Revista Jurídica vol. 03, nº. 65, Curitiba, 2021. pp. 207 - 226

UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO COMBATE DA PANDEMIA DO COVID-19

USING ARTIFICIAL INTELLIGENCE TO COMBAT THE COVID-19 PANDEMIC

PAOLA CANTARINI GUERRA

Pós-doutora pela EGS/Suíça, pela Universidade de Coimbra, Portugal, CES, pela Faculdade de Direito da USP, e pela PUC-SP-TIDD. Doutora e Mestre em Direito pela PUC-SP. Doutora pela Università del Salento (Itália). Pesquisadora colaboradora da UNICAMP, do IEA/USP, do Instituto Lawgorithmics. *Visiting fellow* do European University Institute, Itália, *Visiting researcher* da Scuola Normale Superiore de Pisa, Itália, e da Universidade de Lisboa, Portugal. ORCID: 0000-0002-9610-8440.

WINFRIED NÖTH

Doutor e livre docente na Universidade de Bochum, Alemanha. Professor convidado das Universidades de Wisconsin, PUC São Paulo e Humboldt de Berlim. ORCID: 0000-0002-2518-9773.

VIVIANE COÊLHO DE SÉLLOS KNOERR

Realizou Estágio Pós-Doutoral pelo Ius Gentium Conimbrigae da Faculdade de Direito da Universidade de Coimbra-Portugal. Doutora e Mestre pela Pontifícia Universidade Católica de São Paulo. Graduada em Direito pela Universidade Federal do Espírito Santo. Professora e Coordenadora do Programa de Mestrado e Doutorado em Direito Empresarial e Cidadania do Centro Universitário Curitiba/UNICURITIBA. Membro da diretoria do CONPEDI, da Sociedade Paranaense de Letras e do Instituto dos Advogados do Paraná. Advogada. E-mail: viviane@sellosknoerr.com.br.

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

RESUMO

Objetivo: A inteligência artificial cada vez mais vem sendo utilizada, produzindo efeitos em todos os setores sociais, surgindo um novo tipo de governança, a governança algorítmica. É essencial evitar na sua utilização o abuso de poder de mercado assim como a concentração de poderes. Com a utilização da inteligência artificial no contexto do combate da pandemia do COVID-19, é importante desenvolver *frameworks* para superar a inefetividade de princípios éticos e jurídicos e a possível ocorrência da lavagem ética. Visa-se analisar as regulamentações da utilização da IA em termos de heterorregulação, de autorregulação e de autorregulação regulada, traçando *frameworks* a partir da análise dos limites jurídicos e éticos da utilização da IA no controle da pandemia do COVID-19.

Metodologia: A metodologia e as técnicas de pesquisa irão conjugar pesquisa teórica no âmbito nacional e internacional, promovendo o diálogo entre os diversos campos do saber, em uma visão interdisciplinar.

Resultados: Resultados a serem destacados são algumas propostas preliminares para soluções para superar as problemáticas pouco exploradas com relação à aplicação da IA no combate à pandemia do COVID-19.

Contribuições: O artigo propõe possíveis soluções e medidas para ultrapassar problemas críticos para os quais, no que diz respeito às estratégias reais de utilização da IA para o controle da pandemia da COVID-19.

Palavras-chave: Inteligência artificial; Pandemia do COVID-19; Lavagem ética. Autorregulação regulada.

ABSTRACT

Objective*: Artificial intelligence is being increasingly used for social purposes. A new type of governance is emerging, the algorithmic governance. The abuse of market power and the rise of monopolies need to be impeded. In the use of artificial intelligence in campaigns against the COVID-19 pandemic, frameworks to overcome the inefficiency of ethical and legal principles need to be developed in order to avoid ethical laundering. The aim of this paper is to analyze existing regulations for the use of AI. Hetero-regulation, regulated self-regulation, and self-regulation are needed and frameworks for the analysis of legal and ethical restrictions in the use of AI must be developed in measures to control the COVID-19 pandemic.*

Methodology*: The methodology and research techniques of this paper combines national and international theoretical research methods promoting the dialogue between the various fields of knowledge in an interdisciplinary perspective.*

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

***Results**: The methodology and research techniques of this paper combines national and international theoretical research methods promoting the dialogue between the various fields of knowledge in an interdisciplinary perspective.*

***Contributions**: The paper proposes possible solutions and measures to overcome critical problems for which regarding the actual strategies of using AI against the COVID-19 pandemic.*

***Keywords**: Artificial intelligence; Pandemic COVID-19; Ethical laundering; Regulated self-regulation.*

1 INTRODUÇÃO

Os problemas tratados na presente pesquisa impõem um diálogo constante entre o Direito, a Filosofia (Ética) e a Tecnologia, já que estamos tratando de temas com características como a da transversalidade, sendo imprescindível a aproximação de campos científicos não jurídicos, resultando numa espécie de equivalente atual do que outrora, ainda há pouco, foi o direito ambiental (CANTARINI, 2020).

