

O Capitalismo de Vigilância e a Política da Desinformação

Julian Affonso de Faria

Centro Universitário Una, Brasil - jullianfaria@hotmail.com

Cláudio Márcio Magalhães

Centro Universitário Una, Brasil - claudiomagalhaes@uol.com.br

Resumo

Como o capitalismo de vigilância contribui para a economia política da desinformação? Esse artigo tem como objetivo demonstrar a estreita relação entre o fenômeno que tem dominado o mundo cibernético – o tráfico legal e ilegal de dados obtidos a partir da vigilância do cidadão – com outro fenômeno contemporâneo, a desinformação, centrada principalmente nas notícias falsas que deixaram sua excepcionalidade para se transformarem em ações orquestradas capazes de abalar práticas democráticas. Para tal, realizou-se

uma exposição de casos sintomáticos de acontecimentos contemporâneos com o objetivo de ilustrar uma breve revisão da literatura com as temáticas sobre Capitalismo de Vigilância, Cidadania e a Política da Desinformação. Chegou-se à conclusão que a adoção de políticas públicas relacionadas à educação e regulação do tema, sem a violação de direitos humanos fundamentais dos indivíduos, é a melhor forma de proteger a sociedade dos efeitos nefastos desse fenômeno contemporâneo.

Palavras-Chave: vigilância digital, *big data*, *fake news*, cidadania, democracia.

Surveillance Capitalism and the Policy of Disinformation

Abstract

How does surveillance capitalism contribute to the political economy of disinformation? This article aims to demonstrate the close relationship between the phenomenon that has dominated the cyber world - the legal and illegal traffic of data obtained from citizen surveillance - with another contemporary phenomenon, disinformation, centered mainly on false

news that left its exceptionality to transform into orchestrated actions capable of undermining democratic practices. To this end, an exhibition of symptomatic cases from contemporary events were held in order to illustrate a brief review of the literature on the themes of Vigilance Capitalism, Citizenship and the Policy of Disinformation. It was concluded

that the adoption of public policies related to education and regulation of the theme, without violating the fundamental human rights of individuals, is the best way to protect society from the harmful effects of this contemporary phenomenon.

Keywords: digital surveillance, big data, fake news, citizenship, democracy.

INTRODUÇÃO

A monetização dos dados pessoais trouxe uma nova ordem econômica que utiliza informações extraídas das pessoas, através da vigilância, como matéria-prima gratuita para práticas comerciais. Trata-se do “Capitalismo de Vigilância”, um novo modelo de negócio que procura prever e modificar o comportamento humano como forma de controlar o mercado e produzir receitas (Zuboff, 2018). Ocorre que o uso de dados como mercadoria pode trazer prejuízos consideráveis aos cidadãos. Além da violação da privacidade e intimidade das pessoas, o capitalismo de vigilância pode também influenciar e modificar o comportamento humano, desinformando e induzindo o indivíduo a tomar decisões que podem impactar negativamente a sua vida e a vida das outras pessoas.

Para Orłowski (2019), as grandes empresas de tecnologia têm como modelo de negócio a venda da “certeza” de que seus anunciantes terão o máximo de sucesso em suas campanhas publicitárias. Para tanto, é necessária a obtenção de muitos dados através do rastreamento infinito dos hábitos das pessoas. Tais dados são usados para criar modelos que preveem as ações dos indivíduos cujo objetivo é descobrir o que deve ser mostrado para eles, a fim de manipular os seus hábitos de consumo. O produto vendido por essas empresas é a gradativa e imperceptível mudança no comportamento dos cidadãos, para que eles vejam o mundo da forma que o anunciante queira. Portanto, num mundo onde se tornou fundamental ter conexões virtuais, a comunicação e cultura passam a estar irremediavelmente ligadas às práticas da desinformação e manipulação (Orłowski, 2019).

As empresas que praticam o capitalismo de vigilância, após extraírem e refinarem os dados pessoais dos cidadãos, criam modelos de previsão comportamental e vendem tais informações para quem quiser e puder pagar, sejam grandes corporações, sejam governos autoritários (Frazão, 2019). E é nesse sentido que a economia política da desinformação é alimentada diretamente pelo capitalismo de dados, uma vez que

O Capitalismo de Vigilância e a Política da Desinformação

para se manipular alguém é preciso ter amplo acesso a seus dados.

