Revista Jurídica vol. 01, nº. 63, Curitiba, 2021. pp. 89 - 113

CAPITALISMO DE VIGILÂNCIA E A AMEAÇA AOS DIREITOS FUNDAMENTAIS DA PRIVACIDADE E DA LIBERDADE DE EXPRESSÃO

SURVEILLANCE CAPITALISM AND THE THREAT TO THE FUNDAMENTAL RIGHTS OF PRIVACY AND FREEDOM OF EXPRESSION

JOSÉ ADÉRCIO LEITE SAMPAIO

Pós-doutor pela Universidad de Castilla la Mancha. Doutor em Direito. Coordenador do Curso de Mestrado e Doutorado em Direito da Escola Superior Dom Helder Câmara. Professor da PUC-MG e ESDHC/BRASIL. Procurador da República. Currículo Lattes: http://lattes.cnpq.br/6500803835232465. ORCID: https://orcid.org/0000-0002-9452-4811. E-mail: joseadercio.contato@gmail.com

DAVID MENDIETA

Doutor em Direito Constitucional pela Universidade Complutense de Madri (Espanha). Professor de dedicação exclusiva na Universidade de Medellín (Colômbia). Membro do grupo de pesquisas jurídicas da Faculdade de Direito da Universidade de Medellín (Colômbia). Currículo Lattes: http://lattes.cnpq.br/2977074832780697. ORCID: 0000-0002-6944-6815. E-mail: dmendieta@udem.edu.co; davidmendietagonzalez@hotmail.com

MEIRE FURBINO

Doutoranda e Mestre em Direito Público pela PUC-MG/BRASIL. Especialista em Direito Público e Tributário. Bacharel em Direito e Administração. Membro do Grupo de Pesquisa "Direito, Racionalidade e Inteligência Artificial – DR.IA.UnB". Professora

[Received/Recebido: Agosto 18, 2020; Accepted/Aceito: Dezembro 19, 2020]

Universitária. Currículo Lattes: CV: http://lattes.cnpq.br/2767731526290041. ORCID: https://orcid.org/0000-0003-4463-9554. E-mail: meirefurbino@gmail.com

LAVÍNIA ASSIS BOCCHINO

Mestranda na linha de pesquisa "Constitucionalismo democrático" do Programa de Pós-Graduação em Direito da PUC Minas, com bolsa da CAPES-PROEX. Bacharel em Direito (PUC Minas). Membro do Grupo de Pesquisa "Direito, Racionalidade e Inteligência Artificial – DR.IA.UnB". Currículo Lattes: CV: http://lattes.cnpq.br/5508879787247579. ORCID: https://orcid.org/0000-0003-1295-3442. E-mail: lavinia9assis@gmail.com

RESUMO

Objetivo: Analisa-se o capitalismo de vigilância, sob a perspectiva de Shoshana Zuboff, sua relação com a cultura da vigilância e as consequências dessa nova política econômica para os direitos fundamentais - privacidade e liberdade de expressão -, atentando para as possíveis medidas de proteção desses direitos face aos abusos que permeiam as plataformas digitais.

Metodologia: Aplicou-se o método normativo-dedutivo, fundado em revisão bibliográfica nacional e estrangeira, com estudo comparado dos instrumentos jurídicos que discutidos ou utilizados no Brasil, Estados Unidos e União Europeia.

Resultados: A cultura de vigilância e o capitalismo que dela decorre por meio da exploração de big data, expõe a necessidade de se estabelecer transparência por parte das grandes empresas que investem nesse setor. Demanda também legislações que protejam os dados, impeçam o abuso da liberdade de expressão e a disseminação de desinformação intencional.

Contribuições: Aponta-se as facilidades advindas da revolução digital, os riscos decorentes de seu uso e a possibilidade de manipulação dos comportamentos consumeristas, políticos e sociais. Diante da existência do capitalismo baseado na mercancia de dados - capitalismo de vigilância -, a conscientização do público é imprescindível para proteger a liberdade e a privacidade das pessoas. Educação (alfabetização) digital e elaboração de normativas transparentes são meios de limitar o poder das plataformas de mídia digital e impedir que o interesse econômico se sobreponha ao interesse humano.

[Received/Recebido: Agosto 18, 2020; Accepted/Aceito: Dezembro 19, 2020]

Palavras-chave: Capitalismo de vigilância. Direitos fundamentais. Direito à privacidade. Direito à liberdade de expressão. Legislação.

ABSTRACT

Objective: Surveillance capitalism is analyzed, under the perspective of Shoshana Zuboff, its relationship with the culture of surveillance and the consequences of this new economic policy for fundamental rights - privacy and freedom of speech -, paying attention to possible protection measures these rights in the face of the abuses that permeate digital platforms.

Method: The normative-deductive method was applied, based on a national and foreign bibliographic review, with a comparative study of the legal instruments that were discussed or used in Brazil, the United States and the European Union.

Results: The culture of surveillance and the capitalism that results from it through the exploitation of big data, exposes the need to establish transparency on the part of the large companies that invest in this sector. It also demands legislation that protects data, prevents the abuse of freedom of speech and the spread of intentional misinformation.

Contributions: It points out the facilities arising from the digital revolution, the risks arising from its use and the possibility of manipulating consumerist, political and social behaviors. Given the existence of capitalism based on data merchandising - surveillance capitalism - public awareness is essential to protect people's freedom and privacy. Digital education (literacy) and the development of transparent regulations are ways of limiting the power of digital media platforms and preventing economic interest from overlapping human interest.

Keywords: Surveillance capitalism. Fundamental rights. Right to privacy. Freedom of speech. Legislation.

1 INTRODUÇÃO

A partir do uso do computador como meio nas transações econômicas, novas práticas mercadológicas estão sendo incorporadas na era digital, a ponto de permitir se falar em novo estágio ou fase do capitalismo. Os nomes variam, mas o que têm em comum é um novo modelo de negócio, baseado na vigilância dos usuários pelas

plataformas digitais, para definir-lhes padrões de comportamento e induzir-lhes orientações de consumo. A cultura de vigilância normaliza as condutas abusivas dessa nova política econômica, dificultando a conscientização das pessoas quanto aos abusos praticados pelas plataformas de mídia digital, principalmente quanto a extração e análise dos seus dados sem consentimento e sem observar a devida transparência, o que acarreta severas violações aos direitos fundamentais.

O objetivo encontra-se, então, na busca de medidas razoáveis para proteger os direitos fundamentais à liberdade de expressão e à privacidade, sem que seja configurada censura, no contexto do denominado 'capitalismo de vigilância' e das novas tecnologias. Para tanto, metodologicamente, procedeu-se ao estudo comparado de algumas medidas adotadas pelos Estados Unidos, Itália e Brasil, que optaram por criar regulamentos para a proteção dos dados, além de medidas para evitar a propagação de distúrbios informacionais (*fakes news*), principalmente em tempos eleitorais.