Vivemos na denominada fase da sociedade de dados, economia dos dados, governança de algoritmos, ocorrendo a hipertrofia do modelo de “capitalismo de vigilância”, tal como aponta Shoshana Zuboff (2021), também se falando do surgimento de uma nova forma de soberania, a soberania digital, como aponta Byung-Chul Han (2016). É a generalização da sociedade de controle e da nova forma de panóptico, o panóptico digital, prevista antecipadamente por G. Deleuze (1992), em seu “Post-scriptum sobre as sociedades de controle”, seguindo os desenvolvimentos inicialmente traçados por M. Foucault, em seus estudos sobre a sociedade da disciplina, regulamentação e normalização. Surgem novas formas de apartheid, como o apartheid digital, já que milhares de pessoas sequer possuem acesso à internet como bem aponta Paula Sibilia (2020).

Mais do que nunca é urgente a análise dos aspectos éticos, políticos e jurídicos da IA, já que seu uso está aumentando de forma exponencial, tornando-se mais diversificada, e "invisível", ampliando o já conhecido problema das denominadas

"caixas pretas" dos algoritmos de IA, já que esta possui as características da ubiquidade e da opacidade, potencializadas com a internet das coisas e dos serviços, misturando-se ao dia-a-dia de todas as pessoas, sendo um aspecto corriqueiro da vida quotidiana ao se incorporar a diversos objetos e em todos os ambientes.

Vivemos na denominada fase da sociedade de dados, economia dos dados, governança de algoritmos, ocorrendo a hipertrofia do modelo de "capitalismo de vigilância", alterando conceitos tradicionais como os de democracia, cidadania, e soberania, vinculados agora ao atributo da digitalização de nossas personas e vidas. Ocorre uma nova forma de sociedade, a sociedade de controle e uma nova forma de panóptico, o panóptico digital. São as sociedades de controle que substituem as sociedades disciplinares e que surgem com o fundamental suporte das tecnologias eletrônicas e digitais, nesta nova etapa do capitalismo de dados que surge no final do século XX e no início do XXI. Surgem novas formas de controle, agora não mais apenas suaves, mas duras mesmo, relacionadas com as mídias sociais, a partir da primeira década do século XXI, como pode ser observado pela utilização das mídias sociais pelo Departamento de Segurança Interna dos Estados Unidos (DHS) para fins de vigilância "mais dura", sendo criada a "Socmint" (Social Media Intelligence) como um departamento dentro das agências de segurança.

Nas palavras de Deleuze: "'controle' é o nome que Burroughs propõe para designar o novo monstro e que Foucault reconhece como nosso futuro próximo. Paul Virilio também analisa sem parar as formas ultrarrápidas de controle ao ar livre, que substituem as antigas disciplinas que operavam na duração de um sistema fechado" (apud DELEUZE, 1992, p. 2ss.). Virilio continua:

> A empresa introduz o tempo todo uma rivalidade inexpiável como sã emulação, excelente motivação que contrapõe os indivíduos entre si e atravessa cada um, dividindo-o em si mesmo. O princípio modulador do "salário por mérito" tenta a própria Educação nacional: com efeito, assim como a empresa substitui a fábrica, a formação permanente tende a substituir a escola, e o controle contínuo substitui o exame. Este é o meio mais garantido de entregar a escola à empresa (ibid., p. 1-2).

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

Ocorre então a criação de novas formas de vigilância e controle, constituintes de uma governamentalidade (cf. OLIVEIRA, 2019) algorítmica, denominadas de "tecnopolíticas", relacionadas ao *big data*, à prática de mineração de dados e à possibilidade de criação de diversos perfis comportamentais, práticas preditivas, prevendo o comportamento humano, trazendo uma nova configuração de poder, modulando ou manipulando comportamentos humanos para fins econômicos e políticos, sendo um desafio ao Estado Democrático de Direito.

Corrobora tais afirmações o artigo "Cultura da vigilância: envolvimento, exposição e ética na modernidade digital" de David Lyon, no livro *Tecnopolíticas da vigilância*, onde afirma esta nova vigilância de todos sobre todos, dando origem a novos imaginários de vigilância e práticas de vigilância, respectivamente que se entrecruzam. A vigilância torna-se um novo modo de vida, encontra-se internalizado, não sendo apenas institucionalizado, sendo que nos tornamos cúmplices voluntários ao fornecer nas mídias e redes digitais *on line* todas as informações possíveis sobre nossas pessoas. Em suas palavras:

> A cultura da vigilância já se tornava visível na virada do século XXI, especialmente após os ataques do 11 de Setembro nos Estados Unidos e o advento das mídias sociais, e tornou-se ainda mais evidente depois que Snowden copiou e divulgou documentos da NSA em 2013. Os historiadores talvez consigam discernir os primeiros sinais da cultura da vigilância em fins do século XX, mas ela agora está presente em vasta escala e seus contornos estão ficando claros. (LYON, 2018, p. 153)

A nova tecnologia e o acesso às maravilhas da internet e ao mundo digital potencializam e manipulam desejos. Por isso são tão insidiosas em seus efeitos se desejarem manipular comportamentos, pois contam com o aspecto da voluntariedade, as pessoas vinculam-se à rede digital e às nova tecnologias aparentemente de forma livre, apesar de diversas coações que impõem tal comportamento, mas em especial porque estas permitem que sejam satisfeitos desejos os quais no mundo digamos "real" seriam impossíveis de serem satisfeitos. Uma pessoa de baixa renda pode ter um avatar como um importante homem de negócios, uma pessoa com sobrepeso

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

pode construir um avatar de uma modelo ou cantora famosa com uma estética perfeita, etc.

