna do País;
- V - a probidade na administração;
- VI - a lei orçamentária;
- VII - o cumprimento das leis e das decisões judiciais.

⁹⁴ (PLANALTO.gov.br, Lei 1.079/50 1950) art. 4º São crimes de responsabilidade os atos do Presidente da República que atentem contra a Constituição Federal, e, especialmente, contra:

- I - A existência da União;
- II - O livre exercício do Poder Legislativo, do Poder Judiciário e dos poderes constitucionais dos Estados;
- III - O exercício dos direitos políticos, individuais e sociais;
- IV - A segurança interna do país;
- V - A probidade na administração;
- VI - A lei orçamentária;
- VII - A guarda e o legal emprego dos dinheiros públicos;
- VIII - O cumprimento das decisões judiciais (Constituição, artigo 89)

⁹⁵ (PLANALTO.gov.br, Lei 1.079/50 1950) art. 13. São crimes de responsabilidade dos Ministros de Estado;

- 1 - os atos definidos nesta lei, quando por eles praticados ou ordenados;
- 2 - os atos previstos nesta lei que os Ministros assinarem com o Presidente da República ou por ordem deste praticarem;
- 3 - A falta de comparecimento sem justificação, perante a Câmara dos Deputados ou o Senado Federal, ou qualquer das suas comissões, quando uma ou outra casa do Congresso os convocar para pessoalmente, prestarem informações acerca de assunto previamente determinado;
- 4 - Não prestarem dentro em trinta dias e sem motivo justo, a qualquer das Câmaras do Congresso Nacional, as informações que ela lhes solicitar por escrito, ou prestarem-nas com falsidade.

⁹⁶ (PLANALTO.gov.br, Lei 1.079/50 1950) art. 39. São crimes de responsabilidade dos Ministros do Supremo Tribunal Federal:

- 1- altera, por qualquer forma, exceto por via de recurso, a decisão ou voto já proferido em sessão do Tribunal;
- 2 - proferir julgamento, quando, por lei, seja suspeito na causa;
- 3 - exercer atividade político-partidária;
- 4 - ser patentemente desidioso no cumprimento dos deveres do cargo;
- 5 - proceder de modo incompatível com a honra dignidade e decôro de suas funções.

Procurador Geral da República⁹⁷. No entanto, nenhum desses crimes resulta em ofensa à honra de um cidadão. (PLANALTO.gov.br, Lei 1.079/50 1950)

Nessa seara, vale ressaltar que os crimes contra a honra, no ordenamento jurídico brasileiro, são classificados como crimes comuns e não como crimes de responsabilidade. Quanto à natureza, os crimes contra a honra se dividem em crimes de natureza objetiva (calúnia e difamação) e de natureza subjetiva (injúria).

São considerados crimes contra a honra, a calúnia, a difamação e a injúria. A calúnia ocorre quando alguém atribui a outrem um falso crime. A difamação ocorre quando alguém ofende a reputação de outrem. E a injúria ocorre quando alguém ofende a dignidade ou decoro de outrem. Todos serão tratados mais adiante, sob a ótica do Direito Penal.

1.5 - Liberdade de manifestação do pensamento e da informação

A facilidade de acesso aos meios de comunicação favoreceu o livre fluxo da troca de informações nas redes sociais e nos aplicativos de mensageria, fato que estimulou sobremaneira a manifestação do pensamento dos seus usuários.

O direito da livre manifestação do pensamento é assegurado pelo artigo 5º, inciso IV da CRFB/88, sendo vedado o anonimato. O inciso VIII deste mesmo artigo, assegura que ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se descumprir obrigação fixada em lei.

A CRFB/88 também garante a livre expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.

Quanto à comunicação social, o artigo 220⁹⁸ da CRFB/88 elimina qualquer tipo de restrição à

Art. 39-A. Constituem, também, crimes de responsabilidade do Presidente do Supremo Tribunal Federal ou de seu substituto quando no exercício da Presidência, as condutas previstas no art. 10 desta Lei, quando por eles ordenadas ou praticadas.

Parágrafo único. O disposto neste artigo aplica-se aos Presidentes, e respectivos substitutos quando no exercício da Presidência, dos Tribunais Superiores, dos Tribunais de Contas, dos Tribunais Regionais Federais, do Trabalho e Eleitorais, dos Tribunais de Justiça e de Alçada dos Estados e do Distrito Federal, e aos Juizes Diretores de Foro ou função equivalente no primeiro grau de jurisdição.

⁹⁷ (PLANALTO.gov.br, Lei 1.079/50 1950) art. 40. São crimes de responsabilidade do Procurador Geral da República:

- 1 - emitir parecer, quando, por lei, seja suspeito na causa;
- 2 - recusar-se a prática de ato que lhe incumba;
- 3 - ser patentemente desidioso no cumprimento de suas atribuições;
- 4 - proceder de modo incompatível com a dignidade e o decôro do cargo.

Art. 40-A. Constituem, também, crimes de responsabilidade do Procurador-Geral da República, ou de seu substituto quando no exercício da chefia do Ministério Público da União, as condutas previstas no art. 10 desta Lei, quando por eles ordenadas ou praticadas.

Parágrafo único. O disposto neste artigo aplica-se:

- I – ao Advogado-Geral da União;
- II – aos Procuradores-Gerais do Trabalho, Eleitoral e Militar, aos Procuradores-Gerais de Justiça dos Estados e do Distrito Federal, aos Procuradores-Gerais dos Estados e do Distrito Federal, e aos membros do Ministério Público da União e dos Estados, da Advocacia-Geral da União, das Procuradorias dos Estados e do Distrito Federal, quando no exercício de função de chefia das unidades regionais ou locais das respectivas instituições.

⁹⁸ (PLANALTO.gov.br, CRFB/88 1988) CAPÍTULO V - DA COMUNICAÇÃO SOCIAL

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação

manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, sendo vedada toda e qualquer censura de natureza política, ideológica e artística. (PLANALTO.gov.br, CRFB/88 1988)

Neste sentido, a CRFB/88 amplia o regime de liberdade relativamente à atuação da imprensa, deixando-a salvaguardada de qualquer tipo de restrição quando do seu exercício, independentemente do suporte da veiculação, físico ou tecnológico.

O Código de Ética dos Jornalistas Brasileiros – CEJB de 2007⁹⁹ prevê em seu artigo 2º que o jornalista não pode ser impedido, por nenhum tipo de interesse, de divulgar informação de forma precisa e correta, sendo esse um dever dos meios de comunicação. (CEJB 2007)

Para RODRIGUES (2009, 55), a liberdade de expressão está na possibilidade de se exteriorizar e transmitir opiniões ou pensamentos para outras pessoas, principalmente àquelas que tenham ponto de vista divergente.

Enquanto direito de informar, para SILVA (2012, 264) a liberdade de manifestar o pensamento, nada mais é do que um direito individual que foi tomado por um sentido coletivo, transformado pelos meios de comunicação.

A CRFB/88, em seu artigo 1º, inciso III, prevê como direito e garantia fundamental, além de outros, a dignidade da pessoa humana. Em seu artigo 4º, inciso II, a CRFB/88 rege-se, nas relações internacionais, pelo princípio da prevalência dos direitos humanos.

1.6 - Código Penal

É fato que as mensagens veiculadas nas redes sociais têm sido muitas vezes, objeto de ofensas ou inverdades em relação a pessoas ou fatos, que acabam violando direitos individuais garantidos pela CRFB/88, como é o caso da inviolabilidade da honra.

O ordenamento jurídico brasileiro considera como crimes contra a honra, a calúnia, a difamação e a injúria. São classificados como “crimes comuns” e se dividem em crimes de natureza objetiva (calúnia e difamação) e de natureza subjetiva (injúria).

social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

⁹⁹ (CEJB 2007) art. 2º Como o acesso à informação de relevante interesse público é um direito fundamental, os jornalistas não podem admitir que ele seja impedido por nenhum tipo de interesse, razão por que:

I - a divulgação da informação precisa e correta é dever dos meios de comunicação e deve ser cumprida independentemente de sua natureza jurídica - se pública, estatal ou privada - e da linha política de seus proprietários e/ou diretores.

II - a produção e a divulgação da informação devem se pautar pela veracidade dos fatos e ter por finalidade o interesse público;

III - a liberdade de imprensa, direito e pressuposto do exercício do jornalismo, implica compromisso com a responsabilidade social inerente à profissão;

IV - a prestação de informações pelas organizações públicas e privadas, incluindo as não-governamentais, é uma obrigação social.

V - a obstrução direta ou indireta à livre divulgação da informação, a aplicação de censura e a indução à autocensura são delitos contra a sociedade, devendo ser denunciadas à comissão de ética competente, garantido o sigilo do denunciante.

Enquanto a honra subjetiva, se manifesta internamente no indivíduo em razão do amor próprio, valor moral, social e da autoestima, a honra objetiva se vincula às qualidades como ele é visto pelos outros, como o respeito, a reputação e a fama.

A calúnia ocorre quando alguém atribui a outrem um falso crime. A difamação ocorre quando alguém imputa um fato que ofende a reputação de outrem. E a injúria ocorre quando alguém ofende a dignidade ou decoro de outrem.

A CRFB/88, em seu artigo 5º, inciso X, garante a inviolabilidade da honra do cidadão e ainda assegura o direito de ser indenizado pelo dano sofrido. O Código Penal Brasileiro, em seus artigos 138, 139 e 140, assenta penalidades para os crimes de calúnia¹⁰⁰, difamação¹⁰¹ e injúria¹⁰². (PLANALTO.gov.br, Decreto 2.848/40 1940, 45-47)

O Código Penal Brasileiro¹⁰³, em seu artigo 141, §2º determina a aplicação em triplo da pena quando o crime contra a honra for cometido ou divulgado em qualquer modalidade das redes sociais da rede mundial de computadores. (PLANALTO.gov.br, Decreto-Lei 2.848/40 1940, 45-47)

Os crimes contra a honra podem até mesmo atingir outros direitos, como o direito ao nome, à imagem e à privacidade, os quais são garantidos pela CRFB/88 e pelos artigos 17¹⁰⁴, 20¹⁰⁵ e 21¹⁰⁶ do

¹⁰⁰ (PLANALTO.gov.br, Decreto 2.848/40 1940, 45-47) art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2º - É punível a calúnia contra os mortos.

Exceção da verdade

§ 3º - Admite-se a prova da verdade, salvo:

I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;

II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

¹⁰¹ (PLANALTO.gov.br, Decreto 2.848/40 1940, 45-47) art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa.

Exceção da verdade

Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

¹⁰² (PLANALTO.gov.br, Decreto 2.848/40 1940, 45-47) art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II - no caso de retorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem **aviltantes**:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3º - Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:

Pena - reclusão de um a três anos e multa.

¹⁰³ (PLANALTO.gov.br, Decreto 2.848/40 1940, 45-47) art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:

§ 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.

¹⁰⁴ (PLANALTO.gov.br, CCB/02 Lei 10.406/02 2002) art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.

¹⁰⁵ (PLANALTO.gov.br, CCB/02 Lei 10.406/02 2002) art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

¹⁰⁶ (PLANALTO.gov.br, CCB/02 Lei 10.406/02 2002) art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Código Civil Brasileiro – CCB de 2002. (PLANALTO.gov.br, CCB/02 Lei 10.406/02 2002)

Para GODOY (2008, 28), à honra se vinculam noções de como o indivíduo se vê e de como é visto pela sociedade, no meio em que vive.

Quanto às matérias sem comprovação de veracidade veiculadas nas redes sociais e nas mídias tradicionais, observa-se o fenômeno contemporâneo da desinformação, o qual tem provocado um descrédito de grande proporção por parte dos usuários.