Além de iniciativas regulatórias e internacionais, a exemplo do *Global Network Iniciative* (GNI), este trabalho também propõe a necessidade de uma política de educação digital, como forma de emancipação do indivíduo frente aos novos desafios da era digital, para que o cidadão esteja apto a exercer e exigir os seus direitos. Os mecanismos sugeridos visam tornar as pessoas menos vulneráveis às manipulações exercidas pelas plataformas e redes digitais, bem como impedir que os usuários sejam vítimas de predadores ocultos e tenham seus dados pessoais violados.

A análise parte da legislação dos referidos países e da interpretação fornecida por autores nacionais e estrangeiros, quanto não apenas à normatização, mas também às novas práticas que capturam informações e as mercantilizam, a despeito da inércia das pessoas mais interessadas e que, por vezes, têm seus dados expostos, em franca violação aos princípios constitucionais de defesa da privacidade e da liberdade.

[Received/Recebido: Agosto 18, 2020; Accepted/Aceito: Dezembro 19, 2020]

2 A CULTURA DA VIGILÂNCIA E O CAPITALISMO DE VIGILÂNCIA

As pessoas estão se acostumando a terem suas vidas vigiadas dia a dia, seja pelas câmeras de segurança em espaços públicos e privados, seja pelos serviços de localização de veículos ou pelas plataformas de mídia. Esses dispositivos coletam, armazenam, transmitem e analisam os dados sem que o usuário se dê conta. Além disso, as pessoas também desenvolvem um papel ativo, desde o engajamento nas redes sociais, avisos de acidentes ou crimes às instituições de segurança e emergências. Em razão dessas novas práticas, a cultura de vigilância aumenta cada vez mais (LYON, 2019).

Essa rotina de vigilância, da qual se extrai lucro e poder, está diretamente ligada ao capitalismo de vigilância. A cultura de vigilância facilita e normaliza o capitalismo de vigilância, bem como aquela é dependente e alimentada por este. As pessoas que aceitam essa vigilância, geralmente, acreditam que, pela eficiência para se conectar com outras pessoas, vale a pena conviver com os problemas gerados aos seus direitos de privacidade ou liberdades civis (LYON, 2019). Trocam direitos pela comodidade.

Para Shoshana Zuboff (2018, p. 18), o capitalismo de vigilância[1], expressão que cunhou para designar esse estágio da economia capitalista, é a consequência de uma nova lógica de acumulação, o *Big Data*, e se traduz numa "[...] nova forma de capitalismo da informação [que] procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado". A fim de melhor compreender o fenômeno é necessário entender como funciona o *Big Data* e qual é o seu significado. Para Zuboff (2018, p. 25), essa lógica de acumulação em rede tornou-se um "[...] modelo-padrão para a maior parte das *startups online* e aplicativos", sendo que a empresa pioneira dessa lógica foi a *Google*. A partir da análise dos artigos *Beyond Big Data* e *Computer Mediated Transactions* do economista chefe da *Google*,

[1] Esse tipo de capitalismo recebeu outras nomenclaturas, a exemplo de 'capitalismo de plataforma' (SRNICEK, 2016) e 'sociedade de plataforma' (VAN DIJCK; POELL; DEWALL, 2018). As plataformas, no contexto de capitalismo, são verdadeiras infraestruturas digitais por onde circula o capital (GROHMANN, 2019).

Hal Varian, a autora observa que o computador impactou as transações econômicas, sendo o principal mediador dessas relações na atualidade (ZUBOFF, 2018).

Entre os elementos que compõem as transações mediadas por computador estão a "[...] extração e análise de dados", pontos essenciais para compreender o *Big Data* (Zuboff, 2018, p. 26). Para tanto, a autora examina os termos 'extração', 'análise' e 'dados'. Os dados seriam a matéria-prima desse processo, fonte de riqueza, ou seja, o novo petróleo, embora, diferentemente do petróleo, não se esgotem e até se ampliem para novos usos. Segundo Zuboff (2018, p. 27-31), há cinco fontes de dados: (1) "[...] dados derivados de transações econômicas mediadas por computadores"; (2) dados mediados por computador de modo exponencial. Uma estrutura inteligente que advém também de "[...] objetos, corpos e lugares" conectados à *internet*, como por exemplo, "[...] drones", "[...] carros automatizados", "[...] nanopartículas que patrulham o corpo procurando sinais de doenças" (ZUBOFF, 2018, p. 27-31). Essa infraestrutura é conhecida como '*internet* das coisas' (IoT), a permitir a interação humana com as tecnologias inteligentes; (3) "[...] bancos de dados governamentais e corporativos", que incluem os dados ligados às operações bancárias, às "[...] companhias aéreas", "[...] às operações de planos de saúde", "[...] às empresas farmacêuticas e de comunicação [...] e outros mais"; (4) dados provenientes de "[...] câmeras de vigilância públicas e privadas, incluindo qualquer coisa desde *smartphones* até satélites, do Google Street View ao Google Earth"; (5) *small data*, dados não mercantis coletados das pequenas ações, mediadas por computador, que o indivíduo pratica no seu dia a dia, como por exemplo, "[...] curtidas do Facebook", "[...] buscas no Google, e-mails, [...] localizações, [...] compras [...] visualizações de páginas e muito mais" (ZUBOFF, 2018, p. 28, 31).

Os rastros que as pessoas deixam na *internet* começaram a ser vistos como uma forma de aumentar o lucro das empresas, pois passaram a ter um valor financeiro, sendo adquiridos "[...] como matéria-prima para análise e produção de algoritmos que poderiam vender e segmentar a publicidade por meio de um modelo de leilão exclusivo" (ZUBOFF, 2018, p. 32). Criou-se a 'propaganda direcionada': por meio dos rastros deixados pelos usuários é possível descobrir quais os prováveis produtos que têm interesse em comprar, bastando sugestioná-los e direcioná-los à

propaganda do 'correto' anunciante. A *Google* foi a primeira a usar esse modelo de propaganda e, ao perceber que cobrar pelos seus serviços poderia diminuir o número de usuários, passou a investir na venda da 'atenção' dos seus usuários aos anunciantes (ZUBOFF, 2018).

Conforme Jathan Sadowski (2019, p. 2), os dados não são algo que já existe e que é necessário encontrar, como o petróleo, na verdade, os "[...] dados são uma abstração registrada do mundo criado e valorizado por pessoas que usam a tecnologia". Por isso, para o autor seria mais correto usar o termo 'fabricação' de dados ao invés de 'mineração' de dados. Ao considerar os dados como um recurso natural, reforça-se o regime de sua acumulação, quando o que ocorre é que os controles que coletam e processam dados também permitem que eles sejam criados e re-criados (SADOWSKI, 2019).

A extração de dados está relacionada ao processo de "[...] tomar algo" e geralmente é feito pelas empresas sem diálogo e consentimento dos usuários (ZUBOFF, 2018, p. 34). Também não importam os "[...] sentidos individuais" que eles atribuem aos dados, de modo que "[...] os métodos de produção de *big data* a partir de *small data* e as formas pelas quais o *big data* adquire valor refletem a indiferença formal que caracteriza o relacionamento da empresa com suas populações de usuários" (ZUBOFF, 2018, p. 34).