Mais do que nunca é urgente a análise dos aspectos éticos, políticos e jurídicos da tecnologia persuasiva, já que seu uso está aumentando de forma exponencial, tornando-se mais diversificada, e "invisível". Com isso ocorre um maior potencial de intervenção de forma precisa, no momento e local certos, ampliando-se seu poder persuasivo.

Há um maior potencial intrusivo e persuasivo no caso das novas formas de persuasão, em especial com a utilização da IA, do *big data* e do *machine learning*, já que, como regra geral, as técnicas de persuasão são mais eficazes quando são interativas, possibilitando a adequação das tácticas de influência à medida que a situação concreta vai se alterando e evolui, isto é de acordo com o *feedback* obtido em tempo real. É uma forma de personalização possível diferenciando-se nestes aspectos dos meios de comunicação social tradicionais, que utilizavam táticas de manipulação comportamental, já que estes não conseguem trazer um resultado personalizado. A capacidade dos computadores em termos de uma grande análise de dados (mineração) permite mais facilmente adotar uma das técnicas de persuasão, por exemplo, fazer sugestões. Neste sentido, são utilizadas a filtragem colaborativa ou redes bayesianas – métodos automatizados para fazer inferências.

Um exemplo claro de manipulação é o fenômeno denominado de “dataismo”. Dataismo significa que os usurários das redes sociais confiam nas suas plataformas digitais, acreditando serem seguras e desconhecendo o que de fato ocorre nos bastidores. Nisso desconhecem sua posição real, já que são os produtos e não apenas usuários, assim sendo, nada tem de gratuita tal ferramenta, já que não há pagamentos em um primeiro momento. Não consideram que pagamos com todos os dados e perfis comportamentais e com o aspecto de seremos ratos de laboratórios para dezenas de experimentos comportamentais que são realizados, sem nosso conhecimento, sem ética ou transparência. Nas palavras de David Lyon:

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

> Segundo pesquisadores da *Pew Internet and American Life*, as revelações de Snowden de fato tiveram um impacto no uso de mídias sociais. Por exemplo, 34% (ou 30% de todos os adultos) daqueles que estão cientes dos programas de vigilância governamental tomaram pelo menos uma medida para esconder ou proteger suas informações do governo – mudando configurações de privacidade, usando outros meios de comunicação fora das mídias sociais ou evitando certos aplicativos. Uma proporção ligeiramente menor (25%) mudou seu uso de telefones, e-mail ou mecanismos de busca após Snowden. Saber mais sobre vigilância governamental produz mais evidências de modificação de comportamento. (LYON, 2018, p. 159)

2 CRÍTICA DA UTILIZAÇÃO DA IA NO CONTROLE DA PANDEMIA DO COVID-19

Diante da utilização crescente da IA, Jess Whittlestone aponta para a urgência de encontrar maneiras de incorporar a ética no desenvolvimento e na aplicação da IA, embora afirme que até o momento a ética em IA se concentrou em princípios gerais que não informam a solução no caso de conflito entre princípios éticos, afirmando a ineficácia dos princípios éticos gerais (TZACHOR, WHITTLESTONE, SUNDARAM, 2020).

Também nesta área há uma influência do fenômeno das *fake news* e das *deep fakes*, relacionando-se com a criação de perfis falsos, não utilizados por pessoas humanas, mas por bots, a ferramenta tecnológica voltada à modulação de comportamentos, emoções e hábitos, trazendo muitas vezes notícias falsas no tocante à pandemia do COVID-19. Ressalva-se que esta é uma das fases previstas dentro do capitalismo de vigilância em que vivemos, ocorrendo o caos epistêmico causado por amplificação movida a algoritmos e lucros por má informação, desinformação ou fake news.

Como equilibrar via ponderação a necessária observância do segredo industrial e comercial, da proteção intelectual, envolvidas nos programas de computador e nos algoritmos de IA, vistos de forma absoluta nesta seara, com a necessidade de respeitar os direitos fundamentais, o princípio da transparência e da explicabilidade, quando da aplicação da IA no âmbito da saúde e do controle da pandemia do COVID-19? Visa-se, pois, contribuir para alternativas quando da

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

utilização da IA em setores críticos como o da saúde, a partir da preocupação com o fortalecimento do Estado Democrático de Direito, já que muitas destas práticas podem comprometer o aspecto democrático bem como o aspecto do Estado de Direito desta nossa "fórmula política" (GUERRA FILHO, 2007, p. 15ss.).

O mais recente uso da inteligência artificial refere-se ao controle da pandemia do Coronavírus, com relação à vigilância no aspecto de cumprimento pela população de medidas de quarentena, monitoramento do surto e à aceleração de testes de medicamentos, envolvendo a área da vigilância global de doenças. Em 31/03/2019, a empresa canadense Blue-Dot, utilizando-se de IA para revisar mídias e redes sociais, detectou a propagação de uma doença incomum na China, em Wuhan, antes das primeiras manifestações da ONU e da OMS. Países tais como China, Coreia do Sul e EUA conseguem antecipar possíveis áreas de contaminação utilizando a IA (aplicativo Private KIT) para obter dados de geolocalização, disponíveis via smartphones, para verificar o cumprimento da quarentena e do isolamento social.