III – O PROJETO DE LEI 2.630/20 – LEI DAS *FAKE NEWS*

As relações interpessoais na internet favoreceram o surgimento de grupos sociais virtuais. São verdadeiras comunidades inseridas no ciberespaço cuja interação e facilidade de acesso permitiu a troca de mensagens e informações de forma rápida e abrangente.

Entretanto, em muitos países democráticos a diversidade e o nível crescente de informações conflitantes veiculadas nas redes sociais, nas mídias tradicionais e em sites políticos, têm falseado matérias jornalísticas, disseminando desinformações.

É fato que a perda de confiança nas instituições pode levar o cidadão a desacreditar nas informações oficiais e passar a se fiar em fontes não oficiais como meio de informação e comunicação.

Mas a preocupação não se restringe somente à desinformação. Uma parte considerável das mensagens veiculadas nas redes sociais e mídias tradicionais apresenta verdadeiro ataque à honra de personalidades do meio político.

DEROSA (2018, 5) lembra o que David Lazer publicou em um de seus artigos, quando comentou que notícias falsificadas não são novidade, pois sempre existiram. E que nos últimos anos as *fake news* ganharam sua “versão politicamente orientada”.¹⁰⁷

Não é de se estranhar que essa situação tem gerado uma grande preocupação no meio político, que julga ser objeto de insegurança para a legitimidade democrática.

Por conta disso, diversos Projetos de Lei têm sido apresentados visando à coibição de boatos, notícias falsas e desinformação, quer por motivos políticos, econômicos ou pessoais.

Nesse sentido, em 13/05/20, o Senador Alessandro Vieira, do partido Cidadania/SE, propôs um Projeto de Lei específico¹⁰⁸ (PL-2.630) para tratar dessa questão. O PL pretendia combater a desinformação e dar transparência aos conteúdos pagos. Ficou conhecido como o PL das *fake news*, cuja relatoria no Senado coube ao Senador Ângelo Coronel (PSD-BA). (SENADO FEDERAL PL-2.630, 2020)

O relator afirmou que o referido Projeto de Lei era apenas um primeiro passo em defesa da população quanto à desinformação e assédio virtual. E, completou que é preciso avançar sobre a criminalização de condutas, pois é constrangedor constatar penas irrisórias para quem ofende alguém na internet. (SENADO FEDERAL PL-2.630, 2020)

¹⁰⁷ DEROSA (2018, 5). FAKE NEWS - Quando os jornais fingem fazer jornalismo. Conforme artigo de David Lazer e outros: “o que os autores querem dizer é que grande parte do conteúdo do que eles chamam de fake news é simplesmente conteúdo conservador ou de direita. Ao que parece, a hegemonia da esquerda em todo o aparato midiático não tolera vozes discordantes e tão logo surjam são imediatamente catalogadas como um problema global a ser resolvido.”

¹⁰⁸ (SENADO FEDERAL PL-2.630/20, 2020) Estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções para o descumprimento da lei.

O Projeto de Lei em questão visava a desestimular abusos e/ou manipulações que tinham potencial de causar danos individuais ou coletivos, estabelecendo normas, diretrizes e mecanismos de transparência nas redes sociais e serviços de mensageria privada.

Os objetivos constantes no texto original do PL eram fortalecer o processo democrático por meio do combate à desinformação, fomentar a diversidade das informações na internet, dar transparência aos conteúdos pagos e desencorajar o uso de contas inautênticas para disseminar desinformação.

Registra-se a seguir, mudanças realizadas no texto original do PL-2.630/20 no SENADO FEDERAL, com alterações significativas quanto aos objetivos, aos princípios, à atuação do poder público e às sanções previstas para os infratores.

Para os provedores de aplicação com menos de dois milhões de usuários registrados, que ofereçam serviço de rede social ao público brasileiro, essas normas não se aplicam. A intenção é servir de parâmetro para que esses provedores apliquem programas de boas práticas, com medidas proporcionais de combate à desinformação.

Entretanto, seu escopo se estende aos provedores de aplicação não sediados no Brasil desde que ofereçam serviços ao público brasileiro ou que, pelo menos, algum integrante do mesmo grupo econômico esteja estabelecido no Brasil.

Os objetivos¹⁰⁹ do PL passaram a ter foco na garantia da liberdade de expressão, no impedimento da censura, no comportamento inautêntico, na moderação dos conteúdos postados e nos conteúdos impulsionados e publicitários. (CÂMARA DOS DEPUTADOS 2020, 2)

O texto original definia “conta inautêntica” como sendo aquela criada ou usada com o propósito de disseminar desinformação ou assumir identidade de terceira pessoa para enganar o público.

Essa definição foi alterada, passando a considerar como sendo contas criadas ou usadas com o propósito de assumir ou simular identidade de terceiros para enganar o público, ressalvados o direito ao uso de nome social e à pseudonímia, bem como o explícito ânimo humorístico ou de paródia.

Observa-se com isto, que a alteração realizada no referido PL não considerou o propósito de disseminar desinformação como característica de uma conta inautêntica, fato que induz a interpretação de que não se deu importância às *fake news*.

O PL 2.630/20 prevê que os provedores de redes sociais e de serviços de mensageria privada

¹⁰⁹ (CÂMARA DOS DEPUTADOS 2020, 2) art 4º incisos I – o fortalecimento do processo democrático por meio do combate ao comportamento inautêntico e às redes de distribuição artificial de conteúdo e do fomento ao acesso à diversidade de informações na internet no Brasil;

II – a defesa da liberdade de expressão e o impedimento da censura no ambiente online;

III – a busca por maior transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais, com a garantia do contraditório e da ampla defesa;

IV – a adoção de mecanismos e ferramentas de informação sobre conteúdos impulsionados e publicitários disponibilizados para o usuário

adotem medidas preventivas¹¹⁰ a fim de proteger a liberdade de expressão e o acesso à informação, fomentando o livre fluxo de ideias na internet. (CÂMARA DOS DEPUTADOS 2020, 3)

Dentre os princípios basilares do PL, pautados no artigo 3º, destacam-se a liberdade de expressão e de imprensa, a garantia dos direitos individuais, como personalidade, dignidade, honra e privacidade, bem como o respeito ao usuário na livre formação de preferências políticas.

Nessa seara, o artigo 6º prevê que é vedado aos provedores de redes sociais e de serviços de mensageria privada restringir conteúdos religiosos, políticos ou manifestações artísticas intelectuais, observada a CRFB/88 em seu artigo 5º, inciso IX e no artigo 220¹¹¹. (PLANALTO.gov.br, CRFB/88 1988, 3 e 110)

Vale ressaltar a distinção definida no artigo 3º do PL, entre “Rede de distribuição artificial” e “Impulsionamento”. Este nada mais é do que uma ampliação do alcance de conteúdos, viabilizados através de pagamento pecuniário. Aquele, se refere a contas automatizadas ou tecnologia utilizada para comportamento coordenado e articulado na distribuição de conteúdos.

Em ambos os casos, são consideradas ações lícitas apenas aquelas promovidas por empresas enquadradas no referido PL, principalmente as relativas às redes de distribuição artificial, que utilizam interface de programação de aplicações, com a finalidade de impactar de forma artificial a distribuição de conteúdos.

O PL considera que as empresas jornalísticas que promoverem conteúdos nos termos do artigo 222 da CRFB/88¹¹² não serão consideradas provedores de redes sociais. Atribuir este entendimento ao

¹¹⁰ (CÂMARA DOS DEPUTADOS 2020, 3) art 6º incisos I – vedar o funcionamento de contas inautênticas;

II – vedar contas automatizadas não identificadas como tal, entendidas como aquelas cujo caráter automatizado não foi comunicado ao provedor de aplicação e, publicamente, aos usuários; e

III – identificar todos os conteúdos impulsionados e publicitários cuja distribuição tenha sido realizada mediante pagamento ao provedor de redes sociais.

§ 1º As vedações do caput não implicarão restrição à manifestação artística, intelectual ou de conteúdo satírico, religioso, político, ficcional ou literário, ou a qualquer outra forma de manifestação cultural, nos termos dos arts. 5º, inciso IX, e 220 da Constituição Federal.

§ 2º A identificação de conteúdos impulsionados e publicitários de que trata este artigo deve ser disponibilizada de maneira destacada aos usuários e mantida inclusive quando o conteúdo ou mensagem for compartilhado, encaminhado ou repassado de qualquer maneira.

§ 3º Os provedores de redes sociais e de serviços de mensageria privada devem desenvolver procedimentos contínuos para melhorar sua capacidade técnica para o cumprimento das obrigações estabelecidas neste artigo.

§ 4º Os provedores de redes sociais e de serviços de mensageria privada devem adotar medidas técnicas que viabilizem a identificação de contas que apresentem movimentação incompatível com a capacidade humana, devendo informá-las em seus termos de uso ou outros documentos disponíveis aos usuários. Os provedores de redes sociais e de serviços de mensageria privada desenvolverão políticas de uso que limitem o número de contas controladas pelo mesmo usuário.

¹¹¹ (PLANALTO.gov.br, CRFB/88 1988, 3)

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.

(PLANALTO.gov.br, CRFB/88 1988, 110)

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

¹¹² CRFB/88 art. 222. A propriedade de empresa jornalística e de radiodifusão sonora e de sons e imagens é privativa de brasileiros natos ou naturalizados há mais de dez anos, ou de pessoas jurídicas constituídas sob as leis brasileiras e que tenham sede no País.

referido artigo, s.m.j., não parece ter conexão com o fato dessas empresas jornalísticas não se enquadrarem como provedores de redes sociais, uma vez que nada impede que possam vir a ser.

Em relação aos seus usuários, o PL prevê que os provedores de redes sociais e de serviços de mensageria privada podem requerer suas identificações, inclusive através da apresentação de documento de identidade válido.

Essa previsão só é possível nos casos de indícios de contas inautênticas, automatizadas não identificadas ou nos casos de cumprimento de ordem judicial. Mas, o PL não determina se os indícios devem ser devidamente comprovados, fato que pode gerar transtornos para os usuários pré-julgados pelos provedores.

Quanto aos serviços de mensageria privada, o PL 2.630/20 determina em seu artigo 9º, que os provedores devem criar políticas de utilização que, entre outros termos, limite o número de encaminhamento de uma mesma mensagem a usuários ou grupos e limite o número máximo de membros por grupo.

Referido artigo aparenta refletir uma preocupação do legislador quanto a uma possível disseminação de mensagens para múltiplos destinatários cujo conteúdo possa vir a causar danos coletivos. Essa limitação parece ser uma forma de buscar restringir ou reduzir o alcance das mensagens.

Em seu artigo 10, o PL considera que “encaminhamento em massa” é o envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 dias, tanto para grupos de conversa, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários.

Neste sentido, define que os registros relativos a essas mensagens deverão ser guardados pelo prazo de três meses pelos serviços de mensageria privada, resguardada a privacidade dos seus conteúdos. O acesso a esses registros dependerá de ordem judicial, tanto para constituir prova em investigação criminal, quanto para instrução processual penal.

Não obstante, a obrigatoriedade dessa guarda não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 usuários e, neste caso, seus registros deverão ser destruídos, conforme preceitua a LGPD, uma vez não atendendo aos princípios¹¹³ de finalidade, adequação e necessidade. (PLANALTO.gov.br, Lei 13.709/18 2018, 4)

O PL deixa explícito que os provedores de aplicação de internet devem garantir o direito de acesso à

¹¹³ (PLANALTO.gov.br, Lei 13.709/18 2018, 4) art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

informação e à liberdade de expressão de seus usuários. Porém, em caso de denúncia ou de medida aplicada em função de violação dos termos de uso das aplicações, o usuário deverá ser notificado sobre a fundamentação, o processo em análise e a aplicação da medida.

O artigo 12 determina que o provedor deverá garantir o direito de o usuário recorrer da indisponibilização de conteúdos/contas. Caso seja caracterizado dano decorrente de interpretação equivocada de conteúdos caberá ao provedor de redes sociais reparar, no âmbito e nos limites técnicos do serviço.