A coleta massiva dos dados sem respeitar a privacidade dos usuários acarretou diversos processos contra a *Google*, relacionados à varredura de *e-mails* sem autorização, à retenção dos rastros de pesquisas e ao rastreamento da localização, dentre outros (ZUBOFF, 2018). Não apenas a *Google*, como também, as demais empresas do setor coletam dados sem o devido consentimento do usuário, o que, para Zuboff (2018, p. 36), resume a extração na "[...] ausência de reciprocidades estruturais entre empresa e suas populações".[2]

[2] A crise causada pela pandemia aumentou o comércio eletrônico e, em consequência, gerou ainda mais dados exploráveis por plataformas como Amazon e Alibaba. O setor de entretenimento também colaborou, no período, para a valorização de plataformas, a exemplo da Netflix, YouTube, Instagram, TikTok. Empresas que se dedicam à entrega em domicílio (Rappi, Ifood, Glovo) também tiveram sua demanda aumentada consideravelmente (BRANDZ, 2019).

Por fim, para a análise desse enorme volume de dados é necessária uma aparelhagem de alta qualidade, com grande força de resfriamento e energia elétrica, além de especialistas qualificados em "[...] análises preditivas, mineração de realidade, análise de padrões de vida e assim por diante" (ZUBOFF, 2018, p. 40). Esse material e método de análise distanciam ainda mais a empresa de seus usuários, que não conseguem compreender o processo de 'dados, extração e análise'. Nem são estimulados a compreender. Por outro lado, as empresas não estão interessadas em responsabilizar-se pelos dados ou por proteger a privacidade dos usuários. O foco é exclusivamente o lucro.

Segundo Zuboff (2018, p. 40-1), os dados comercializáveis formam os "[...] ativos de vigilância", que podem ser considerados "[...] bens roubados", vez que "[...] foram tomados, ao invés de fornecidos", e os investimentos que esses ativos atraem são denominados de "[...] capital de vigilância". O capitalismo da informação, que a autora reconhece como 'capitalismo de vigilância', tornou-se o "[...] modelo-padrão de negócios na maioria das empresas e startups, em que as rotineiras estimativas de valor dependem de 'olhos', mais do que de receita para prever a remuneração dos ativos de vigilância" (ZUBOFF, 2018, p. 41).

Um dos efeitos colaterais desse 'novo' capitalismo é o preço da privacidade. Resta saber se é possível reduzi-lo ou mesmo zerá-lo.

3 VIOLAÇÃO À PRIVACIDADE

Os dados das pessoas são o alvo no modelo de negócio do capitalismo de vigilância. Quanto mais dados se tem, maior será o lucro (SADOWSKI, 2019). Esse cenário permeia diversas relações político-econômicas na sociedade. Há empresas que usam a *internet* para obter lucro com a propaganda direcionada, enquanto agências de crédito analisam os dados para descobrir qual o risco financeiro do cliente. Os consultores políticos os veem como fonte de informações para influenciar e manipular as pessoas com conteúdos direcionados (SADOWSKI, 2019).

No capitalismo de vigilância, as pessoas passaram a ser compreendidas como um conjunto de dados que podem e devem ser explorados, em prol do lucro, sem terem respeitados os seus direitos fundamentais. Como bem pontuam Aza Raskin e Tristan Harris, o serviço que as plataformas oferecem só é gratuito aos usuários, porque eles, os usuários, são os 'produtos' com os dados que são repassados aos anunciantes (O DILEMA..., 2020). Não tem como prevalecer a neutralidade quando as plataformas recebem incentivos para moldar o comportamento e interesses dos usuários e as informações que são destinadas a eles.

Uma forma de conseguir legitimidade para as suas acões, e mesmo algum nível de conivência das autoridades públicas, dá-se por meio da cooperação com essas autoridades para auxiliar no cumprimento da lei (JØRGENSEN, 2019). Na verdade, as empresas acabam auferindo independência para decidir sem a interferência da autoridade pública. Isso ocorre, por exemplo, na retirada do discurso de ódio, que, mesmo com a cooperação público-privado, sem a devida fiscalização, torna-se uma maneira pela qual as empresas assumem o controle sobre quais conteúdos serão retirados da plataforma e como esses conteúdos serão administrados.

A *Global Network Iniciative* (GNI), fundada em 2008, é o resultado de um grande projeto de cooperação entre empresas, governo e sociedade civil. Trata-se de uma plataforma multissetorial única, com a participação de empresas de tecnologia da informação e comunicação (TIC), organizações de direitos humanos e liberdade de imprensa, acadêmicos e investidores, que visam proteger os direitos à liberdade de expressão e a privacidade no meio digital e no âmbito internacional. Dos esforços comuns foram elaborados os Princípios e as Diretrizes de Implementação da GNI destinados a assegurar um padrão global para os direitos humanos no setor de TIC. A GNI promove e compartilha esses objetivos e aprendizados, havendo, inclusive, um fórum com os governos e instituições internacionais, para que, de maneira conjunta, haja o incentivo e a defesa das leis e políticas que visam proteger a liberdade de expressão e a privacidade (*GLOBAL NETWORKING INICIATIVE*, 2020).

[Received/Recebido: Agosto 18, 2020; Accepted/Aceito: Dezembro 19, 2020]

Jørgensen (2019) faz algumas criticas contundentes acerca do GNI, alegando que os padrões que as empresas devem seguir não explicam com clareza as práticas corporativas. Ela ressalta, ainda, que mesmo com a criação do índice *Ranking Digital Rights*, para dar mais transparência às condutas que as plataformas adotam com a finalidade de garantir a proteção dos direitos humanos, há algumas práticas que permanecem obscuras. Por exemplo, as regras que são aplicadas para a retirada dos discursos de ódio e de contas não autênticas, bem como a falta de evidências de que as plataformas respeitem o padrão *Do Not Track*, instrumento utilizado para não rastrear os usuários, impedindo as propagandas direcionadas.

Segundo Z. Bauman (2016, p. 58), isso ocorre porque as plataformas se preocupam muito mais com a aplicação de uma tecnologia que mantenha um padrão

> "[...] público e/ou clientela-alvo", a fim de fazer jus ao "[...] dinheiro graúdo de marketing" que recebem, do que com a integridade dos direitos. Além disso, as pessoas passam a ser 'cidadãs-clientes', de modo que os consumidores assumem uma posição de vulnerabilidade frente às plataformas, aderindo a acordos sem consensos, além de uma conduta manipulável e dependente, sem participação ativa.