Um dos principais pontos nesta seara é a crescente utilização das fake news, como uma prática não democrática em razão da desinformação criada em áreas tão sensíveis como a da saúde. Outra questão problemática é a necessidade de anonimização dos dados como medida de segurança. Já que estamos falando de dados sensíveis, contudo, há pouca transparência nesta área, não há sempre a elaboração de um documento essencial, qual seja, o Relatório de Impacto à Proteção de Dados, ou quando envolver a aplicação da IA, o Relatório de Impacto Algorítmico (Algorithmic Impact Assessment [AIA]) ou Artificial Intelligence Impact Assessment (AIIA). Também não há avaliação do respeito à anonimização dos dados de forma independente, além da fragilidade da própria técnica de anonimização, a qual na prática, sempre poderia ser revertida, ainda mais com a utilização da inteligência artificial, a depender dos recursos financeiros disponíveis por aqueles que desejam tal reversão.

A proteção dos dados pessoais está intimamente relacionada com os critérios a serem observados para a estruturação da IA, consoante lista produzida pela Comissão Europeia, com destaque para a proteção de dados e privacidade (*European*

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and "Autonomous" Systems, 2018).

Como fundamentações para justificar de certa forma tal opacidade ou a denominada caixa preta dos algoritmos, são apontadas a proteção do segredo de negócio/industrial, prevenção de concorrência desleal por outras empresas e proteção da propriedade intelectual da empresa. Contudo, até o momento são justificativas vistas sob a ótica de um direito absoluto, inexistente, como bem sabemos, e nada se fala em termos de ponderação de direitos fundamentais envolvidos em tais questões. Em razão das inúmeras possibilidades de danos em razão da produção de decisões via IA, como discriminação, racismo digital, vieses outros, vazamento de dados ou outros incidentes de segurança, abuso de poder de mercado, surge a denominada governança de algoritmos visando reduzir tal problemática ou trazer uma maior regulamentação, reduzindo os resultados indesejáveis.

Contudo, como se pode observar, a maioria das ferramentas de governança não agem sobre o algoritmo, mas sim sobre os dados de que ele precisa para funcionar. E aí está parte do problema, pois tal regulamentação não é suficiente, já que em nada contribui para o desenvolvimento da inteligência artificial explicável e o princípio da explicabilidade, o que seriam centrais se queremos falar em centralização do ser humano e controle humano da tecnologia. É fundamental, pois, que sejam adotados instrumentos de governança para estimular a adoção de certos níveis de transparência, ou de algoritmos abertos.

Neste sentido deverá haver uma conjugação da heterorregulação, aplicando corretamente a ponderação para os casos de colisões de direitos fundamentais ao invés de se reputar a priori sempre a prevalência do segredo industrial/negocial ou direito de propriedade intelectual, como vem ocorrendo. Estamos diante de mais um dos denominados "hard cases", casos de difícil solução, sendo imprescindível sua solução caso a caso, via ponderação, quando serão sopesados não o segredo industrial/negocial em si, mas o direito fundamental atrás destes, como o livre desenvolvimento da atividade econômica, a livre iniciativa, e de outro lado os direitos à privacidade, à autodeterminação informativa, à intimidade, entre outros. Não é

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

possível se postular como uma prioridade absoluta *a priori* dos segredos de negócio/industrial ou da proteção dos direitos intelectuais, como vem ocorrendo. Precisamos de uma prática de sopesamento ou balanceamento, analisando-se diante do caso concreto via princípio da proporcionalidade, sempre tendo em consideração o aspecto central da dignidade humana, a qual em nenhuma hipótese poderá ser maculada, já que é o valor axial de todo Estado de Direito verdadeiramente democrático e de direito (cf. GUERRA FILHO, 2007, p. 77ss., CANTARINI; GUERRA FILHO, 2020, p. 15ss.).

Quanto à conjugação com práticas de autorregulação regulada, é imprescindível a adoção de mecanismos idôneos complementares para se garantir a imparcialidade, transparência e veracidade. Isto porque quando se fala em autorregulação neste setor, sempre caberá indagar se haverá uma possibilidade real de imparcialidade e busca do bem comum, de medidas que venham a beneficiar a sociedade como um todo, em contrapartida à busca normalmente desempenhada por pessoas jurídicas privadas no sentido de incremento do lucro e da minimização de custos, no lugar da proteção do interesse público, por exemplo.

As empresas particulares devem observar na construção dos algoritmos certos padrões estabelecidos refletindo o interesse público, com transparência e responsabilização em níveis adequados, possibilitando um processo de revisão independente, para garantir a integridade e a conformidade com tais valores, como se daria no setor, por exemplo, da indústria automobilística ao trazer padrões de qualidade e segurança para software utilizado nos automóveis. Outro ponto fundamental é a supervisão governamental por meio da regulação dos algoritmos.

Outra questão problemática nesta seara são as práticas de abuso de concorrência, como ponto a ser observado no sentido de ser impossível deixarmos apenas nas mãos da autorregulação tais iniciativas. Acerca deste ponto, o BNDES, em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), apoiou a realização de um estudo para o diagnóstico e a proposição de plano de ação estratégico de Internet das Coisas (*Internet of Things*, IoT), o qual, em seu relatório final, de janeiro de 2018, concluiu pelo modelo da corregulação ou

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

regulação híbrida (MALDONADO; BLUM, 2019, p. 35ss., nota 76) para a certificação de dispositivos de IoT, mediante a consolidação do modelo de certificação voluntária, com a participação de conselho multissetorial ou agência pública focada em segurança da informação.