Ainda de acordo com o artigo 12 os provedores estão dispensados de notificar o usuário caso verifiquem risco: de dano imediato de difícil reparação; para a segurança da informação ou do usuário; de violação a direito de crianças e adolescentes; de preconceito de raça ou cor, entre outros.

Em qualquer dos casos o usuário terá direito de defesa, porém o prazo para essa defesa será diferido quando se tratar de conteúdo que use imagem ou voz manipulada para imitar candidato a cargo público, induzindo a erro acerca da sua identidade.

Quanto à questão da transparência, o PL prevê que os provedores de redes sociais devem produzir relatórios trimestrais, a serem disponibilizados em seus sítios eletrônicos para informar procedimentos e decisões de tratamento de conteúdos.

A identificação de todos os conteúdos impulsionados e publicitários é exigida pelo PL de forma a registrar a conta responsável pelo impulsionamento ou do anunciante, permitindo ao usuário acesso a essas informações de contato.

Para os impulsionamentos de propaganda eleitoral (PLANALTO.gov.br, Lei 9.504 1997), os provedores de redes sociais devem disponibilizar ao público todo o conjunto de anúncios, visando à transparência do sistema, incluindo valores gastos, tempo de veiculação etc.

Os provedores de redes sociais e de serviços de mensageria privada, segundo o parágrafo 3º do artigo 6º do PL, devem adotar medidas técnicas que viabilizem a identificação de contas que apresentem movimentação incompatível com a capacidade humana. Assim constatadas, devem informá-las em seus termos de uso ou outros documentos disponíveis aos usuários.

O parágrafo 5º do artigo 6º do PL prevê que os provedores de redes sociais e de serviços de mensageria privada desenvolvam políticas de uso que limitem o número de contas controladas pelo mesmo usuário.

Para o agente político, caso possua mais de uma conta em uma plataforma, deverá indicar aquela que representa oficialmente seu mandato ou cargo, sendo as demais eximidas das obrigações submetidas aos princípios da Administração Pública.

As sanções previstas no artigo 31 do PL sujeitam os provedores de redes sociais e de serviços de mensageria privada à aplicação de advertência ou multa, sem prejuízo de responder pelas demais sanções civis, criminais ou administrativas.

O artigo 30 do PL prevê que os provedores de redes sociais e de serviços de mensageria privada poderão criar instituição de autorregulação com atribuições focadas na transparência e na responsabilidade no uso da internet.

Dentre essas atribuições, destaca-se o desenvolvimento de boas práticas, em articulação com empresas de telefonia móvel, para suspensão de contas de usuários cuja autenticidade for questionada ou cuja inautenticidade for estabelecida.

O PL determina que as instituições de autorregulação terão que ser certificadas por um Conselho de Transparência e Responsabilidade na Internet, o qual está previsto para ser instituído pelo Congresso Nacional no prazo de até sessenta dias contados da aprovação e publicação dessa Lei.

Registra-se que os pontos anteriormente elencados, são parte integrante do texto original do PL-2.630/20 proposto e discutido no SENADO FEDERAL e são considerados temas importantes para o presente estudo.

Durante o trâmite no Senado Federal, o PL-2.630 foi objeto de 1.239 Requerimentos e 152 Emendas dos Parlamentares, com as mais diversas proposições de alteração. Entre elas, a alteração do nome do PL das FAKE NEWS, que passou a se chamar Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. (SENADO FEDERAL 2020, 2)

Registra-se que o PL 2.630/20, cuja proposição foi do Senador Alessandro Vieira (Cidadania/SE) e a relatoria do Senador Ângelo Coronel (PSD-BA), teve um intervalo de menos de dois meses entre sua proposição e a aprovação do texto final, incluindo sessões nas comissões específicas, sessões deliberativas em plenário e avaliação de possíveis emendas ao texto final.

A aprovação do PL 2.630/20 pelo Senado Federal ocorreu em junho/20. Referido Projeto foi encaminhado e recebido pela Câmara dos Deputados no dia 21/06/20. O texto preliminar foi objeto de uma série de mudanças, que resultaram em inclusões e exclusões na redação da proposta original.

Em agosto de 2020, após um ciclo de debates, o coordenador do grupo de trabalho na Câmara dos Deputados, Deputado Federal Orlando Silva (PC do B-SP), apresentou um substitutivo ao texto preliminar recebido do Senado Federal, alterando vários pontos como penas, transparência, rastreabilidade e outros.

Vale lembrar que atualmente existem mais de 60 Projetos de Lei na Câmara dos Deputados apensados ao PL 2.630/20 os quais sugerem propostas diversas, entre elas, relativas à desinformação

e/ou à regulação das plataformas das redes sociais.

É bem verdade que várias dessas propostas sequer passaram pela apreciação do Senado Federal, quando o PL 2.630/20 por lá tramitou no ano de 2020. Mas, também não foram objeto de discussão nos debates promovidos após o recebimento do referido PL na Câmara dos Deputados.

Em 15/04/21, com base no atendimento ao Mérito e ao artigo 54 do RICD¹¹⁴ – Regulamento Interno da Câmara dos Deputados, foi solicitado parecer de diversas Comissões Especiais da Câmara, as quais elencamos: (CÂMARA DOS DEPUTADOS RICD 1989)

- CCTCI - Comissão de Ciência e Tecnologia, Comunicação e Informática
- CFT – Comissão de Finanças e Tributação
- CCJC – Comissão de Constituição e Justiça e de Cidadania

Registra-se que, embora o PL 2.630/20 tenha sido distribuído para essas Comissões, até início de 2021 nenhum parecer havia sido apresentado. E, após longos meses sobrestado, o PL 2.630/20 só voltou a ser discutido no Parlamento em junho de 2021.

Essa paralização se deu, em razão de troca na composição da mesa de direção da Câmara, da formação de novas coligações políticas e anulação das distribuições para apreciação nas diferentes Comissões de mérito da Câmara.

Quanto à direção, em 1º de fevereiro de 2021, em eleição decidida logo em 1º turno pela maioria absoluta dos votos, o deputado Arthur Lira (PP-AL) foi nomeado presidente da Câmara dos Deputados, tomando posse logo em seguida.

Em sessão extraordinária (virtual) de 09/06/2021, o presidente Arthur Lira decidiu pela transformação da sessão plenária em Comissão Geral para debate da regulamentação do combate à desinformação, as chamadas *fake news*.

O novo presidente da Câmara delegou a análise do PL 2.630/20 a um GT (grupo de trabalho) específico, em lugar de seguir o rito tradicional da Câmara dos Deputados através de uma Comissão Especial.

Referido GT iniciou suas atividades no começo de julho de 2021, sendo presidido pela deputada Bruna Furlan (PSDB-SP) e tendo como relator o deputado Orlando Silva (Pc do B-SP).

O GT analisou e aprovou uma série de requerimentos solicitando audiências públicas com mais de uma centena de nomes para serem ouvidos. A intenção seria aproveitar o período de recesso

¹¹⁴ (CÂMARA DOS DEPUTADOS RICD 1989) art. 54. Será terminativo o parecer:

I - da Comissão de Constituição e Justiça e de Cidadania, quanto à constitucionalidade ou juridicidade da matéria

II - da Comissão de Finanças e Tributação, sobre a adequação financeira ou orçamentária da proposição;

III - da Comissão Especial referida no art. 34, II, acerca de ambas as preliminares.

parlamentar para realizar essas audiências, uma vez que o GT tem o prazo de 90 dias para apresentar um parecer sobre o PL.

No despacho proferido no dia 7 de junho de 2021, Lira apensou ao PL das fake news o Projeto de Lei 693/20, que tipifica o crime de divulgação ou compartilhamento de informações falsas que atentem contra a segurança sanitária.

Em decorrência disso, o PL 2.630/20 foi redistribuído para também tramitar na Comissão de Seguridade Social e Família (CSSF), como mais uma comissão de mérito do texto. Dessa forma, por força regimental, o texto deveria ser analisado por uma Comissão Especial.

Assim, com base no atendimento ao Mérito e ao artigo 54 do RICD – Regulamento Interno da Câmara dos Deputados, o PL 2.630/20 foi distribuído para colher parecer das seguintes Comissões Especiais da Câmara:

- CCJC - Comissão de Constituição e Justiça e de Cidadania
- CCTCI – Comissão de Ciência e Tecnologia, Comunicação e Informática
- CFT - Comissão de Finanças e Tributação
- CSSF - Comissão de Seguridade Social e Família

Ressalta-se que até a presente data nenhum parecer foi apresentado pelas Comissões Especiais para as quais o PL foi distribuído. Até seria justificável porque ainda não completaram os 90 dias de prazo que o GT tem para apresentar parecer.

Entretanto, na realidade, as tratativas desse PL 2.630/20 foram sobrestadas em razão do andamento e direcionamento dos parlamentares para com a CPI da COVID.

VI – MEDIDAS PROCESSUAIS OU CAUTELARES DE COMBATE AS *FAKE NEWS*

Nos últimos cinco anos tem-se evidenciado uma crescente e exponencial quantidade de mensagens veiculando nas diversas plataformas de redes sociais e nas mídias tradicionais. Mensagens essas que, por vezes, conflitam quanto aos conteúdos, gerando desconfiança por parte dos usuários/leitores relativamente à veracidade das notícias.

Esse fenômeno, que mais parece uma “era de desinformação”, é altamente perigoso porque gera incerteza do que seja realmente verdade sobre determinados assuntos importantes para a sociedade como saúde, política, educação etc.

No Brasil, desde a última eleição presidencial, uma quantidade significativa de mensagens principalmente sobre política tem dominado as comunicações nas plataformas de redes sociais, muitas vezes veiculando notícias falsas. O meio político tem acompanhado com bastante preocupação esse fenômeno, que considera um perigo para a democracia.

Tramita a passos lentos na CÂMARA DOS DEPUTADOS o Projeto de Lei nº 2.630/20, conhecido popularmente como Lei das Fake News, embora urgente sua aprovação quanto ao processo da normatização da comunicação nas redes sociais visando a coibir veiculação de fake news.

No Projeto de Lei 2.630/20 original foi proposto que os provedores apliquem programas de boas práticas através de medidas proporcionais ao combate à desinformação. Finalizado no Senado Federal, referido PL alterou os objetivos para, entre eles, propor o combate ao “comportamento inautêntico”.

Entretanto referida alteração, dentre as demais considerações constantes do artigo 5º para efeito do PL 2.630/20 não definiu o que vem a ser “comportamento inautêntico”, fato que, s.m.j., deixa a sua interpretação muito subjetiva.

No que diz respeito às exclusões de páginas e aos bloqueios de canal, a proposta do Projeto de Lei 2.630/20 impõe que os provedores de serviço estabeleçam em suas políticas de uso transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais, garantindo ao usuário o direito do contraditório e da ampla defesa.

Não obstante pendente a aprovação de uma Lei sobre fake news, o Marco Civil da Internet, Lei 12.965/14, normatizou o uso da internet, que acaba regulando as veiculações de mensagens pelas redes sociais.

Conforme o Marco Civil da Internet, a neutralidade da rede é um princípio que vale para todos os provedores e reflete no princípio da isonomia, onde todos são iguais perante a Lei.

Enfatiza-se isso, porque os conteúdos das mensagens que têm veiculado nas redes sociais têm

apresentado um viés político claramente polarizado, entre direita e esquerda. E o que se critica é que está havendo vários pesos e várias medidas por parte dos provedores, violando o princípio da isonomia, princípio basilar do Marco Civil da Internet.

Diante desse viés político, muitas críticas e agressões verbais têm sido veiculadas nas redes sociais, ofendendo a honorabilidade de Instituições e também de seus integrantes, podendo ser consideradas como ataque a democracia.