Fato é que os usuários, via de regra, não leem os 'Termos de Uso e Serviço', os quais também não apresentam linguagem acessível e clara àqueles. Não havendo ciência sobre como as plataformas criam as regras e as aplicam, não há que se falar em negociação desses contratos. Por essa razão, os interesses dos usuários não são bem representados. Esses 'Termos' apenas concedem poderes e dificilmente os limitam. Estão longe de ser uma espécie de pacto ou constituição do mundo digital. Segundo Suzor (2018, p. 8, tradução nossa), "[...] o constitucionalismo digital requer uma contestação muito confusa das maneiras apropriadas pelas quais o poder das plataformas deve ser limitado", de forma que esses contratos não protegem adequadamente os direitos dos usuários, bem como não responsabilizam devidamente as plataformas; na verdade aumentam o poder delas.

O uso dos dados dos usuários do *Facebook*, em 2016, pela *Cambridge Analytica* nas eleições dos EUA, para manipulação do eleitorado em prol do candidato Donald Trump, provocou um grande escândalo e preocupação acerca dos direitos de privacidade e obrigações das plataformas. A ex-diretora de desenvolvimento de

[Received/Recebido: Agosto 18, 2020; Accepted/Aceito: Dezembro 19, 2020]

negócios da *Cambridge Analytica*, Brittany N. Kaiser, expôs que os testes disponibilizados no *Facebook* eram usados para criar modelos de personalidade de eleitores dos EUA a partir das respostas dos usuários. Além disso, foram acessados perfis de usuários que realizaram os testes, como também, os perfis de seus amigos, sem qualquer consentimento. Os dados extraídos foram analisados e serviram para mirar propagandas direcionadas às pessoas 'persuasíveis', notadamente, aquelas que podiam mudar de ideia ou que tivessem incertas. A estratégia da *Cambridge Analytica* foi criar um conteúdo personalizado, como *blogs*, artigos de *sites*, vídeos, anúncios, entre outros, para que esses usuários votassem no candidato que financiava o esquema (PRIVACIDADE..., 2019).

É imensa a possibilidade de manipulação de usuários, a depender do objetivo que se queira alcançar, seja ele em relação ao mercado consumerista ou mesmo político, em que avançadas técnicas ou engenharia são aplicadas para moldar escolhas políticas em determinado viés ideológico, como demonstra Giuliano Da Empoli (2019), ao se referir ao crescimento do populismo de direita e à interferência sobre eleições como a de Donald Trump, em 2016.

Essas circunstâncias demonstram a necessidade de controle por meio de legislação específica. A pesquisa *National Comprehensive Data Protection/Privacy Laws and Bills* 2019, de David Banisar (2019), atualizada em dezembro de 2019, informou que 130 países já adotaram leis de proteção a privacidade de dados, informações pessoais físicas e digitais, por órgãos públicos e privados, e que quase 40 países têm projetos de lei ou iniciativas pendentes. Em quase todos esses países há um órgão de proteção de dados independente ou uma comissão de informação que supervisiona e aplica as leis.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709, de 14 de agosto de 2018, entrou em vigor em setembro de 2020, sendo inspirada pelo Regulamento Geral sobre a Proteção de Dados 2016/679 (*General Data Protection Regulation* - GDPR) da União Europeia, em vigor desde 25 de maio de 2018 (BRASIL, 2018; UNIÃO EUROPEIA, 2016). A proteção de dados no Brasil apresenta um caráter preventivo que busca evitar danos e vazamentos de dados, tendo sido criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão vinculado à Presidência

da República, com autonomia técnica, para regular, orientar e fiscalizar o cumprimento da LGPD. A referida lei elenca princípios como: *i)* 'necessidade', que obriga a utilização apenas dos dados estritamente necessários; *ii)* 'transparência' com relação as informações passadas aos usuários; *iii)* 'segurança' para a adoção de medidas para proteger os dados pessoais; *iv)* 'prevenção' a fim de evitar danos aos titulares; *v)* 'responsabilização e prestação de contas', que obriga as empresas públicas e privadas a adotarem medidas eficazes ao cumprimento das normas (BRASIL, 2018; PORTAL DA PRIVACIDADE, 2018). Uma incipiente e paradoxalmente tardia normativa para um ambiente dinamicamente refratário à regulamentação.

Em que pese o esforço para regulamentar o acesso à *internet*, bem como a exploração do ambiente virtual, muito há a se fazer. Jørgensen (2019), ao entrevistar funcionários da *Google* e do *Facebook*, constatou que não foi estabelecida nenhuma conexão entre a privacidade dos usuários e possíveis limites ou minimização da coleta de dados por seus serviços. Ao contrário, a privacidade foi descrita "[...] como a capacidade dos usuários de prever e controlar o compartilhamento de informações pessoais com outros usuários" (JØRGENSEN, 2019, p. 179). Significa dizer que para as empresas não há conflito entre o direito à privacidade dos usuários e a coleta e compartilhamento de dados pelas plataformas. No entanto, os recursos de privacidade não se devem limitar à possibilidade de navegação no modo anônimo, que, em entrevistas, as empresas demostraram ser suficientes. Para elas, a real ameaça à privacidade dos usuários seria quando o governo exige o acesso aos dados (JØRGENSEN, 2019).

Roger McNamee (O DILEMA..., 2020) argumentou que a manipulação por terceiros não ocorre por meio de *hackers*. Quando a Rússia interferiu nas eleições norte-americanas de 2016, não hackeou o *Facebook*. Na verdade, os russos conseguiram facilmente agir de maneira ardilosa, usando as ferramentas que a própria plataforma criou para anunciantes e usuários legítimos. Nesse sentido, Sandy Parakilas (O DILEMA..., 2020) defende a necessidade de responsabilizar as empresas de tecnologia da informação, alegando não haver problema que essas empresas foquem no lucro, mas que o real obstáculo seria a inexistência de regulamentação,

regras ou alguma concorrência, o que está permitindo que atuem como se fossem governos.

A falta de controles está levando o capitalismo de vigilância a invadir, cada vez mais, a privacidade das pessoas que, por sua vez, entregam mais de seus dados comportamentais incondicionalmente, em um relacionamento em que poucos ganham muito e muitos recebem migalhas. É o capitalismo selvagem do século XXI, que se tornou um problema global e requer uma solução global, como uma declaração dos direitos humanos nos espaços digitais, que proteja as pessoas das posições dominantes e dos abusos dos comerciantes de dados (SAMPAIO; FURBINO; MENDIETA, 2020).

"O mundo gira em torno de motivações financeiras", afirma Jaron Lanier, "[...] a solução para esse problema precisa vir de uma motivação financeira" (O DILEMA..., 2020). Assim sendo, falta um motivo fiscal para que as empresas alterem seus procedimentos, sendo necessário estabelecer regulamentações nesse sentido. O autor sugere que se imponha uma taxa sobre a obtenção e processamento de dados dessas empresas, o que, além de ser motivo econômico-fiscal, impediria que elas acumulassem massivamente os dados.

A tecnologia tem evoluído muito rapidamente, de modo que a lei (ou os legisladores) tem grandes dificuldades para acompanhar e regular as transformações que estão ocorrendo. Por outro lado, a inércia do direito acaba privilegiando tais empresas em detrimento da proteção dos usuários, que estão sendo relegados a 'fonte de extração' de dados. Nesse panorama, como fica a liberdade de expressão e a democracia, principalmente em tempos eleitorais?