Importa observar ainda, declaração publicada pelo *European Data Protection Board* (EDPB) sobre os impactos da proteção de dados em casos de concentração econômica, registrando a intenção de analisar os efeitos da aquisição e da concentração de dados comercialmente críticos sobre os clientes de eventuais concorrentes, no contexto da investigação aberta sobre a proposta de aquisição da Shazam pela Apple. Refere-se ao aumento da concentração de mercado no ambiente digital tem o potencial de ameaçar o nível de proteção de dados (ibid., p. 42 e nota 88).

A Comissão Europeia multou em 2017 a Google por abusar de sua posição dominante no mercado, com o seu mecanismo de busca, por conferir vantagem ilegal a seu produto (ibid., nota 90ss.). Há a necessidade, portanto, de criação de deveres informacionais de trânsito na utilização das plataformas digitais e aplicativos digitais, ou seja, deveres de cuidado, diante das alterações produzidas pelas novas formas de comunicação digital, trazendo desafios para a proteção de dados, considerando-se as próprias condições elementares da infraestrutura comunicacional. Destaca-se ainda a necessidade de uma atuação via modelo de uma autorregulação regulada, unindo aspectos da autorregulação pelos particulares e da regulação externa (pelo Estado), compatibilizando assim a experiência e o conhecimento técnico das empresas à proteção do interesse público.

A proposta da autorregulação regulada traria a vantagem de trazer os aspectos positivos, e eliminando os aspectos negativos das duas outras opções possíveis, quais sejam: modelo tradicional – regulamentação estatal, com normas obrigatórias, e coação, e *self-regulation* (autorregulação), práticas internas elaboradas pelas empresas de tratamento de dados, a exemplo das normas publicitárias e código de ética do CONAR, no âmbito das práticas publicitárias. No caso da regulação estatal o lado negativo é a ausência de atualização e conhecimentos técnicos suficientes por

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

parte do Estado. No caso da self-regulation temos a problemática de que nem sempre as empresas visam ao interesse público ou valores públicos. Já a terceira opção da autorregulação regulada, *enforced self regulation*, um misto dos dois anteriores sistemas, haveria uma base de parâmetros gerais de interesses públicos estabelecidos pelo Estado e pela sociedade, havendo uma regulação por lei de parâmetros gerais que deverão ser observados de forma obrigatória. Haveria um controle governamental acerca do reconhecimento dos parâmetros utilizados como adequados.

3 *FAKE NEWS*

As *fake news* normalmente são conceituadas como notícias falsas, embora haja uma fluidez semântica do termo, sendo um conceito polissêmico, relacionando-se às bolhas, *filter bubbles*, correspondendo a grupos de pessoas com a mesma visão de mundo, conceito de Eli Pariser (2012), associado ao conceito de “câmaras de eco” ou "salas espelhadas", uma espécie de “moldura ideológica” onde tudo o que vemos e consumimos é reflexo de nós mesmos, ou seja, as pesquisas no Google são direcionadas ao que os algoritmos entendem serem nossos interesses, trazendo certa homogeneização das pessoas, pois há a tendência de aproximar os iguais. Há pelo menos sete tipos de *fake news*, sendo, pois, um conceito alargado e extensivo, o que poderia contribuir para a dificuldade da temática e do enquadramento legal, e, portanto, trazendo uma fragilidade em termos de segurança jurídica. As *fakes news* vinculam-se ao conceito de era da pós-verdade com o fim de manipulação para diversos fins, econômicos e políticos, ou trazer fragilidades ao sistema democrático (SANTAELLA, 2018, p. 6ss.).

Segundo Eli Pariser (2012), (a) o conteúdo disponibilizado nos serviços na web como os resultados de buscas, e o feed de redes sociais, são cada vez mais personalizados, de acordo com os nossos hábitos de uso das ferramentas; (b) a mudança do fluxo de informação ocorre de forma invisível para os usuários, os quais

ignoram que as informações são personalizadas; (c) as grandes corporações agem com base em seus próprios interesses e, nem sempre com respeito à ética; (d) ocorre a privação de conteúdos e pontos de vistas diferentes aos usuários.

É urgente a análise dos aspectos éticos, políticos e jurídicos da tecnologia persuasiva, já que seu uso está aumentando de forma exponencial, tornando-se mais diversificada, e "invisível", já que acompanha a característica da ubiquidade das novas tecnologias, ou seja, se integram e se misturam ao dia-a-dia de todas as pessoas que possuem acesso à Internet, e um computador ou celular, sendo um aspecto corriqueiro das nossas vidas.

Com a crescente utilização da internet das coisas e dos serviços, sendo incorporada a IA em todos os objetos do quotidiano e em todos os ambientes, há um potencial de intervenção de forma precisa, no momento e local certos, ampliando-se seu poder persuasivo. A utilização da tecnologia persuasiva abrange cada vez mais áreas, tais como publicidade, marketing, vendas, relações de trabalho, e uso político e econômico em geral.

Quando se fala em *fake news* estamos falando, portanto, de manipulação de informação visando a produção de efeitos quanto a mudança comportamental, como ocorreu no caso paradigmático internacionalmente conhecido com o escândalo da *Cambridge Analytica*. A Cambrige Analytica utilizou-se de pesquisas comportamentais e psicológicas, a partir de dados disponibilizados pelo Facebook, traçando diversos perfis de indivíduos para fins de personalização de anúncios, mensagens ou publicidade com o fim de mudança e manipulação de comportamento, visando a eleição política de determinadas pessoas, seus clientes.