Segundo a CRFB/88 cabe a PGR – Procuradoria Geral da República¹¹⁵, receber a denúncia, investigar e decidir sobre a pertinência da abertura ou não de um processo penal por crimes contra a honra (calúnia, difamação e/ou injúria). (PLANALTO.gov.br, CRFB/88 1988)

O devido processo legal é a segurança dos litigantes de que o processo será igualitário, ou seja, todas as garantias legais serão obedecidas igualmente pelas partes e que no final do processo um juiz imparcial prolatará uma sentença.

Para MOUGENOT (2019, 84), num Sistema inquisitivo as figuras do acusador e do julgador se confundem, de maneira que um único juiz investiga e julga, exercendo o papel de inquisidor. Nesse Sistema, considerado primitivo, não existe a condição do contraditório, pois ao acusado não é permitido se defender. (NEVES 2019, 5)

Segundo TELLES (2020, 3)¹¹⁶ inquéritos têm largo espectro e são capazes de atingir as liberdades.

Se por um lado existe algum risco para o regime democrático no Brasil que precisa ser combatido, há que se preocupar para que as ações tomadas não violem os direitos individuais já consagrados na CRFB/88. Entre esses direitos, destacam-se os relativos à liberdade de expressão e liberdade de opinião, verdadeiros pilares da democracia.

Num breve comparativo entre Brasil e Portugal, registra-se que a liberdade de expressão e o combate à desinformação (DER.pt 2021, 6) foi objeto da Lei Portuguesa n° 27/2021, denominada Carta Portuguesa de Direitos Humanos na Era Digital - CPDHED, que foi aprovada em 17/05/21.

A Lei 27/2021 teve como objetivo a proteção da sociedade quanto à produção, reprodução ou difusão de narrativas consideradas como desinformação, cumprindo o que determina o Plano Europeu

¹¹⁵ (PLANALTO.gov.br, CRFB/88 1988) art. 129. São funções institucionais do Ministério Público:

III - promover o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos

¹¹⁶ TELLES (2020, 3) Argumenta que: “Por isso, a lei processual penal regulamenta os inquéritos com rigor. O artigo 4º do Código de Processo Penal diz que a polícia judiciária será exercida pelas autoridades policiais no território de suas respectivas circunscrições e terá por fim a apuração das infrações penais e da sua autoria. [...] Também o Código de Processo Penal diz, no parágrafo 1º do artigo 5º que o requerimento da autoridade do Judiciário ou do MP que requisitar à polícia a instauração do inquérito descreverá, sempre que possível: a narração do fato, com todas as circunstâncias, a individualização do indiciado ou seus sinais característicos e as razões de convicção ou de presunção de ser ele o autor da infração, ou os motivos de impossibilidade de o fazer.” E complementa: “Inquérito tem que ter objeto específico; [...]”

de Ação contra a Desinformação. (EC.EUROPA 2018, 1)¹¹⁷

Ao contrário do PL 2.630/20, atualmente em trâmite na Câmara dos Deputados no Brasil, no qual o Senado Federal suprimiu o termo “desinformação”, adotando, sem definir, o termo “comportamento inautêntico”, a Lei Portuguesa 27/2021 definiu objetivamente o que é “desinformação”¹¹⁸. (DRE.pt 2021, 6)

Referida Lei enfatiza a necessidade de comprovação da falsidade ou enganação da narrativa, cujo objetivo tenha sido obter vantagens econômicas ou deliberadamente enganar, desde que suscetível de causar um prejuízo público.

Quanto a prejuízo público, a Lei define como sendo ameaça aos processos políticos democráticos, aos processos de elaboração de políticas públicas e a bens públicos.

A intenção de “deliberadamente enganar” esbarra numa questão subjetiva que não parece fácil de ser comprovada a desinformação, pois existe a possibilidade de se ter cometido apenas um mero erro¹¹⁹ na comunicação. (DRE.pt 2021, 7)

A informação só é considerada comprovadamente falsa ou enganadora para textos ou vídeos que são manipulados ou fabricados, para as práticas que visam a inundar as caixas de correio eletrônico e para o uso de redes de seguidores fictícios. (DRE.pt 2021, 7)

Conforme artigo 3º, 2-j da Lei 27/2021, cabe ao Estado assegurar um ambiente digital e defender os direitos humanos, definindo medidas de combate à disponibilização ilícita e divulgação de conteúdos ilegais em rede. (DRE.pt 2021, 6)

Tal qual o artigo 4º, item 2 do PL 2.630/20, em Portugal o artigo 4º da CPDHED garante a todos o direito de exprimir e divulgar o pensamento, sem qualquer tipo ou forma de censura, exceto quando se tratar de conduta ilícita. (DRE.pt 2021, 6)

Comparando o PL 2.630/20 com a Lei 27/2021, diferentemente de Portugal, fica claro que no Brasil a maior preocupação não é com a desinformação. O PL dá foco na utilização de contas falsas, de contas não identificadas e de conteúdos impulsionados e publicitários. E sustenta que defende a liberdade de expressão e impede a censura no ambiente online.

¹¹⁷ (EC.EUROPA 2018, 1) A Alta Representante/Vice-Presidente Federica Mogherini declarou: «A saúde da democracia depende da existência de um debate público aberto, livre e equitativo. Cumpre-nos proteger esse espaço, impedindo a disseminação de desinformação suscetível de alimentar o ódio, as divisões e a desconfiança em relação à democracia. Decidimos, enquanto União Europeia, agir em conjunto a fim de reforçarmos a nossa resposta, promovermos os nossos princípios e apoiarmos a resiliência das nossas sociedades, tanto dentro das nossas fronteiras como nos países vizinhos. É essa a resposta da Europa a um dos principais desafios do nosso tempo».

¹¹⁸ (DRE.pt 2021, 6) Artigo 6º, nº 2 - Considera-se desinformação toda a narrativa comprovadamente falsa ou enganadora criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que seja suscetível de causar um prejuízo público, nomeadamente ameaça aos processos políticos democráticos, aos processos de elaboração de políticas públicas e a bens públicos.

¹¹⁹ (DRE.pt 2021, 7) Artigo 6º, nº 4 – Não estão abrangidos pelo disposto no presente artigo os meros erros na comunicação de informações, bem como as sátiras ou paródias.

Podem ser considerados convergentes, enquanto definições, os termos “rede de distribuição artificial de conteúdo”¹²⁰ comparado a “inundar as caixas de correio eletrônico” e “comportamento inautêntico”¹²¹ comparado com “uso de redes de seguidores fictícios”, ambos abordados tanto no Brasil quanto em Portugal. (CÂMARA DOS DEPUTADOS, PL 2.630/20 2020, 2)

Nessa seara, fica evidente a constante preocupação tanto no Brasil, quanto em Portugal, como também na maior parte dos países, em combater *fake news*, preservando, nos regimes democráticos, o direito às liberdades individuais.

No Brasil, em 27/08/21, o STF através da Resolução 742, instituiu o PCD – Programa de Combate à desinformação no âmbito do Supremo Tribunal Federal, tendo em vista as inúmeras críticas e os ataques sofridos nas redes sociais.

A finalidade é enfrentar os efeitos negativos provocados pela desinformação e pelas narrativas odiosas à imagem e à credibilidade da Instituição, de seus membros e do Poder Judiciário. O objetivo é, a partir de estratégias proporcionais e democráticas, manter a proteção da Corte acerca das liberdades de comunicação. (STF, PCD 2021)

Registra-se que o PL 2.630/20, em seu artigo 4º-I, estabelece como objetivo a busca por maior transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais, com garantia do contraditório e da ampla defesa.

Na prática, não se trata de quais instrumentos de informática estão sendo usados no combate a *fake news*, mas da forma como os provedores estão fazendo uso do resultado das suas análises aplicadas às mensagens que veiculam nas redes sociais.

O Marco Civil da Internet se fundamenta no respeito à liberdade de expressão, sendo este um princípio garantidor, com objetivo de promover o direito ao acesso de todos à internet, bem como de inovar e de fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso.

Nesse sentido, em que pesem os avanços tecnológicos, há que se respeitar o direito a liberdade de expressão. Para tanto, iniciativas dos provedores no intuito de combater *fake news* não devem causar censura prévia, bloqueando ou excluindo mensagens contendo informações consideradas falsas em suas análises.

É notória a grande contribuição que os provedores das redes sociais e de serviços de mensageria

¹²⁰ (CÂMARA DOS DEPUTADOS, PL 2.630/20 2020, 2) comportamento coordenado e articulado por intermédio de contas automatizadas ou por tecnologia não fornecida ou autorizada pelo provedor de aplicação de internet, ressalvadas as que utilizam interface de programação de aplicações, com o fim de impactar de forma artificial a distribuição de conteúdos.

¹²¹ (CÂMARA DOS DEPUTADOS, PL 2.630/20 2020, 2) conta inautêntica criada ou usada com o propósito de assumir ou simular identidade de terceiros para enganar o público, ressalvados o direito ao uso de nome social e à pseudonímia nos termos desta Lei, bem como o explícito ânimo humorístico ou de paródia.

privada têm dado no sentido de coibir a disseminação de notícias falsas. Para tanto têm se valido do uso de algoritmos para identificação de mensagens com conteúdos de *fake news* através de palavras-chave como “COVID-19”, “coronavírus” etc.

Não obstante, é questionável a proporcionalidade do uso de algoritmos nas ações tomadas pelos provedores, tendo em vista que, ao definirem uma mensagem como *fake news*, têm rejeitado a mensagem, reduzido seu alcance ou até mesmo bloqueado a conta do usuário.

Ações como essas, sem o devido esclarecimento ao usuário do porque da ação, geram censura prévia, que contraria um dos principais objetivos do PL-2.630/20, que é a liberdade de expressão, direito fundamental garantido pela nossa Constituição.

É fato que o uso de algoritmos tem um potencial tecnológico enorme, porém como não são transparentes para os usuários podem, silenciosamente, causar efeitos extremamente adversos, violando principalmente o direito de liberdade de expressão.

Uma ação que tem sido liminarmente aplicada pelos provedores é a exclusão de contas inautênticas ou contas automatizadas não autorizadas. Ações como essas não têm amparo jurídico, ainda que previstas no termo de uso das plataformas das redes sociais.

Para assuntos específicos como, por exemplo, COVID-19, os provedores de redes sociais têm se valido de algoritmos no uso de aprendizado de máquina (*deep learning*) e inteligência artificial a fim de triar e classificar as mensagens, visando à identificação de conteúdos com *fake news* ao compará-los com informações oficiais.

Os provedores das redes sociais, uma vez identificado esse tipo de conteúdo, disponibilizam mensagem de alerta ao leitor sobre a existência de plataforma fidedigna com informações exclusivas de COVID-19. Dessa forma, eles não restringem a liberdade de expressão, mas se resguardam quanto à possibilidade de uma imagem negativa das suas redes de comunicação.

O uso de algoritmos tem contribuído para identificar mensagens cujos conteúdos apresentam temas considerados pelos provedores como merecedores de melhor atenção quanto à veracidade.

É fato, que devido à enorme quantidade de mensagens veiculadas nas redes sociais, os provedores têm buscado auxílio das agências checadoras de fatos para identificar quais as mensagens que deverão merecer tratamento diferenciado, a fim de tentar evitar a disseminação de *fake news*.

Mas, essa ação tem sido objeto de preocupação dos usuários, porquanto não são informados sobre quais os algoritmos são utilizados e acaba ocorrendo por vezes interpretações equivocadas por parte dos provedores, prejudicando o direito de defesa do usuário.

Algumas dessas interpretações equivocadas por parte dos provedores quanto à veracidade das

informações têm levado a exclusão da mensagem ou bloqueio do uso da conta pelo usuário, resultando em constrangimento e cerceamento da liberdade de expressão do usuário. Essa ação aparenta ser uma censura prévia e não coaduna com a democracia.