4 LIBERDADE DE EXPRESSÃO E O PROCESSO ELEITORAL DEMOCRÁTICO

A livre manifestação de pensamento é um dos mais caros direitos das sociedades democráticas. Todavia, não é ilimitada. A depender do contexto, quem produz *fake news* ou dissemina discurso de ódio está abusando do seu direito, ao passo que fere o compromisso para com a verdade e viola a esfera do outro (LÔBO;

MOREIRA, 2019). Apesar da necessidade e importância das propostas regulatórias para conter a situação deve-se ficar atento, porém, à tênue linha entre a vigilância das plataformas e a censura institucional (GURUMURHTY; BHARTHUR, 2018). O cuidado com o estabelecimento de limites deve sempre pautar qualquer proposta de regulamentação do fluxo de informação. Na rede e fora dela. As circunstâncias e os impactos da regulamentação devem ser aferidos em juízos de justificação legislativos e testados no caso concreto. O que parece mais perigoso é não tratar do problema pela gravidade de suas consequências. Quando a disseminação massiva de *fake news* extrapola a relação entre os particulares e alcança a esfera pública, como no contexto das eleições, interfere na livre escolha dos eleitores e viola a soberania popular (LÔBO; MOREIRA, 2019).

Ainda que as regulamentações sejam necessárias para o controle das *fake news* e proteção aos direitos fundamentais, essa solução não se tem mostrado suficiente, conforme apontam Camila G. Saraiva e Daniele A. G. D. Mares (2019). As autoras propõem mudança na forma de produção da informação, de modo que permita ao indivíduo protagonizar e influenciar de fato o processo eleitoral, garantindo um resultado democrático: "[...] a comunicação realizada por meio de uma preocupação com autonomia e emancipação do cidadão pode ser um viés capaz de minimizar os males decorrentes de uma sociedade de massa" (SARAIVA; MARES, 2019, p. 40). Porém, a democracia, em nível mundial, vem sofrendo uma crise de autoconfiança devido à falta de credibilidade nas instituições democráticas do governo, às teorias das conspirações sem base científica e ao ódio sem escusas àquele que tem opinião diversa. Segundo Tristan Harris, "[...] isso está acontecendo em grande escala, é controlado por governos, por pessoas milionárias" que querem desestabilizar as eleições, criando guerras culturais e propagando mentiras (O DILEMA..., 2020). Ainda, ressalta Cath O'Neil, a inteligência artificial não pode distinguir a verdade, simplesmente porque não consegue saber o que é a verdade e, assim, resolver o problema da disseminação de informações enganosas (O DILEMA..., 2019).

A inteligência artificial que a *Google* e o *Facebook* empregam serve ao mesmo tempo para "[...] filtrar notícias falsas e remover contas e usuários falsos envolvidos

em campanhas de influência política" (MANHEIM; KAPLAN, 2019, p. 42, tradução nossa), bem como, para beneficiá-los na disseminação de conteúdo enganoso, colocando em dúvida o policiamento das plataformas. O controle sem limites destas empresas, segundo eles, proporciona "[...] uma vasta transferência de direitos dos cidadãos para os diretores corporativos, que devem fidelidade aos acionistas, e não à constituição" (MANHEIM; KAPLAN, 2019, p. 48, tradução nossa).

5 MEDIDAS PARA GARANTIA DOS DIREITOS FUNDAMENTAIS

É certo que os mecanismos relacionados à inteligência de máquina vieram para ficar. Isso, contudo, não significa aguardar os acontecimentos sem buscar alternativas para evitar que algoritmos invadam a privacidade dos indivíduos ou violem impunemente seus direitos. É imperioso que haja um controle sobre as empresas, sujeitando-as a multas e à responsabilidade civil (LÔBO; MOREIRA, 2019). Também se faz necessária uma campanha de educação digital dos cidadãos, ainda que seja um processo de longa duração, principalmente, no que diz respeito às políticas de restrição de discurso de ódio, racismo e discriminação das minorias.

Os indivíduos com alfabetização digital têm mais autonomia para verificar a confiabilidade das mensagens divulgadas nas plataformas de mídia, por isso, são menos vulneráveis às manipulações. Os setores, tanto privado quanto público, não têm "[...] medidas ou incentivos adequados para proteger os dados das pessoas" (TENOVE, 2018, p. 37). Algumas práticas em educação digital devem ser adotadas pelos países. [3] Para Claire Wardle e Hossein Derakhshan (2017), deveria ser estimulado o aprendizado e desenvolvido um conteúdo que aportasse:

> [...] (i) habilidades tradicionais de alfabetização de notícias; (ii) habilidades de verificação de mídia social forense; (iii) informações sobre o poder dos

[3] É inegável importância da educação digital como instrumento de enfrentamento do capitalismo de vigilância. A pandemia gerada pelo Covid-19 expôs um paradoxo: obrigou o uso de tecnologias tanto para o trabalho (*home office*), ensino à distância etc., como também denunciou o fosso existente entre ricos e pobres. Certo é que, ao utilizar essas plataformas, todos, indistintamente, tornam-se potenciais fornecedores de dados.

> algoritmos de moldar o que é apresentado a nós; (iv) as possibilidades, mas também as implicações éticas oferecidas pela inteligência artificial; (v) técnicas para desenvolver ceticismo emocional para anular a tendência de nosso cérebro de ser menos crítico ao conteúdo que provoca uma resposta emocional; e (vi) numeracia estatística (WARDLE; DERAKHSHAN, 2017, p. 70, tradução nossa).

Todavia, não basta colocar totalmente o ônus sobre os usuários e a educação digital que recebem para que eles protejam seus dados e as suas liberdades. Ao contrário, é imprescindível que as empresas de tecnologia da informação e governos tornem as "[...] atividades on-line mais seguras, inclusive responsabilizando as organizações responsáveis pela segurança" (TENOVE, 2018, p. 38, tradução nossa).

Conforme Matteo Monti (2018), as soluções que cada país venha a adotar devem atender aos valores e direitos que suas constituições defendem. Para exemplificar, o autor faz um estudo comparado entre a legislação da Itália e a dos EUA, evidenciando que a primeira assegura o dever da imprensa em respeitar a verdade, agindo contra as notícias falsas criadas com malícia real, enquanto os estadunidenses acabam por proteger a informação falsa, em função da Primeira Emenda dos Estados Unidos que "[...] não distinguiu a liberdade de expressão da liberdade de informação" (MONTI, 2018, p. 7, tradução nossa). Por isso, impedir a divulgação de notícias falsas apresenta mais dificuldades para os norte-americanos do que para o italianos.