A utilização do computador, da inteligência artificial e outras tecnologias para tal finalidade de manipulação comportamental é muito mais potente do que tal possibilidade ser realizada apenas por seres humanos, devido ao grau de intrusão, de velocidade alcançada e por serem tecnologias interativas, potencialização a vulnerabilidade das pessoas alvo. Neste caso como se observa pelo próprio adjetivo utilizado “persuasiva”, a mudança comportamental é intencional, não apenas um acaso ou erro e processamento.

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

Apesar de ser a tecnologia no geral neutra, podendo gerar efeitos positivos, tais como motivar uma pessoa a se exercitar mais, se alimentar de forma mais adequada e saudável, parar de fumar, controlar melhor suas finanças, aprender a meditar, como no caso do aplicativo “Headspace”, sendo cada vez mais utilizados e criados aplicativos para tais finalidades, há diversos impactos negativos, em especial, a depender de quem iria se beneficiar da mesma. De outro lado, não se pode negar que tal utilização é restrita a uma minoria qualificada, não sendo uma possibilidade de utilização democrática, já que envolve conhecimento técnico de ponta, qualificado, em especial acerca da inteligência artificial, envolvida nos novos processos de manipulação comportamental.

Os pontos negativos vão desde um impacto no sentido de causar dependência física e psicológica aos indivíduos, a falta de transparência, a ampla coleta de dados pessoais e dados pessoais sensíveis sem um consentimento adequado, sem prestação de informações suficientes, em nível qualitativo e quantitativo, até à manipulação de comportamento visando auferir vantagens econômicas, visando a indução ao consumo de determinada marca ou produtos específicos, acirrando a polarização da sociedade. Isso permite ainda maior manipulação, como fica claro no exemplo de algumas eleições políticas recentes, tanto no Brasil como no exterior, fazendo parte desta metodologia a utilização de *bots*, robôs que replicam em quantidade avassaladora fake news, induzindo a erro, confusão, polarizações, com o fim de minar a democracia, onde a multiplicidade de visões e opiniões é essencial.

A persuasão pode levar a uma maior normalização de práticas antiéticas e não democráticas à homogeneização de pessoas e comportamentos, à doutrinação, à coerção, à lavagem cerebral e outros resultados indesejáveis, inexistindo até o momento estudos científicos, multidisciplinares em especial, quanto aos aspectos éticos envolvidos.

Há um projeto de lei em votação pela Câmara dos Deputados relativo ao combate às *fake news*, o PL 2.630/2020 apresentado pelo senador Alessandro Vieira (Cidadania-SE) aprovado pelo Senado em 30/06/2020, criando a Lei Brasileira de

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

Liberdade, Responsabilidade e Transparência na Internet, trazendo normas para as redes sociais e serviços de mensagem como WhatsApp e Telegram com o fim de coibir as notícias falsas, contas falsas e robôs, sendo de fundamental importância em setores sensíveis como o da saúde e do controle da pandemia COVID-19.

Referido projeto de lei, contudo, é criticado pela doutrina por excluir de seu âmbito de incidência notícias mesmo que falsas, desde que com conteúdo humorístico, salvo, quando houver objetivo de enganar as pessoas sobre a identidade de candidato a cargo público, com relação às *deep fakes* no período eleitoral. É o que esclarecem Juliano Maranhão e Ricardo Campos, apontando para o risco de uma indesejada criminalização do discurso público, já que a regulamentação está focada no indivíduo, ao contrário da experiência internacional com um viés mais centrado no plano estrutural, bem como a afronta ao princípio da proporcionalidade (MARANHÃO; CAMPOS, 2020). Haveria uma obrigação desproporcional no tocante a proposta de identificação compulsória de todas as contas de usuários de plataformas digitais, a fim de prevenção de crimes, por facilitar a detecção da autoria (art. 5º do PL). Há a obrigação de recadastramento de todas as contas pré-pagas de celular do país, com verificação de identidade dos seus titulares, sendo que pelo menos 0,25% dos dados relativos aos assinantes possui alguma inconsistência cadastral. Afronta-se com isso o princípio da proporcionalidade, pois há necessidade de que somente o mínimo de dados e informações seja coletado, para se atingir a finalidade pretendida com o tratamento de tais dados, utilizando-se do meio menos prejudicial a direitos fundamentais correlacionados. A mesma finalidade seria alcançada com uma regulação que determinasse a inversão do ônus da prova, ou seja, de forma menos gravosa. Ou seja, não seria feita uma prévia exigência de identificação generalizada, evitando-se o acúmulo indiscriminado de dados pessoais (princípio da minimização de dados ou necessidade), estabelecendo-se deveres procedimentais às plataformas, em especial o dever de oferecer uma funcionalidade para a notificação de contas inautênticas na própria plataforma, garantindo assim o contraditório quando da notificação fundamentada por terceiros ou pela provedora de aplicação, responsáveis pela moderação de conteúdo, dando início ao procedimento de apuração. Tal

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

procedimento tem como seu pressuposto o dever de identificação do usuário da conta notificada, suspendendo-se as atividades da conta até haver tal identificação ou cancelando a conta após um determinado período *in albis*.