Especificamente em relação aos algoritmos, o uso de forma indiscriminada tem levado a uma censura prévia que, pela falta de transparência dos provedores na definição das políticas de uso, acaba prejudicando o usuário, ao sofrer injustas punições.

O Instagram expandiu seu programa de checagem de fatos para as publicações que considera *fake news*, capturadas através do aprendizado de máquina. Aos verificadores de notícias cabe fazer uma filtragem na aba Explorar e na pesquisa por *hashtags*, exibindo um aviso de que o conteúdo é falso. Com esse procedimento a visibilidade no *feed* e no *stories* é reduzida, ficando mais difícil para o usuário o acesso ao conteúdo falso.

Ao deparar com uma notícia considerada falsa, o usuário visualizará uma tela de aviso para que decida se quer continuar a ler, confiar ou compartilhar o conteúdo. Neste caso, o Instagram utilizará o aprendizado de máquina para capturar as *fake news* e aplicar a tela de aviso.

Todos os usuários que encontram o post, seja no feed, no perfil, nos stories ou em mensagens do direct, recebem esse aviso. Também, um link externo é disponibilizado contendo informações de fontes confiáveis para que o usuário possa consultar.

Fica por conta do usuário a decisão de acessar Entenda, para visualizar porquê a publicação foi identificada como falsa e/ou de acessar Ver publicação, para visualizar a mensagem. Dessa forma, não é violado o direito de acesso à informação, nem a liberdade de expressão de quem originou a mensagem.

A plataforma WhatsApp tem contribuído com medidas de auxílio no combate às *fake news*. Pode-se citar: o limite de mensagens encaminhadas, reduzido para apenas cinco contatos ou grupos; a remoção de contas identificadas pela inteligência artificial como sendo spam.

Atualmente, a contribuição dos instrumentos informáticos (AL, ML, AI) utilizados na identificação de notícias consideradas falsas tem se mostrado eficiente quando, em suas análises, comparam as mensagens com informações oficiais disponibilizadas nos meios de comunicação.

Na esteira das inovações tecnológicas, a Finlândia, referência mundial em educação, lançou em 2014 uma ferramenta denominada FactBar (*Faktabaar*) buscando preparar os seus cidadãos para um cenário digital cada vez mais complexo. O Factbar vem ajudando as pessoas na identificação de notícias falsas. (SALO, 2015)

Trata-se de um serviço de verificação de fatos, que retorna com precisão o resultado de uma

pesquisa, em especial para os debates eleitorais públicos. Usa redes sociais para coletar e distribuir informações factuais para as multidões, através de checagens pedagógicas e blogs sobre distúrbios de informação na plataforma de publicação de segurança cibernética.

O Instituto de Pesquisa em Computação do Catar (QCRI) desenvolveu uma ferramenta para incentivar a alfabetização digital dos seus cidadãos e o consumo de notícias verdadeiras. Conhecida como Tanbih, reúne artigos conforme os acontecimentos, inserindo informações adicionais sobre as fontes. Com essas informações, a plataforma gera perfis dos meios de comunicação, sua ideologia política, reputação e histórico. (BRAVO, 2019)

Em 2019, a União Europeia divulgou a criação do “Guia Ético por uma Inteligência Artificial Confiável” (*Ethics Guidelines For Trustworthy AI*) cujo objetivo é ajudar os Estados-membros a criar sistemas autônomos “de confiança” sem reproduzir discriminações, assegurando a autonomia humana.

No Brasil, o STF está investindo recursos para dar origem a um laboratório de inovações tecnológicas no Poder Judiciário, com a criação do PCD – Programa de Combate à desinformação no âmbito do Supremo Tribunal Federal.

Em razão das inúmeras críticas veiculadas nas redes sociais, o PCD pretende enfrentar os efeitos negativos provocados pela desinformação e pelas narrativas odiosas à imagem e à credibilidade da Instituição. Utilizará de estratégias proporcionais e democráticas para manter a proteção da Corte acerca das liberdades de comunicação.

É fato que os algoritmos são essenciais para identificar mensagens que contêm um determinado assunto pesquisado, mas para saber se o conteúdo é uma informação ou uma desinformação, é preciso ir além e analisar o contexto.

Segundo NOVAIS et al (2018, 1)¹²², as análises poderiam apresentar resultados mais precisos se também fossem considerados, além das palavras escritas, os aspectos não verbais nas mensagens a fim de identificar o perfil emocional do autor.

Neste caso, o aprendizado de máquina, através do uso constante de novas estratégias de mineração e modelos de detecção de emoções em textos, poderia contribuir para apontar se o autor da mensagem teve a intenção de disseminar *fake news*. (NOVAIS et al, 2018, 1)

Em que pese o inevitável avanço tecnológico na criação de novos instrumentos de combate a *fake news*, a questão se concentra na preocupação com o uso indevido das análises por parte dos provedores, em incontestável desrespeito ao direito da liberdade de expressão dos usuários.

¹²² NOVAIS et al (2018, 1). O métodos de detecção lexical tendem a ter baixa precisão porque classificam todas as mensagens contendo termos específicos, sem abordar aspectos emocionais.(interpretação nossa)

V – CONSIDERAÇÕES FINAIS

O presente estudo se desenvolveu sob a ótica da INFORMÁTICA e do DIREITO, com a finalidade de analisar a necessidade de tipificação de um crime especial de responsabilidade e das medidas de combate propostas no PL 2.630/20 (Lei Brasileira da Liberdade, Responsabilidade e Transparência).

A análise compreendeu o período em que o referido Projeto de Lei tramitava na CÂMARA DOS DEPUTADOS, desde o dia de recebimento do texto original provindo do SENADO FEDERAL até a presente data, isto porque continua sendo discutido naquela Casa Legislativa.

Estamos vivendo na era da informação, na qual ocorre um uso sem precedentes de comunicações digitais, com uma imensa quantidade de informações, notícias e troca de mensagens.

Em meio a essas comunicações encontram-se mensagens com informações e/ou notícias que muitas vezes não traduzem a verdade dos fatos, consideradas *fake news*.

Essas *fake news* têm gerado grande preocupação mundial, uma vez que a comunicação digital tem seu acesso cada vez mais facilitado e mais amplo em razão das novas tecnologias.

Em que pese os avanços tecnológicos terem possibilitado aos internautas o exercício da liberdade de expressão e de pensamento, o baixo nível de confiabilidade das informações/notícias o tem dificultado de filtrar tempestivamente as mensagens disseminadas nas redes sociais. Essa dificuldade é consequência do enorme volume e da rapidez na troca das mensagens.

Os provedores, que até então permitiam o livre fluxo de informações, passaram a desenvolver e utilizar mecanismos de checagem dos fatos, confrontando as informações com fontes oficiais, dado o alto nível de preocupação com a perda de credibilidade da sua plataforma.

Dessa forma, os provedores começaram a se valer também de parceiros, como foi o caso das agências checadoras de fatos, que fornecem resultados das suas análises relativamente à veracidade das notícias.

Tanto no Brasil como em Portugal, essas agências checadoras de fatos têm sido parceiras importantes na análise desenvolvida pelos provedores das redes sociais. Entretanto, não podem perder de vista a questão de combater as *fake news* sem violar a liberdade de expressão dos usuários.

Na Informática, muito se tem falado no uso de algoritmos para identificar mensagens com notícias falsas. Entretanto, o uso abusivo desses algoritmos na forma de censura prévia tem preocupado os usuários, por violar o direito constitucional de liberdade de expressão.

Nessa seara, o ordenamento jurídico deveria estabelecer limites para os provedores de redes sociais na aplicação de algoritmos no combater as *fake news*, de forma a preservar a liberdade de expressão.

Diversas vezes o uso de uma determinada palavra, definida pelo algoritmo, acaba levando o usuário a ser temporariamente bloqueado na plataforma ou até mesmo excluído.

Daí o grande desafio das TIC para garantir confiabilidade e integridade aos sistemas informacionais no combate às *fake news*, sem, no entanto, violar o direito da liberdade de expressão e opinião.

Mas para tanto, segundo proposto no PL 2.630/20, os provedores deveriam adotar maior transparência nas práticas de moderação de conteúdos postados nas redes sociais, de forma a não gerar censura prévia.

É fato que algumas das ações que os provedores estão aplicando para combater as *fake news*, são objeto de proposições constantes no PL 2.630/20, mas como já dito, referido Projeto ainda está tramitando na CÂMARA DOS DEPUTADOS.

O fator preocupante é que, embora a Informática tenha instrumentos (AL, ML, AI) capazes de identificar mensagens contendo *fake news*, as "punições" que têm sido aplicadas ao "pseudo infrator" muitas vezes não se justificam.

Referidas punições, resultantes de pré-julgamentos na forma de censura, ainda que posteriormente venham a ser desconsideradas, fazem com que o usuário sofra retaliações e tenha sua reputação comprometida.

As iniciativas que têm sido adotadas pelos provedores das redes sociais na tentativa de não deixar a credibilidade minar, por mais que pareçam bem intencionadas, têm levado os usuários a temer pela sua liberdade de expressão, haja vista que suas mensagens passam por intenso crivo quanto à veracidade, inclusive com a ajuda de agências checadoras de fatos, que atuam junto aos provedores.

Nessa seara, têm sido frequentes as limitações impostas nas políticas de uso pelos provedores de redes sociais, diante das mensagens produzidas pelos usuários em flagrante uso da sua liberdade de expressão e de opinião, frutos da materialização da sua liberdade de pensamento.

É inaceitável o uso do poder único do provedor para decidir sobre a veiculação ou não de uma mensagem que considerou ser *fake news*, punindo o usuário por divulgar conteúdo muitas vezes simplesmente crítico, produto da materialização do pensamento, porquanto usando do seu direito à liberdade de expressão.

Essa punição, incidente sobre a liberdade de expressão objetivando reduzir ou eliminar *fake news*, à medida que vai sendo aplicada, vai mitigando a liberdade de pensamento, que abarca a liberdade de expressão e a liberdade de opinião.

É evidente que a dificuldade em se conceituar objetivamente *fake news* impede a aplicação isenta da legislação por parte de quem analisa. Este fato influencia na subjetividade e na discricionariedade

quando da análise de uma notícia.

Nessa seara é necessário dizer o Direito, através do PL 2.630/20, para que sejam definidas as competências dos provedores no tratamento de mensagens veiculadas nas redes sociais e nas mensagerias privadas para coibir *fake news*, ressaltando a importância de proteger a liberdade de expressão e o acesso à informação.

É sabido que o Direito não consegue ser tempestivo na aplicação de normas sobre fatos novos e obviamente não se justifica a criação de normas sobre fatos ainda não existentes.

Considerando-se os avanços tecnológicos, a ação do Direito torna-se ainda mais desafiadora quanto à tempestividade, visto que o ritmo acelerado na evolução da informática afeta de forma globalizada diretamente a vida cotidiana dos cidadãos. Além do que as normatizações devem ser eficazes, porém comedidas, haja vista o cuidado para que não venham a tolher o próprio desenvolvimento tecnológico.

No Brasil, toda essa problemática se acentua em razão da paralisação do PL 2.630/20. E, enquanto não há uma legislação específica definindo as regras de combate às *fake news*, diversos atores se projetam no cenário de combate às notícias falsas, como é o caso dos provedores e do Judiciário.

Nesse sentido, é premente a necessidade de dar continuidade à discussão do PL 2.630/20 para que, se aprovado, se transforme em Lei e sirva de norte a fim de evitar lesão maior aos direitos individuais conquistados e definidos na CRFB/88, principalmente à liberdade de expressão.