Matteo Monti (2018) aponta soluções que não usem o direito penal e nem apliquem a censura, como o instrumento jurídico de 'retificação' da Itália. Isso pode ocorrer em três circunstâncias: "[1] a retificação como dever do jornalista imposta pela lei nº. 69/1963 (Código de Ética do Jornalista), [2] uma correção como consequência de uma decisão judicial e [3] uma correção na mídia após um pedido de um indivíduo" (MONTI, 2018, p. 19). Ele ainda ressalta outra providência efetiva: a 'desindexação' (retirada) de *sites* de disseminação de conteúdos enganosos, desde que tenham sua natureza verificada por uma autoridade independente, ressaltando a importância das agências de checagem de fatos, garantindo um processo imparcial. Contudo, para Monti (2018), nos Estados Unidos, o método da retificação seria provavelmente declarado inconstitucional se instituído por lei, em razão da garantia de não

[Received/Recebido: Agosto 18, 2020; Accepted/Aceito: Dezembro 19, 2020]

regulamentação em respeito a liberdade de expressão ou de imprensa, assegurada pela Primeira Emenda. Por isso, sugere uma autorregulação pelas próprias redes sociais.

Segundo Filippo Donati (2018, p. 440, tradução nossa), a jurisprudência italiana entende que o direito à liberdade de expressão deve ser limitado "[...] apenas para a proteção de outros valores de significado constitucional que com ela possam entrar em conflito", conforme o art. 21 da Constituição da República Italiana [4] . Ressalta, no entanto, que "[...] a divulgação de informações falsas, exageradas ou tendenciosas não é proibida em si mesma, mas apenas quando envolva perturbação da ordem pública" (DONATI, 2018, p. 441, tradução nossa). Somente há a responsabilização ou a punição, quando a notícia falsa prejudica o direito de outrem, de acordo com o art. 656 do Código Penal da Itália[5].

Em fevereiro de 2017 foi apresentado, no ordenamento jurídico italiano, o Projeto de Lei n° 2688, sobre disposições para evitar a manipulação de informações *on line*, garantir transparência na *web* e incentivar a alfabetização midiática (GAMBARO et al., 2017). No entanto, para Filippo Donati (2018), esse projeto, se aprovado, acarretaria em censura, pois ele responsabiliza os gestores do *site*, em caso de publicação ou disseminação de informações enganosas por terceiros/usuários e obriga os Provedores de Servidor de *Internet* (PSIs) a adotarem sistemas de filtragem preventiva contra esse tipo de 'desinformação', o que seria incompatível com a garantia da liberdade de informação da Constituição italiana, além de ir de encontro aos regulamentos nacionais, como o art. 15, §1º, da Diretiva 2000/31 e o art. 17, § 1º do Decreto Legislativo 70/2003, bem como a Declaração de Viena, de 3 de março de 2017 (ITÁLIA, 2000, 2003).

[4] "Art. 21. Todos têm direito de manifestar livremente o próprio pensamento, mediante forma oral ou escrita, e qualquer outro meio de difusão. A imprensa não pode ser sujeita a autorizações ou censuras. Pode-se proceder ao sequestro somente por determinação da autoridade judiciária em caso de delitos, para os quais a lei de imprensa o autorize expressamente, ou em caso de violação das nor- mas que a própria lei exija para a indicação dos responsáveis" (ITÁLIA, [2018], tradução nossa).

[5] "Art. 656. Quem publica ou divulga informação falsa, exagerada ou tendenciosa, que possa perturbar a ordem pública, é punido, se o facto não constituir crime de maior gravidade, com prisão até três meses ou com multa até 309 euros" (ITÁLIA, 2017, tradução nossa).

No Brasil, a liberdade de expressão não é absoluta, não podendo violar outras garantias fundamentais: "[...] 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" (art. 5º, inciso X, CRFB/88) (BRASIL, 1988). Por outro lado, veda a censura prévia (art. 220, § 2º) (BRASIL, 1988). O tema foi discutido no âmbito da Arguição de Descumprimento de Preceito Fundamental (ADPF) 130, que declarou não recepcionada pela Constituição a Lei de Imprensa, Lei n° 5.250/67, editada no período de exceção institucional. Bem pontuou o ministro Ricardo Lewandowski, em seu voto, que, devido ao contexto histórico da edição da referida lei, seu texto estava na contramão dos princípios democráticos da Constituição de 1988, sendo a posição defendida pelo Supremo Tribunal Federal (STF) de que "[...] não cabe ao Estado, por qualquer dos seus órgãos, definir previamente o que pode ou o que não pode ser dito por indivíduos e jornalistas" (BRASIL, 2009, p. 8).

Ainda no contexto brasileiro, entrou em pauta o Projeto de Lei nº 2.630/2020 para o combate das *fake news* no primeiro semestre de 2020 (VIEIRA, 2020). Contudo, referido projeto levantou algumas questões controversas, como a possibilidade de rastreabilidade das mensagens pelos aplicativos, para que se possa identificar a origem dos conteúdos ilegais, na cadeia de compartilhamento. Referida medida, segundo Pablo Bello, diretor de Políticas Públicas do *WhatsApp* para a América Latina, em entrevista a Folha de S. Paulo (MELLO, 2020), poderia acarretar em violação ao direito à privacidade do usuário, por mostrar as pessoas com quem dialoga, ainda que não quebre a criptografia.

O especialista em direito digital, Ronaldo Lemos (2020), defende uma maneira que se vem mostrando eficaz no combate as *fake news*, sem que ocorra a censura prévia, que seria a utilização da estratégia *follow the money* ('siga o dinheiro'). Segundo o autor, a versão brasileira, denominada *Sleeping Giants* Brasil, teve um bom desempenho no combate a desinformação, e, em apenas quatro dias, conseguiu mapear parte do dinheiro que financiava a indústria das *fake news*, servindo, assim, de referência tanto para o Tribunal Superior Eleitoral (TSE), quanto para a Comissão Parlamentar de Inquérito (CPI) das *Fake News*. Apesar de o seu alcance ser limitado, o especialista destaca que as instituições como o Judiciário e o Congresso Nacional

têm um papel fundamental no combate a disseminação de notícias falsas, pois devem identificar e punir aqueles que praticam referido ato.

Este não é um artigo conclusivo, vez que muito há que se pesquisar e debater para serem propostas mudanças efetivas, principalmente quanto ao ordenamento jurídico. Certo é que, como se pronunciou Hal Varian, "[...] não há como colocar o gênio de volta da na garrafa [...]. Todos esperarão ser rastreados e monitorados, já que as vantagens, em termos de conveniência, segurança e serviços, serão enormes [...] o monitoramento contínuo será a norma" (RAINIE; ANDERSON, 2014, n. p., tradução nossa). Entretanto, concomitante com esse novo modelo de capitalismo (de vigilância ou de plataforma), outras maneiras de defesa do indivíduo também deverão ser estabelecidas, de forma a fazer valer as normas que garantem a liberdade e a privacidade, direitos fundamentais assegurados pelas constituições como alicerce democrático.

6 CONSIDERAÇÕES FINAIS

A revolução digital incorporou novos elementos à vida dos indivíduos, para auxiliar nas atividades repetitivas, fornecer maiores comodidades (IoT), encurtar espaços e aproximar pessoas (redes sociais), enfim, facilitar uma série de atividades com emprego de tecnologia baseada em Inteligência Artificial (IA) e algoritmos.