Outra obrigação legal também flagrantemente desproporcional, consoante o PL é a obrigação do aplicativo *WhatsApp* de armazenar todas as mensagens veiculadas para, após decisão judicial, ser checado o caminho da mensagem ilícita, a fim de garantir o direito de resposta; tal obrigação contraria o próprio modelo de negócio do aplicativo, com base na criptografia de ponta-a-ponta, considerado essencial pelo STF para a garantia para a liberdade de comunicação (ADPF 403).

Importa, contudo, observar quando se fala de ponderação e do princípio da proporcionalidade sobretudo todo o seu procedimento objetivo e racional para a adequada ponderação de normas de direitos fundamentais quando em colisão, analisando-se seu procedimento trifásico, seguindo-se a doutrina tedesca e seus desenvolvimentos no Brasil de forma pioneira por Willis S. Guerra Filho, sendo certo que a proporcionalidade não se resume a uma análise acerca da minimização de dados ou necessidade, sendo o subprincípio da necessidade apenas uma de suas fases ou subprincípios, também devendo ser analisada a adequação e a proporcionalidade em sentido estrito, sendo somente com a análise deste último aspecto ou subprincípio da proporcionalidade, aliás, que se evitaria afrontar o núcleo essencial de todo direito fundamental onde se encontra a dignidade humana.

Sobre tal assunto cumpre observar o projeto de lei da Áustria, de 03/09/2020, que visa combater o discurso de ódio na internet, apresentado pelo governo austríaco ao Conselho Nacional (uma das câmaras do Parlamento austríaco), denominado de "Lei das plataformas de comunicação", seguindo o modelo da legislação alemã adotado em 2018 com a lei *Netzwerkdurchsetzungsgesetz*, estabelecendo deveres de remoção de conteúdo ilegal para plataformas com um grande número de usuários ou um volume de negócios em termos financeiros. Referida lei austríaca traz deveres procedimentais dos intermediários, visando ao combate a *fake news* e aos discursos de ódio (*hate speech*) nas redes sociais, assegurando que o provedor será responsabilizado, não pelo conteúdo postado, mas apenas pelo procedimento ou pela

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

omissão em adotar os procedimentos adequados de moderação de conteúdo (MARANHÃO; CAMPOS, 2020, p. 19-40 e p. 219ss.).

Como se observa, há a necessidade, portanto, de criação de deveres informacionais de trânsito, ou seja, deveres de cuidado, diante das alterações produzidas pelas novas formas de comunicação digital, trazendo desafios para o sistema democrático e a proteção de direitos fundamentais relacionados.

Destaca-se ainda a necessidade de uma atuação via modelo de uma autorregulação regulada, unindo aspectos da autorregulação pelos particulares e da heterorregulação (pelo Estado), compatibilizando assim a experiência e o conhecimento técnico das empresas à proteção do interesse público. Cada vez mais ganham destaque as propostas voltadas à arquitetura dos sistemas, a fim de ser assegurado que as diferentes etapas do ciclo de vida de sistemas de tomada de decisão automatizada, por exemplo, e em outros casos de utilização da IA levem em conta a possibilidade de intervenção humana nas decisões resultantes, na esteira do GDPR, que possui um alcance mais abrangente da intervenção humana, não limitada à revisão de decisões automatizadas, já que a intervenção de titulares de dados pode ocorrer até mesmo durante o processo de desenvolvimento de um sistema, a partir de abordagens como o *design* participativo.

Desta forma, permite-se que os titulares de dados tenham acesso aos meios necessários para contestar decisões automatizadas que lhe causem danos, a partir do acesso às informações essenciais para o exercício do direito à revisão e o respeito ao princípio da explicabilidade. Seria possível por meio de tal transparência a reconstrução do ciclo de tomada de decisão, e a identificação das falhas e das responsabilidades.

4 CONSIDERAÇÕES FINAIS

Cada vez mais é apontada a alterativa de se conjugar a heterorregulação por meio de leis eminentemente principiológicas, com a autorregulação, por meio de boas

práticas, cabendo aqui também a influência dos princípios éticos, utilizando-se da própria tecnologia para um empoderamento dos titulares de direitos fundamentais, em uma espécie de regra transversal, incorporando tal proteção por padrão e de forma automática nos sistemas algoritmos desenvolvidos, bem como com a utilização das *Privacy Enhancing Technologies* (PETs), correspondendo aos denominados *privacy by design* (privacidade por concepção, desde a concepção do negócio) e *privacy by default* (privacidade por valor, padrão predefinido, proteção máxima de forma automática), desde a fase da concepção do produto ou serviço, e em quaisquer operações de projeto de sistemas computacionais.

Trata-se da possibilidade do uso da tecnologia para implementar a efetividade do Direito, até mesmo para o melhor controle da tecnologia, como no caso de utilização para tal fim do *design*, contudo, deve-se ter ciência de que o controle pela tecnologia digital poderá ensejar a perda de regulamentação normativa ou outros fins normativamente indesejáveis. Por isso, apesar de ser uma mudança de paradigma, ou ponto de virada na moldura teórica da proteção dos direitos fundamentais envolvidos em tais relações jurídicas, por meio da adoção de uma arquitetura de gerenciamento dos riscos, precaucionaria de danos, quando da utilização da IA, sempre deverá ser uma atuação conjunta com a heterorregulação e possibilitar-se uma revisão independente.