Algumas das medidas de combate às *fake news* propostas no Projeto de Lei 2.630/20 já foram implantadas pelos provedores, antes mesmo da aprovação do PL. Entretanto, por falta dessa aprovação, medidas como exclusão de mensagens e bloqueio de contas não têm uniformidade de procedimento e nem proporcionalidade quanto à aplicação, apresentando-se muitas vezes exageradas.

Parte da proposta do PL exige que os provedores adotem, entre outras, medidas para vedar o funcionamento de contas inautênticas e de contas automatizadas não identificadas, bem como para identificar conteúdos impulsionados e publicitários realizados através de pagamento pelo serviço.

Quanto a essas exigências, os provedores de redes sociais, por iniciativa própria, já implantaram eficientemente ações nesse sentido, utilizando tecnologias (ML, AI) de forma menos abusiva. Ao que tudo indica não terão dificuldade para cumprir as normas, se o PL vier a se transformar em Lei e forem mantidas as referidas exigências.

O PL estabelece não haver restrição quando se tratar de manifestação artística, intelectual ou de conteúdo satírico, religioso, político, ficcional ou literário, ou de qualquer outra forma de manifestação cultural, nos termos da Constituição Brasileira.

Nessa seara, embora o PL ainda esteja em discussão, os provedores têm agido de forma diversa no sentido de vedar algumas dessas manifestações. Essas ações contrapõem o previsto no projeto, de que eles devam garantir segurança e ampla liberdade de expressão, comunicação e manifestação do pensamento.

O PL determina que os provedores devam estabelecer políticas de uso buscando maior transparência nas práticas de moderação de conteúdos postados por terceiros, de modo a garantir o contraditório e a ampla defesa, condição não existente na atualidade.

Relativamente a essa determinação, os provedores de redes sociais têm realizado sucessivas alterações nas políticas de uso, com intuito de dar maior transparência às suas práticas de moderação. Entretanto, não oportunizam a garantia do contraditório e da ampla defesa aos usuários, quando estes são rotulados como disseminadores de *fake news*.

Penso que a legislação brasileira deva estabelecer regras e limites para os provedores quando do tratamento das mensagens veiculadas nas plataformas de redes sociais. O objetivo é que a análise seja realizada com mais critério, não se restringindo a interpretação seca das palavras definidas pelo algoritmo e que sempre seja respeitado o direito de liberdade de expressão do usuário.

E para obtenção de resultados mais criteriosos, as análises poderiam se valer de estratégias de mineração e modelos de detecção de emoções em textos, com foco nos aspectos não verbais das mensagens, a fim de identificar o perfil emocional do autor e detectar se naquele determinado contexto há ou não uma intenção em disseminar *fake news*.

A intenção é evitar que o usuário seja “de pronto” rotulado como disseminador de *fake news* e sofra injustas consequências, sem que pelo menos tenha sido advertido e lhe dado o direito de defesa. O descumprimento dessa condição deveria ser fator de culpabilidade por parte dos provedores de redes sociais, sujeitando-os a punições.

Por fim entendo que, embora as medidas de combate às *fake news* propostas no PL com intuito de proteger a liberdade de expressão e o acesso à informação, atendam aos objetivos e princípios definidos no PL, esse assunto deveria ser objeto de debate na CCTCI em conjunto com profissionais da área tecnológica.

Quanto à questão de tipificação de um novo crime, como resultado da análise realizada, entendo que não se justifica enquadrar como “crime de responsabilidade”. Isto porque que este somente se aplica a infrações político-administrativas, já definidas na CRFB, cometidas por servidores públicos no exercício da função.

Entendo também não se enquadrar como “crime especial” porque a ação aponta para um tipo de

“crime comum”, uma vez que a disseminação de *fake news* que impacta individualmente a honra de outrem já está consagrada no Código Penal.

Mas, por outro lado, a disseminação de *fake news* nas redes sociais pode afetar de forma coletiva a honorabilidade das Instituições democráticas.

Nessa seara, entendo que é necessário tipificar um novo “crime comum”, a ser incluído no Código Penal, como uma espécie de crime contra o Estado Democrático de Direito.

Finalizo enfatizando que, embora um dos objetivos do Projeto de Lei 2.630/20, ainda em tramitação na Câmara dos Deputados Brasileira, seja o fortalecimento do processo democrático por meio do combate ao “comportamento inautêntico”, o referido Projeto não apresenta essa definição.

A indefinição desse objetivo torna arriscadamente subjetiva e genérica a sua interpretação visando à aplicação das medidas de combate, para muito além da questão de disseminação de *fake news* nas redes sociais digitais. Tal situação aponta para uma longa e tortuosa trajetória rumo a uma legislação que atenda aos interesses da sociedade brasileira.

REFERÊNCIAS BIBLIOGRÁFICAS

- ADINOLF, Goffredo 2016. *RELAÇÕES INTERNACIONAIS: O Movimento 5 Estrelas e a lei férrea da oligarquia*. http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri50/RI50_06GAdinolfi.pdf p.3 acessado em 21/02/21
- AGÊNCIA BRASIL. 2018. *Redes sociais adotam medidas para combater fake news nas eleições*. <https://agenciabrasil.ebc.com.br/politica/noticia/2018-07/redes-sociais-adotam-medidas-para-combater-fake-news-nas-eleicoes> acessado em 21/12/20
- ALEXY, Robert. 2008. *Teoria dos direitos fundamentais*. Trad Virgílio Afonso da Silva. São Paulo: Malheiros p.116-118
- ALMEIDA, José Maria Fernandes. 2005. Breve história da INTERNET. Universidade do Minho. Departamento de Sistemas de Informação (DSI). <http://hdl.handle.net/1822/3396> acessado em 12/12/20
- ALPERIN, Brown, HUANG, & SHASTRI, 2001. BOLT, BERANEK, AND NEWMAN INC. *A CASE HISTORY OF TRANSITION: THE STRUCTURE OF ENGINEERING REVOLUTIONS* <http://web.mit.edu/6.933/www/Fall2001/BBN.pdf> acessado em 20/12/20
- ALVES, Lauren Julié Liria Fernandes Teixeira 2019. *RESPONSABILIDADES DOS INFLUENCERS DIGITAIS: A internet não é uma "terra sem lei"*. <https://jus.com.br/artigos/76566/responsabilidades-dos-influencers-digitais> p.1 acessado em 24/02/21
- AOS FATOS 2021. *FactMa*. <https://www.aosfatos.org/fatima/> p.1 acessado em 10/01/21
- BISHOP, Christopher M. 2006. *Pattern Recognition and Machine Learning*. Springer Verlag, 17 de agosto de 2006
- BHATT, D.V., SHULZE, S., HANCKE, G.P. 2006. IEEE. *Secure Internet access to gateway using secure socket layer*. <https://ieeexplore.ieee.org/abstract/document/1634869> acessado em 20/12/20
- BOOKS GOOGLE. 2018 Blommsbury Sigma. David Sumpter. OUTNUMBERED. https://books.google.com.br/books?hl=pt-BR&lr=&id=8bJTDwAAQBAJ&oi=FakeNews&pg=PT7&dq=%22FACEBOOK%22+AND+%22LINK%22+AND+%22IDENTIFY%22+AND+%22FAKE+NEWS%22&ots=NUU2os4wvD&sig=EgiYSNyttYL2C-RgJcRakJlxJZw&redir_esc=y#v=onepage&q=%22FACEBOOK%22%20AND%20%22LINK%22%20AND%20%22IDENTIFY%22%20AND%20%22FAKE%20NEWS%22&f=false acessado em 22/02/21
- BRAVO, Luiza. 2019. *Whow – Empreendedorismo para a vida real - Como a tecnologia está ajudando a combater as fake News* <https://www.whow.com.br/tecnologia/como-tecnologia-esta-ajudando-combater-fake-news/> acessado em 23/11/21
- CAMBRIDGE, Dictionary. s.d. *Algorithms*. <https://dictionary.cambridge.org/es/diccionario/ingles/algorithm> acessado em 15/12/20
- CAMBRIDGE Dictionary s.d. *Artificial intelligence* <https://dictionary.cambridge.org/es/diccionario/ingles/artificial-intelligence> acessado em 19/12/20
- CAMPOS, Luciana Conceição Dias. 2017. UFJF. *VISÃO GERAL SOBRE INTELIGÊNCIA ARTIFICIAL*. <https://www2.uff.br/poseconomia//files/2017/09/Apresentac%cc%a7a%cc%83oIA.pdf> p.46 acessado em 31/12/20
- CANALTECH. 2018. Wagner Wakka. *Google lança iniciativa para combater fake News e mau jornalismo*.

<https://canaltech.com.br/internet/google-lanca-indicativa-para-combater-fake-news-e-mau-jornalismo-110288/> p.1 acessado em 15/12/20

CANALTECH 2019. *Sem fake News! Instagram expande medidas de combate à desinformação.* <https://canaltech.com.br/redes-sociais/sem-fake-news-instagram-expande-medidas-de-combate-a-desinformacao-158083/> p.1 acessado em 23/02/21

CANOTILHO, José Joaquim Gomes et al. (2014) *Constituição Brasileira de 1988. Reflexões em comemoração ao seu 25º aniversário.* Curitiba: Juruá

CARNIELLI, Walter A. E RICHARD L. Epstein. 2011. *Pensamento crítico: o poder da lógica e da argumentação.* São Paulo, Rideel, p.325

CARVALHO, Luiz et al. 2019. *DESAFIOS DE TRANSPARÊNCIA PELA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.* In: *WORKSHOP DE TRANSPARÊNCIA EM SISTEMAS (WTRANS).* Porto Alegre: Sociedade Brasileira de Computação. p. 21-30

CLAUSSEN, KRETSCHMER e MAYRHOFER 2011. *The effects of rewarding user engagement –The case of Facebook apps.* <https://core.ac.uk/reader/189909470> p.3 acessado em 22/02/21

CLAY, Kimberly C., POLYZOS, George C., BRAUN, Hans-Werner. S.d. University of California. *Traffic Characteristics of the T1 NSFAKE NEWSET Backbone.* <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.30.8357&rep=rep1&type=pdf> acessado em 17/02/21

CORNELL LAW SCHOOL s.d. 47 Código dos EUA § 230 - *Proteção para bloqueio privado e triagem de material ofensivo* <https://vormavtkegncfbbadgcgk6x7gm-adv7ofecxzh2qqi-www-law-cornell-edu.translate.goog/uscode/text/47/230> p.1 acessado em 09/04/21

CUNHA, Thiago Chierici. 2016. FUMEC. *PREDIÇÃO DE LINKS EM REDES SOCIAIS ACADÊMICAS: UMA ANÁLISE DA INFLUÊNCIA DAS CARACTERÍSTICAS DA REDE NA EFICÁCIA DOS ALGORITMOS BASEADOS NA TOPOLOGIA.* <http://www.fumec.br/revistas/sigc/article/view/3699> acessado em 13/12/20

DELOITTE s.d. *O que é Artificial Intelligence?* <https://www2.deloitte.com/pt/pt/hot-topics/artificial-intelligence.html> p.2 acessado em 31/12/20

DEROSA, Cristian. 2018. *FAKE NEWS - Quando os jornais fingem fazer jornalismo.* 1ª ed. Florianópolis: Editora: Estudos Nacionais, p.5

DICIO.com.br. s.d. *Algoritmo.* <https://www.dicio.com.br/algoritmo/> p.1 acessado em 15/12/20

DIZIKES, Peter 2018. Study: *On twitter, false News travels faster than true stories.* <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308> p.6 acessado em 29/04/21

DRAFTNEWS. s.d. <https://firstdraftnews.org/about/> p.1 acessado em 10/01/21

EBC. 2016. Memória EBC. *Como os algoritmos definem o que você vê no Facebook e no Google.* <https://memoria.ebc.com.br/tecnologia/2016/06/como-os-algoritmos-definem-o-que-voce-ve-no-facebook-e-no-google> p.1 acessado em 21/12/20