No entanto, ao se valerem dessas novas práticas, os usuários, na maioria das vezes desavisados, deixam rastros em ambiente virtual que permitem aos analistas (nem sempre humanos) captura-los e, a partir deles, extrair preferências e mesmo manipular comportamentos; preferências podem ser moldadas e novos padrões de condutas se convertem em novos hábitos. Uma série de ações são induzidas com base em *big data*. Esse modelo de mercancia com base em dados expostos no ambiente digital favoreceu o surgimento de um novo tipo de capitalismo, o chamado capitalismo de vigilância. A conscientização da existência desse tipo de prática serviu para advertir os usuários dos riscos a que estão expostos ao usar o ambiente digital

sem o devido cuidado e, com isso, contribuindo para o aumento do lucro das empresas.

É inegável que a aplicação de inteligência artificial é positiva e praticamente irrenunciável. Todavia, vislumbram-se riscos à liberdade e à privacidade que merecem especial atenção, a requerer que, não apenas o segmento privado, como também o poder público, desenvolvam ferramentas que inibam a invasão e intromissão indesejada na vida particular e na vida coletiva. Saber-se 'produto' resultante da utilização gratuita de ferramentas digitais já impõe um certo cuidado por parte de usuários. Todavia, isso não é suficiente.

Os estados têm trabalhado no sentido de editar normas que limitem a atuação dos gigantes do setor, enquadrando atividades que ultrapassem a razoabilidade e impondo padrões para as práticas corporativas. Essas normativas, no entanto, carecem de transparência e, quando há colaboração das referidas empresas com os governos, prevalece um interesse empresarial, associado ou não ao poder de controle estatal, em detrimento do interesse particular.

As ações produzidas por meio digital vão muito além de simples compras na *internet*. Por trás das propagandas pode haver um direcionamento de comportamento subliminar a ocasionar decisões importantes que impactam a vida de toda a coletividade, como, por exemplo, na manipulação de eleições em prol de determinados candidatos. Por certo, essa prática compromete a liberdade de autodeterminação política e sujeita os indivíduos a resultados distorcidos.

A conscientização, pela população, de todo esse mecanismo existente nos bastidores do ambiente virtual poderia diminuir os riscos de atividades impróprias ou com interesses espúrios. A educação ou alfabetização digital mostra-se imprescindível para esse objetivo.

No âmbito governamental, tem-se o desafio de elaborar leis que inibam a divulgação de discurso de ódio, *fake news*, conteúdos enganosos, que tenham o desiderato de fazer prevalecer a liberdade do cidadão, bem como manter sua privacidade, sem, contudo, violar a liberdade de expressão - bem jurídico também garantido constitucionalmente. Essa é uma missão urgente para os países democráticos que, em que pese respeitarem a liberdade de expressão, deverão

conjugá-la com outros princípios fundamentais significativos como a liberdade e a privacidade, a fim de evitar que o capitalismo de vigilância (ou de plataforma) se sobreponha ao interesse do cidadão.

Por fim, em tempos digitais, o público e o particular devem voltar sua atenção para um denominador comum: fazer com que os interesses humanos e de alteridade sejam superiores aos econômicos, esses capitaneados pela exploração de dados e de tecnologia digital. É um caminho que permite a inovação sem corromper os valores da dignidade humana, bem maior a ser beneficiado pelas revoluções, inclusive a tecnológica.

REFERÊNCIAS

BANISAR, David. ***National Comprehensive Data Protection/Privacy Laws and Bills 2019*.** 30 nov. 2019, atualizado: 05 dez. 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416#>. Acesso em: 28 set. 2020.

BAUMAN, Zygmunt. **Babel:** entre incerteza e a esperança. Trad. Renato Aguiar. Rio de Janeiro: Zahar, 2016.

BRANDZ. ***Top 100 most valuable global brands 2019 report***. 2019. Disponível em: <https://www.brandz.com/admin/uploads/files/BZ_Global_2019_WPP.pdf>. Acesso em: 28 nov. 2020.

BRASIL. [**Constituição (1988**)]. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 27 jun. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 30 mai. 2020.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Arguição de Descumprimento de Preceito Fundamental 130 Distrito Federal.** Arguição de Descumprimento de Preceito Fundamental (ADPF). Lei de imprensa. [...]. Regime constitucional da "liberdade de informação jornalística", expressão sinônima de liberdade de imprensa. A "plena" liberade de imprensa como categoria jurídica proibitiva de qualquer tipo de censura prévia. [...]. Peculiar fórmula constitucional de proteção a interesses privados

que, mesmo incidindo a posteriori, atua sobre as causas para inibir abusos por parte da imprensa. Proporcionalidade entre liberdade de imprensa e responsabilidade civil por danos morais e materiais a terceiros. [...]. A imprensa como instância natural de formação da opinião pública e como alternativa à versão oficial dos fatos. Proibição de monopolizar ou oligopolizar órgãos de imprensa como novo e autônomo fator de inibição de abusos. [...]. Não recepção em bloco da Lei nº 5.250/1967 pela nova ordem constitucional. Efeitos jurídicos da decisão. Procedência da ação. Relator: Ministro Carlos Britto, 30 de abril de 2009. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605411>. Acesso em: 27 jun. 2020.

DONATI, Filippo. *Fake news e libertà di informazione.* ***MediaLaws -*** *Rivista di diritto dei media*, Itália, 2/2018, maggio, p. 440-6, 25 jun. 2018. Disponível em: <http://www.medialaws.eu/wp-content/uploads/2019/05/RDM-2-2018.pdf>. Acesso em: 20 set. 2020.

EMPOLI, Giuliano Da. **Os engenheiros do caos:** como as fake news da conspiração e os algoritmos estão sendo utilizados para disseminar ódio, medo e influenciar eleições. Trad. Arnaldo Bloch. São Paulo: Vestígio, 2019.

GAMBARO, Adele et al. ***Disegno di Legge n. 2688/2017.*** *Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica.* Senato della Repubblica, 28 fev. 2017. Disponível em: <https://www.senato.it/leg/17/BGT/Schede/Ddliter/47680.htm>. Acesso em: 23 set. 2020.

GLOBAL NETWORKING INICIATIVE (GNI). ***About GNI.*** 2020. Disponível em: <https://globalnetworkinitiative.org/about-gni/>. Acesso em: 19 set. 2020.

GROHMANN, Rafael. Financeirização, midiatização e datatificação como sínteses sociais. ***Mediaciones de la Comunicación*****,** Montevideo, v. 14, n. 2, p. 97-117. Disponível em: <https://revistas.ort.edu.uy/inmediaciones-de-la-comunicacion/article/download/2916/2991>. Acesso em: 21 jun. 2020.

GURUMURTHY, Anita; BHARTHUR, Deepti. ***Democracy and the algorithmic turn:*** Issues, challenges and the way forward. *SUR 27*, v. 15, n. 27, p. 41-52, 2018. Disponível em: <https://www.researchgate.net/publication/328760413_Democracy_and_the_algorithmic_turn-_Issues_challenges_and_the_way_forward>. Acesso em: 15 set 2020.