É fundamental haver um balizamento no sentido de um *framework* mínimo de princípios éticos e jurídicos, não deixando apenas à inciativa privada tal regulamentação, não sendo justificativa suficiente a sua dificuldade de implementação, por questões de barreiras, obstáculos, como a possibilidade de uma lavagem ética. Há possibilidade de utilização de princípios éticos por empresas de grande poder financeiro, como forma de lavagem ética ao tentarem com isso evitar a adoção de princípios jurídicos e regras com força obrigatória. Contudo, com a conjugação de tais regulamentações, no âmbito da moral, do Direito, e da autorregulamentação por meio de boas práticas e *frameworks* por setores independentes e imparciais, seria mitigada tal problemática, bem como diante da observância de sanções sociais, no caso de descumprimento de princípios éticos.

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

Sem uma base principiológica, por meio de princípios éticos e jurídicos de que forma seria possível a promoção de uma IA eticamente responsável e centrada no ser humano, ao se deixar apenas nas mãos das empresas que lidam com IA e que até o momento não atuaram de forma a superar tais problemáticas?

Merece atenção a recente contribuição denominada “Inteligência Artificial com Princípios: Consenso de Mapeamento”, estudo elaborado pelo Berkman Klein Center for Internet & Society da Harvard Law School (FJELD et al., 2020), traçando um panorama mundial das principais contribuições em termos de princípios éticos da IA, incluindo a construção e uma linha do tempo, apesar de as conclusões, por outro lado, apresentam-se um tanto simplistas, resumindo-se, em suma, aos seguintes pontos: há um grande *gap* entre teoria e prática na articulação destes conceitos e a sua realização concreta; apesar de certos pontos de convergência, de modo geral não há uniformidade, mas sim pontos de contradição; haveria um maior número de participação de múltiplos interessados, com potencial de haver ainda mais resultados e entendimentos diversificados; não haveria ainda a elaboração de princípios orientados para aplicações específicas de IA, tais como o reconhecimento facial ou veículos autónomos; há a problemática dos diversos conceitos, concepções e definições acerca da palavra "justiça"; há divergências quanto às consequências nocivas da IA.

É essencial a construção de um mapa conceitual de problemas éticos relacionados a algoritmos para se revisar o debate atual sobre a ética dos algoritmos e identificar quais problemas éticos os algoritmos levantam e quais soluções têm sido oferecidas na literatura relevante para abordar esses problemas, sendo essencial para se falar em justiça algorítmica, devendo ser sempre pautada tal análise na centralidade da pessoa humana, na dignidade humana e na possibilidade humana do controle de tal tecnologia.

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]

REFERÊNCIAS

CANTARINI, Paola. **Teoria fundamental do direito digital**: uma análise filosófico-constitucional. São Paulo: Clube de autores, 2020.

CANTARINI, Paola. GUERRA FILHO, Willis Santiago. **Teoria inclusiva dos direitos fundamentais e direito digital**. São Paulo: Clube de autores, 2020.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. *In*: **Conversações: 1972-1990**. Tradução: Peter Pál Pelbart. São Paulo: Editora 34, 1992, p. 223-231.

FJELD, Jessica; NELE, Achten, HANNAH Hilligoss, HAGY, Adam, SRIKUMAR, Madhulika. *Principled Artificial Intelligence: Mapping Consensus. In:* ***Ethical and rights-based approaches to principles for AI.*** Cambridge, MA: Berkman Klein *Center for Internet & Society,* 2020. Disponível em: https://dash.harvard.edu/handle/1/42160420. Acesso em: 1 de mar. de 2021.

GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 5. ed. São Paulo: RCS, 2007.

HAN, Byung-Chul. **Sociedade da transparência**. Tradução: Enio Paulo Giachini. São Paulo: Editora Vozes, 2016.

LYON, David. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. Tradução: Heloísa Cardoso Mourão et al. *In*: BRUNO, Fernanda et al. (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018, p. 151-180.

MALDONADO, Viviane Nóbrega; BLUM, Renato. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

MARANHÃO, Juliano; CAMPOS, Ricardo. Fake news e autorregulação regulada das redes sociais no Brasil: fundamentos constitucionais. *In*: ABBOUD, Georges; NERY Jr., Nelson; CAMPOS, Ricardo (org.). **Fake news e regulação**. 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2020, cap. 15.

OLIVEIRA, Lorena Silva. O conceito de governamentalidade em Michel Foucault. **Revista Ítaca**, Rio de Janeiro, v. 34, p. 48-72, 2019. Disponível em: https://revistas.ufrj.br/index.php/Itaca/article/view/26395. Acesso em: 20 de febr. de 2021.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

SANTAELLA, Lucia. **A pós-verdade é verdadeira ou falsa?** São Paulo: Estação das Letras e Cores, 2018.

SIBILA, Paula. **O show do eu:** a intimidade como espetáculo. Rio de Janeiro: Contraponto Editora, 2020.

TZACHOR, Asaf; WHITTLESTONE, Jess; SUNDARAM, Lalitha; Ó hÉIGEARTAIGH, Seán. *Artificial intelligence in a crisis needs ethics with urgency.* ***Nature Machine Intelligence***, Berlin, v. 2, p. 365–366, 2020.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância.** São Paulo: Editora Intrínseca, 2021.

[Received/Recebido: Janeiro 11, 2021; Accepted/Aceito: Março 06, 2021]