EMPOLI, Giuliano da. 2019. *Os engenheiros do caos.* tradução Arnaldo Bloch. – 1ª ed. – São Paulo: Vestigio

FILHO, Eduardo Tomasevicius 2016. *MARCO CIVIL DA INTERNET: uma lei sem conteúdo normativo.* <https://doi.org/10.1590/S0103-40142016.00100017> p.5 acessado em 20/05/21

FOLHA.UOL.com.br. 2020. *Combate a fake news requer critérios democraticamente legítimos*. <https://www1.folha.uol.com.br/poder/2020/04/combate-a-fake-news-requer-criterios-democraticamente-legitimos.shtml> acessado em 15/12/20

FORBES 2019. *Instagram lança ferramenta para denúncia de informação falsa*. <https://forbes.com.br/colunas/2019/08/instagram-lanca-ferramenta-para-denuncia-de-informacao-falsa/> p.1 acessado em 23/02/21

FRANÇA, Rubens Limongi. 1996. *Instituições de Direito Civil*. 4ª ed. São Paulo: Saraiva p. 939-940

G1.GLOBO 2020. *Instagram anuncia ferramentas para evitar informações falsas sobre o coronavírus*. <https://g1.globo.com/economia/tecnologia/noticia/2020/03/24/instagram-anuncia-ferramentas-para-evitar-informacoes-falsas-sobre-o-coronavirus.ghtml> p.2 acessado em 23/02/21

GOOGLE. s.d. News Initiative: *Hands-on Machine Learning: What is Machine Learning?* https://storage.googleapis.com/gweb-news-initiative-training.appspot.com/upload/Hands-on_Machine_Learning.pdf p.16-20 acessado em 16/12/20

GOOGLE . 2020. GOOGLE BLOG BRASIL. *Apoiando iniciativas no combate à desinformação sobre COVID-19* . <https://brasil.googleblog.com/2020/04/combate-desinformacao-covid.html> p.2 acessado em 05/03/2021

GOOGLE. 2020. Support. *O que é um feed ?* <https://support.google.com/adsense/answer/9189559?hl=pt-BR> p.1 acessado em 22/02/21

GOOGLE . 2021. GOOGLE BLOG BRASIL. *Os mitos e fatos sobre como combatemos desinformação*. <https://brasil.googleblog.com/2021/01/os-mitos-e-fatos-sobre-como-combatemos-desinformacao.html> p.2 acessado em 22/02/2021

GRECO, Rogério 2020. Consulta realizada 19/09/20 por e-mail rogerio.greco@terra.com.br via site www.rogeriogreco.com.br

HEGEMAN, John 2020. *Providing People With Additional Context About Content They Share* <https://about.fb.com/news/2020/06/more-context-for-news-articles-and-other-content/> p.1 acessado em 27/03/21

HIGA, Paulo. 2015. TECNOBLOG - *Como entrar na deep web utilizando o Tor*. <https://tecnoblog.net/189897/como-acessar-deep-web-links/> p.1 acessado em 29/06/21

HOTMART 2019. Blog Hotmart: *Como se tornar um digital influencer!*. <https://blog.hotmart.com/pt-br/como-se-tornar-um-digital-influencer/> p.2 acessado em 24/02/21

JR. 2019. FOLHA UOL. *Toffoli abre inquérito para apurar fake news e ameaças contra ministros do STF*. <https://www1.folha.uol.com.br/poder/2019/03/toffoli-abre-inquerito-para-apurar-fake-news-e-ameacas-contra-ministros-do-stf.shtml> acessado em 30/08/21

JUNIOR, Gilberto Gomes Reis. SANTOS, Fabiola Martins dos. 2018. *AS PLATAFORMAS DIGITAIS, OPINIÃO DE USUÁRIOS E O RANQUEAMENTO DOS MEIOS DE HOSPEDAGEM COMO FATORES DE DECISÃO NA ESCOLHA DOS CLIENTES DA HOTELARIA*. <https://repositorio.ifsc.edu.br/bitstream/handle/123456789/944/Gilberto%20Gomes%20Reis%20Junior%20TC%202018.pdf?sequence=1&isAllowed=y> p.1 acessado em 04/03/21

JURNO, A. C.; D'ANDREA, C. F. (2017, 463-484) DE B. *“(In)visibilidade algorítmica no ‘feed de notícias’ do*

Facebook". Contemporânea-Revista de Comunicação e Cultura. V. 15. n°2 p.463-484

KLEINROCK, Leonard. 2010. HISTORY OF COMMUNICATIONS: *An Early History Of The Internet*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5534584> acessado em 27/12/20

KLONICK, Kate 2018. HARVARDLAWREVIEW. *THE NEW GOVERNORS: THE PEOPLE, RULES, AND PROCESSES GOVERNING ONLINE SPEECH*. https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf p.1620. acessado em 29/04/21

LAURENTIIS & THOMAZINI 2020. Revista Direitos e Praxis. *Liberdade de Expressão: Teorias, Fundamentos e Análises de Casos*. <https://www.scielo.br/j/rdp/a/XjtMWwY7WnnnvZg4Q7mgX3G/?format=pdf&lang=pt> p.2266 acessado em 22/03/21

LEINER, Barry M. at all. 1997. Brief history of the internet. <https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet> acessado em 25/12/20

MANZANO, J. A.; OLIVEIRA, J. 2005. Algoritmos: Lógica para desenvolvimento de programação de computadores. https://www.mendeley.com/catalogue/fc128292-05b8-3174-a0ee-fd3b2c1ba75a/?utm_source=desktop&utm_medium=1.19.6&utm_campaign=open_catalog&userDocumentId=%7Be15a78c6-f437-4b24-9c7c-5b1a6e4328ed%7D p.6 acessado em 15/12/20

MARTINI, Mara Rovida. COSTA, Jhenifer Neves. 2019. Revista AlterJor. *Algoritmos no Facebook - como entendê-los e considerá-los na produção de notícias*. <http://www.revistas.usp.br/alterjor/article/view/157853> acessado em 18/12/20

MDH 2018. Ministério da Mulher, da Família e dos Direitos Humanos. *Artigo 19 da DUDH Declaração Universal dos Direitos Humanos de 1948 – Liberdade de Expressão e Opinião*. <https://www.gov.br/mdh/pt-br/assuntos/noticias/2018/novembro/artigo-19deg-todo-ser-humano-tem-direito-a-liberdade-de-expressao-e-opiniao-1> p. 1 acessado em 02/05/21

MICROSOFT 2016. News Microsoft. *A visão da Microsoft sobre inteligência artificial, fundamentada em pesquisas e conversas*. <https://news.microsoft.com/pt-br/a-visao-da-microsoft-sobre-inteligencia-artificial-fundamentada-em-pesquisas-e-conversas/> p.1-2 acessado em 31/12/20

MONTEIRO, Silvana Drumond. FIDENCIO, Marcos Vinicius. 2013. PUC Campinas: As dobras semióticas do ciberespaço: da web visível à invisível. https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-37862013000100004&lng=pt&tlng=pt. p.6 acessado em 29/04/21

MOUGENOT, Edilson. 2019. *Curso de processo penal*. 13ª ed. São Paulo: Saraiva educação

MOWERY & SIMCOE. 2002. ScienceDirect. *Is the Internet a US invention? An economic and technological history of computer networking*. <https://www.sciencedirect.com/science/article/pii/S0048733302000690?pes=vor> acessado em 17/02/21

NEUMAN, W.Russell. 2010. *Media, Technology, and Society: Theories of Media Evolution*. <https://www.fulcrum.org/concern/monographs/ms35tb771> acessado em 20/12/20

NEVES, Gioto Motta Tribuzi. 2019. *I(LEGALIDADE) DO INQUÉRITO 4781/STF: INQUÉRITO DAS FAKE NEWS*. <https://www.metzger.com/projects/ilegalidade-do-inquerito-4781stf-inquerito-das-fake-news-5f634eebb32829001891334a> p.5 acessado em 30/08/21

NOFERESTI, Samira. SHAH-HOSSEINI, Hamed 2012. Researchgate. *A Hybrid Algorithm for Solving Steiner Tree*

Problem

<https://www.researchgate.net/publication/235789008> A Hybrid Algorithm for Solving Steiner Tree Problem acessado em 18/12/20

NOVAIS, Paulo et al. 2014. *Establishing the Relationship between Personality Traits and Stress in an Intelligent Environment*. <http://repositorium.sdum.uminho.pt/handle/1822/34180> p.1 acessado em 16/03/21

NOVAIS, Paulo et al. 2016. *Intelligent Distributed Computing IX – Proceedings of the 9th International Symposium on Intelligent Distributed Computing – IDC'2015*, Guimarães, Portugal, October. Editora Springer, 2016. p.257-258

NOVAIS, Paulo et al. 2018. *Hate speech classification in social media using emotional analysis*. 2018 7th Brazilian Conference on Intelligent Systems (BRACIS), 61-66. https://scholar.google.com.br/citations?user=D_NLlcAAAAJ&hl=pt-BR p.1 acessado em 29/03/21

NOVAIS, Paulo et al. 2020. *Predicting an election's outcome using sentiment analysis* <https://repositorium.sdum.uminho.pt/bitstream/1822/69230/1/WorldCist2020-pre-print.pdf> p.6 acessado em 05/05/2021

ORUMIE, Ukamaka Cynthia, EBONG, Daniel. 2014. Scientific Research. *A Glorious Literature on Linear Goal Programming Algorithms*. https://www.scirp.org/html/2-1040278_44149.htm acessado em 18/12/20

PESSOA, Flávia Moreira Guimarães. FILHO, Rodolfo Pamplona. 2017. *COMPARTILHAMENTO DE INFORMAÇÕES PELO WHATSAPP E FACEBOOK: A PROIBIÇÃO DO COMISSARIADO DE HAMBURGO E A CONCRETIZAÇÃO DO DIREITO A PRIVACIDADE DO USUÁRIO NO BRASIL PELO MARCO CIVIL DA INTERNET INFORMATION SHARING BY WHATSAPP AND FACEBOOK: THE BAN OF THE COMMISSIONER OF HAMBURG AND THE CONCRETIZATION OF THE RIGHT TO THE USER'S PRIVACY IN BRAZIL BY THE CIVIL FRAMEWORK OF THE INTERNET*. <http://177.66.14.82/bitstream/riuea/1255/1/Compartilhamento%20de%20informa%C3%A7%C3%B5es%20pelo%20whatsapp%20e%20facebook%20-%2020a%20proibi%C3%A7%C3%A3o%20do%20comissariado%20de%20Hamburgo%20e%20a%20concretiza%C3%A7%C3%A3o%20do%20direito%20a%20privacidade%20do%20usu%C3%A1rio%20No%20Brasil%20pelo%20marco%20civil%20da%20Internet.pdf> p.4-5 acessado em 24/02/21

PORIYE, Monika, UPADHYAYA, Shuchita. 2015. Procedia Computer Science.. *Secure Communication Using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks*. <https://www.sciencedirect.com/science/article/pii/S1877050915032858> acessado em 20/12/20

QUEIROZ, Ruy J.G.B. de 2018. *Fake News, Deep Fakes, e seus efeitos sobre a Democracia*. <https://www.slideshare.net/ruydequeiroz/fake-news-deep-fakes-e-seus-efeitos-sobre-a-democracia> p.6 acessado em 29/04/21

RAPOSO, Miguel 2017. Editorial Presença: *Torna-te um guru das redes sociais*. <https://static.Fake Newsac-static.com/multimedia/PT/pdf/9789898818959.pdf> p.20 acessado em 21/01/21

RIBEIRO, Ronaldo.2010 *Uma Introdução à Inteligência Computacional: fundamentos, ferramentas e aplicações*. 1ª Edição. Rio de Janeiro, Alexander Daltio Vialli, p.8