ITÁLIA. *Codice Penale*. ***Edizione Aggiornata al 25 ago.*** 2017. Disponível em: <http://www.procuragenerale.trento.it/attachments/article/31/cp.pdf>. Acesso em: 23 set. 2020.

ITÁLIA. **Constituição da República Italiana de 1947.** Senato della Repubblica, Costituzione Italiana Edizione In Lingua Portoghese, [2018]. Disponível em:

<https://www.senato.it/application/xmanager/projects/leg18/file/repository/relazioni/libreria/novita/XVII/COST_PORTOGHESE.pdf#page50>. Acesso em: 20 set. 2020.

ITÁLIA. Decreto Legislativo 9 aprile 2003, n. 70. *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.* ***Gazzetta Ufficiale,*** Supplemento Ordinario n. 61, n. 87 del 14 aprile 2003. Disponível em: <https://www.camera.it/parlam/leggi/deleghe/03070dl.htm>. Acesso em 24 set 2020.

JØRGENSEN, Rikke Frank. *Rights Talk: In the Kingdom of Online Giants. In*: JØRGENSEN, Rikke Frank (ed.). ***Human rights in the age of platforms***. Cambridge, MA: MIT Press, 2019. p. 163-87.

LEMOS, Ronaldo. Contra fake news, siga o dinheiro. ***Folha de S.Paulo***, 24 mai. de 2020. Disponível em: <https://www1.folha.uol.com.br/colunas/ronaldolemos/2020/05/contra-fake-news-siga-o-dinheiro.shtml>. Acesso em: 24 mai. 2020.

LÔBO, Edilene; MOREIRA, Pedro Henrique Costa e. Fake News e autenticidade das eleições brasileiras. *In*: OLIVEIRA, Armando Albuquerque de et al. (coords.). **Teoria da democracia e da filosofia do estado e direito constitucional.** Zaragoza: Prensas de la Universidad de Zaragoza, 2019. p. 285-300.

LYON, David. *Surveillance capitalism, surveillance culture and data politics*. *In*: BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn (ed.). ***Data Politics***: *Worlds, Subjects, Rights*. Abingdon: Routledge, 2019. p. 64-77. Disponível em: <https://www.taylorfrancis.com/books/e/9781315167305>. Acesso em: 1 set. 2020.

MANHEIM, Karl; KAPLAN, Lyric. Artificial Intelligence: Risks to Privacy and Democracy. ***21 Yale Journal of Law and Technology*** 106, 2019.

MELLO, Patrícia Campos. Lei de fake news será 'tornozeleira eletrônica' para milhões de pessoas, diz diretor do WhatsApp**.** ***Folha de S. Paulo***, 22 de jun. de 2020. Disponível em: <https://www1.folha.uol.com.br/poder/2020/06/lei-de-fake-news-sera-tornozeleira-eletronica-para-milhoes-de-pessoas-diz-diretor-do-whatsapp.shtml>. Acesso em: 22 jun. 2020.

MONTI, Matteo. ***The new populism and fake news on the Internet:*** *how populism along with Internet new media is transforming the Fourth Estate*. Stals Research Paper 4, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175280>. Acesso em: 20 ago. 2020.

O DILEMA das Redes. **Direção:** Jeff Orlowski. Estados Unidos: Netflix, 2020.

PRIVACIDADE Hackeada. **Direção:** Karim Amer e Jahane Noujaim. Roteiro: Karim Amer e Pedro Kos. Estados Unidos, 2019. Distribuidor: Netflix. Documentário, 1h 50min.

PORTAL DA PRIVACIDADE. **Os 10 Princípios para o Tratamento de Dados Pessoais.** 19 jul. 2018. Disponível em: <https://www.portaldaprivacidade.com.br/infografico-04-os-10-principios-para-o-tratamento-de-dados-pessoais/?_sf_s=Os+10+princ%C3%ADpios+para+o+tratamento+de+dados>. Acesso em: 29 set. 2020.

RAINIE, Lee; ANDERSON, Janna. ***The future of privacy*****:** *digital life in 202*5. Dec. 18, 2014. Disponível em: <https://www.pewresearch.org/internet/2014/12/18/future-of-privacy/>. Acesso em: 20 ago. 2020.

SAMPAIO, José Adércio Leite; FURBINO, Meire; MENDIETA, David. *La Declaración Universal de Derechos Humanos en Espacios Digitales: una necesidad en los tiempos cibernéticos.* **Revista Juridica,** [S. l.], v. 4, n. 61, p. 30-69, oct. 2020. Disponible en: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/4451>. Consultado en: 29 nov. 2020. doi: http://dx.doi.org/10.21902/revistajur.2316-753X.v4i61.4451

SARAIVA, Camila Gonçalves; MARES, Daniele Aparecida Gonçalves Diniz. O discurso de ódio e a recusa aos fatos: Fake news nas eleições brasileiras. *In*: LÔBO, Edilene; OMMATI, José Emílio Medaur (coords.). **Processo Eleitoral e Estado de Direito:** Diálogos sobre democracia e política. Belo Horizonte: Conhecimento, 2019. p. 21-44.

SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da (orgs.). **A sociedade de controle:** manipulação e modulação nas redes digitais. São Paulo: Hedra, 2018.

SRNICEK, Nick. ***Platform Capitalism***. Cambridge, UK-Malden, MA: Polity, 2016.

SUZOR, Nicolas. *Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms.* ***Social Media+ Society***, v. 4, n. 3, 2018. https://doi.org/10.1177/2056305118787812

TENOVE, Chris et al. ***Digital Threats to Democratic Elections****: How Foreign Actors Use Digital Techniques to Undermine Democracy. Centre for the Study of Democratic Institution*s, UBC, 2018. http://dx.doi.org/10.2139/ssrn.3235819

UNIÃO EUROPEIA. **Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (Directiva sobre o comércio electrónico).** Parlamento Europeu, Conselho

da União Europeia, 8 jun 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32000L0031>. Acesso em: 23 set 2020.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados 2016/679.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 29 set. 2020.

SADOWSKI, Jathan. *When data is capital: datafication, accumulation, and extraction.* ***Big Data & Society***, p. 1-12, jan.-jun. 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/2053951718820549>. Acesso em 21 set. 2020.

VIEIRA, Alessandro. **Projeto de Lei nº 2630, de 2020.** Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em: 26 jun. 2020.

WARDLE, Claire; DERAKHSHAN Hossein. ***Information Disorder:*** *Toward an Interdisciplinary Framework for Research and Policy Making.* Strasbourg: Council of Europe, 2017. Disponível em: <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c>. Acesso em: 20 jun. 2020.

ZUBOFF, Shoshana. Big other*:* capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, F. et al. (orgs.). **Tecnologias da vigilância**: perspectivas da margem. Trad. H. M. Cardozo et al. São Paulo: Boitempo, 2018. p. 17-68.