RICH, Elaine 1998. *Inteligência Artificial*. 1. ed. São Paulo: Mcgraw-hill, p.17

ROSENZWEIG, Roy. 1998. The American Historical Review. *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*. <https://academic.oup.com/ahr/article-abstract/103/5/1530/187277> acessado

em 25/12/20

SALO, Mikko. 2015. FAKTABAARI. <https://faktabaari.fi/in-english/> acessado em 23/11/21

SALLUM, Erick. 2019. JUS.COM.BR - *Investigar, acusar e julgar: por um necessário reequilíbrio de forças* <https://jus.com.br/artigos/72769/investigar-acusar-e-julgar-por-um-necessario-reequilibrio-de-forças> acessado em 29/08/21

SANTOS, V.L.C. e SANTOS J.E. 2014. HOLOS Ano 30, Vol 6 - *AS REDES SOCIAIS DIGITAIS E SUA INFLUÊNCIA NA SOCIEDADE E EDUCAÇÃO CONTEMPORÂNEAS*. <https://redalyc.org/articulo.oa?id=481547175023> acessado em 21/01/21

SEMANTIC SCHOLAR 2008. *An Ethnography of Social Network in Cyberspace: The*. <https://www.semanticscholar.org/paper/An-Ethnography-of-Social-Network-in-Cyberspace%3A-The-Heiman/43e2a0b951c04075eff5f7cb344cc9b76265eded?p2df> p.1 acessado em 05/03/21

SILVA, José Afonso da. 2014. *Comentário Contextual à Constituição*. 9ª ed. São Paulo: Malheiros Editores p.497-498

SUMBALY, Roshan et al. 2019. AI.FACEBOOK.COM *Using AI to detect COVID-19 misinformation and exploitative content* <https://ai.facebook.com/blog/using-ai-to-detect-covid-19-misinformation-and-exploitative-content/> acessado em 04/11/21

TECHTUDO. 2018. *Fake news no Facebook: cinco medidas da rede social para banir boatos* <https://www.techtudo.com.br/listas/2018/10/fake-news-no-facebook-cinco-medidas-da-rede-social-para-banir-boatos.ghtml>

TEIXEIRA, Virginia Melo do Egypto. 2018. *O LIMITE DO DIREITO PENAL NO MUNDO DIGITAL À LUZ DAS FAKE NEWS E DA LIBERDADE DE EXPRESSÃO* <https://repositorio.ufpb.br/jspui/bitstream/123456789/11552/1/VMET15062018.pdf> p.21 acessado em 19/09/20

TELLES, Cássio Lisandro. 2020. OAB-PR. *Artigo: O inquérito do fim do mundo*. <https://www.oabpr.org.br/artigo-o-inquerito-do-fim-do-mundo/> p.3 acessado em 30-08-21

THE VERGE. 2018. By Chaim Gartenberg@cgartenberg Mar 20, 2018, 11:00am EDT *'We need to do more' Google News Initiative announced to fight fake news and support journalism* <https://www.theverge.com/2018/3/20/17142788/google-news-initiative-fake-news-journalist-subscriptions> p.2 acessado em 18/12/20

UNESCO. 2018. UNESCO COURIER. *Inteligência Artificial: entre o mito e a realidade*. <https://pt.unesco.org/courier/2018-3/inteligencia-artificial-o-mito-e-realidade> p.7 acessado em 19/02/21

VENÂNCIO, Pedro Dias. 2013. Tese: *A Tutela Jurídica do Formato de Ficheiro Eletrónico*. <http://repositorium.sdum.uminho.pt/handle/1822/35678> p.89. acessado em 30/12/20

ZANATTA, Rafael 2015. *A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet*. São Paulo: Quartier Latin. p.447

LEGISLAÇÕES

CÂMARA DOS DEPUTADOS 1989. Resolução 17/89. *RICD – Regimento Interno da Câmara dos Deputados*. file:///C:/Users/Public/Documents/_%20EM%20SER%20a%20partir%20de%2020210216/DISSERTA%C3%87%C3%830%20-%20Fase%20FINAL/Refer%C3%Aancias%20DEFINITIVAS%20inclu%C3%ADdas%20no%20trabalho/RICD%20-%20Regimento%20%20Interno%20da%20%20C%C3%A2mara%20dos%20Deputados%20230821.pdf

acessado em 23/08/21

CÂMARA DOS DEPUTADOS 1992. Decreto Lei 27/92 - *CADH – Convenção Americana sobre Direitos Humanos - Pacto São José da Costa Rica*. <https://www2.camara.leg.br/legin/fed/decleg/1992/decretolegislativo-27-26-maio-1992-358314-exposicaodemotivos-143572-pl.html> p.1 acessado em 07/05/21

CÂMARA DOS DEPUTADOS 2020. PROJETO DE LEI 2.630 - *Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983 acessado em 20/05/21

CJF Enunciado 274 2006. CONSELHO DE JUSTIÇA FEDERAL. *IV JORNADA DE DIREITO CIVIL*. <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/IV%20Jornada%20volume%20I.pdf> p.35 acessado em 21/03/21

CJF Enunciado 554 2006. CONSELHO DE JUSTIÇA FEDERAL. *IV JORNADA DE DIREITO CIVIL*. <https://www.cjf.jus.br/enunciados/enunciado/625> acessado em 07/05/21

CJF 2018. CONSELHO DE JUSTIÇA FEDERAL. *VIII JORNADA DE DIREITO CIVIL*. <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/viii-enunciados-publicacao-site-com-justificativa.pdf> p.1 acessado em 21/03/21

CRFB/88 1988. *CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988*. http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm acessado em 20/03/21

DRE.pt 1998. Diário da República. Lei n.º 67/1998 *Lei da Proteção de Dados Pessoais* <https://dre.pt/web/guest/legislacao-consolidada/-/lc/74901117/201704032357/73315962/diplomaPagination/diploma/1> acessado em 30/08/21

DRE.pt 2021. Diário da República. Lei n.º 27/2021 *Carta Portuguesa de Direitos Humanos na Era Digital* <https://dre.pt/application/conteudo/163442504> acessado em 30/08/21

FAKE NEWS CEJB 2007. *FAKE NEWS* – Federação Nacional dos Jornalistas. *CEJB – Código de ética dos jornalistas brasileiros*. https://fenaj.org.br/wp-content/uploads/2014/06/04-codigo_de_etica_dos_jornalistas_brasileiros.pdf acessado em 11/05/21

MDH 2018. Ministério da Mulher, da Família e dos Direitos Humanos. *Artigo 19 da DUDH Declaração Universal dos Direitos Humanos de 1948 – Liberdade de Expressão e Opinião*. <https://www.gov.br/mdh/pt-br/assuntos/noticias/2018/novembro/artigo-19deg-todo-ser-humano-tem-direito-a-liberdade-de-expressao-e-opiniao-1> p. 1 acessado em 02/05/21

PLANALTO.gov.br 1940. Decreto-Lei 2.848/40 *CÓDIGO PENAL BRASILEIRO*. http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm acessado em 25/05/21

PLANALTO.gov.br 1950. Lei 1.079/50. *CRIMES DE RESPONSABILIDADE*. https://www.planalto.gov.br/ccivil_03/leis/l1079.htm acessado em 22/05/21

PLANALTO.gov.br 1953. Lei 2.083/53 *LIBERDADE DE IMPRENSA*.

http://www.planalto.gov.br/ccivil_03/leis/L2083.htm p.3 acessado em 07/05/21

PLANALTO.gov.br. 1988. CRFB/88 - *CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988*.
http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm acessado em 20/03/21

PLANALTO.gov.br 1992. Decreto 678/92. *CADH – Pacto São José da Costa Rica*.
http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm p.1 acessado em 07/05/21

PLANALTO.gov.br 1992. Lei 8.429/92 *Atos de Improbidade Administrativa*.
http://www.planalto.gov.br/ccivil_03/leis/l8429.htm acessado em 20/05/21

PLANALTO.gov.br 1997. Lei 9.504 – *LEI DAS ELEIÇÕES*. http://www.planalto.gov.br/ccivil_03/leis/l9504.htm
acessado em 22/08/21

PLANALTO.gov.br 2002. CCB/02 – *CÓDIGO CIVIL BRASILEIRO*.
http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm acessado em 20/05/21

PLANALTO.gov.br. 2010. Decreto 7.175/10. *Programa Nacional de Banda Larga – PNBL*.
http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7175.htm acessado em 17/02/21

PLANALTO.gov.br 2014. Lei 12.965/14 – *MARCO CIVIL DA INTERNET*.
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm acessado em 21/03/21

PLANALTO.gov.br. 2018. Decreto 9.612/18. *Políticas públicas de telecomunicações.*,
http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9612.htm#art14 artigo 14. acessado
em 17/02/21

PLANALTO.gov.br 2018. Lei 13.709/18. *LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD*.
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
acessado em 22/03/21

SENADO FEDERAL 2003. PLC 89/03 8ª versão proposta pelo Senador Eduardo Azeredo de Alteração no
Código Penal. <https://legis.senado.leg.br/sdleg-getter/documento?dm=4808011&ts=1593940738494&disposition=inline> acessado em 18/08/21

SENADO FEDERAL PL-2.630/20. 2020. PROJETO DE LEI 2.630/20. *Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. <https://legis.senado.leg.br/sdleg-getter/documento?dm=8110634&ts=1612303001672&disposition=inline>
acessado em 07/05/21

JURISPRUDÊNCIAS

CJF Enunciado 274 2006. CONSELHO DE JUSTIÇA FEDERAL. *IV JORNADA DE DIREITO CIVIL*. <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/IV%20Jornada%20volume%20I.pdf> p.35 acessado em 21/03/21

CJF Enunciado 554 2006. CONSELHO DE JUSTIÇA FEDERAL. *IV JORNADA DE DIREITO CIVIL*. <https://www.cjf.jus.br/enunciados/enunciado/625> acessado em 07/05/21

CJF 2018. CONSELHO DE JUSTIÇA FEDERAL. *VIII JORNADA DE DIREITO CIVIL*. <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/viii-enunciados-publicacao-site-com-justificativa.pdf> p.1 acessado em 21/03/21

STF ADI 4451 2019. ADI – Ação Direta de Inconstitucionalidade. *ADI n° 4451*. <https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&queryString=liberdade%20de%20pensamento%20e%20democracia&sort=score&sortBy=desc> p.1 acessado em 29/06/21

STF ADI 5418 2021. ADI – Ação Direta de Inconstitucionalidade. *ADI n° 5418*. https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=ADI%205418&sort=score&sortBy=desc acessado em 20/03/21

STF RCL 22.328 2015. *RCL 22.328 MC/RJ*. <https://luisrobertobarroso.com.br/wp-content/uploads/2015/11/Liberdade-de-expressao-Rcl-22328-1.pdf> p.1 acessado em 29/06/21

STF RE 1193343 2019. RE – *Recurso Especial n° 1193343* <https://stf.jusbrasil.com.br/jurisprudencia/729369299/recurso-extraordinario-re-1193343-se-sergipe> acessado em 20/03/21

STF DJE 2021. Diário da Justiça Eletrônico. Resolução n.º 472 - Programa de Combate à Desinformação no âmbito do Supremo Tribunal Federal <https://sintse.tse.jus.br/documentos/2021/Ago/30/diario-da-justica-eletronico-stf/resolucao-no-742-de-27-de-agosto-de-2021-institui-o-programa-de-combate-a-desinformacao-no-ambito-do> acessado em 31/08/21

TST RR 613. 2205. *TST RR 613/2000-013-10-00, DJ 10.06.2005 1ª Turma Rel. João Oreste Dalazen*. <https://tst.jusbrasil.com.br/jurisprudencia/1724843/recurso-de-revista-rr-613002320005100013-61300-2320005100013/inteiro-teor-10792867?ref=juris-tabs> acessado em 20/05/21