Considerada uma das maiores ameaças à democracia, a economia da desinformação consiste no uso de aplicações na internet com o fim de propagar informações falsas ou manipuladas em prol de algum grupo político (Brisola & Bezerra, 2018). Essa estratégia normalmente é utilizada em redes sociais digitais como WhatsApp e Twitter, tendo em vista o seu baixíssimo custo operacional e seu efeito de propagação de informações em rede.

O presente trabalho visa investigar como as práticas do chamado capitalismo de vigilância podem ser utilizadas para alimentar a política da desinformação e como tal fato pode afetar as bases da democracia. Para tanto, utilizou-se uma pesquisa bibliográfica a partir de uma revisão de literatura sobre os temas propostos, bem como uma pesquisa documental, analisando dados e informações oriundos de fontes primárias.

Nosso percurso metodológico parte do conceito do fenômeno Capitalismo de Vigilância e de como a monetização dos dados pessoais alimenta uma cultura de vigilância que viola dos direitos dos indivíduos relacionados à sua cidadania. Após, apontamos as estratégias da política da desinformação, ressaltando a sua face mais perigosa, as chamadas *fake news*. Depois de demonstrar como a segurança de dados se tornou uma preocupação mundial, apontamos possíveis caminhos para a sociedade se proteger dos fenômenos pesquisados.

A CULTURA DA VIGILÂNCIA E O CAPITALISMO DE DADOS

Os dados são o novo petróleo. Esta é uma das frases mais repetidas no meio econômico nos últimos anos. E não por acaso. O avanço das tecnologias de informação levou os dados pessoais a ser um produto incansavelmente procurado por empresas que surgiram com o capitalismo de vigilância. Assim como foi a terra na sociedade agrícola, as máquinas a vapor e a eletricidade na sociedade industrial, e os serviços na pós-industrial, a informação é o novo elemento estruturante da nossa era (Bioni, 2020).

Neste sentido, a monetização dos dados pessoais constitui uma preocupação mundial, uma vez que as consequências desse novo capitalismo de dados não se restringem apenas à seara econômica. A sociedade em geral, a democracia e os direitos dos cidadãos, são vítimas dessa nova forma de vigiar visando o lucro.

Segundo Bioni (2020), com o avanço da tecnologia e o novo modelo organizacional das empresas em rede, o consumidor passou a participar de uma forma mais ativa do ciclo de consumo, uma vez que a publicidade passou a ser direcionada com base na preferência dos consumidores. Nessa lógica, é necessária uma monitoração constante do comportamento das pessoas, uma vez que suas informações pessoais acabam se tornando a matéria-prima a ser explorada por esse tipo de atividade econômica (Zuboff, 2020).

O comportamento humano exposto no mundo digital tornou-se, portanto, uma mercadoria valiosa nesses tempos de sociedade de informação. E para conseguir essa mercadoria empresas de extração de dados usam diversos tipos de métodos.

Para isso, segundo Zuboff (2018), o componente principal do capitalismo de vigilância é o *big data*. Sobre tal fenômeno, pode-se afirmar que:

O big data é constituído pela captura de *small data*, das ações e discursos, mediados por computador, de indivíduos no desenrolar da vida prática. Nada é trivial ou efêmero em excesso nessa colheita: as “curtidas” do Facebook, as buscas do Google, e-mails, textos, fotos, músicas e vídeos, localizações, padrões de comunicação, redes, compras, movimentos, todos os cliques, palavras com erros ortográficos, visualizações de páginas e muito mais. Esses dados são adquiridos, tornados abstratos, agregados, analisados, embalados, vendidos, analisados mais e mais e vendidos novamente (Zuboff, 2018, p.31).

Assim, não são poucas as fontes de dados que alimentam o capitalismo de vigilância na sua nova lógica de acumulação de capital. Dentre tais fontes estão a “internet das coisas”, onde uma rede de sensores inteligentes e dispositivos conectados à internet podem monitorar todos os passos de uma pessoa em tempo real; os bancos de dados governamentais e corporativos, inclusive aqueles ligados à intermediação de pagamentos eletrônicos, bancos, operações por cartões de crédito, planos de saúde e às agências de avaliação de crédito; os dados decorrentes das câmeras de vigilância públicas e privadas, que podem ter sua origem desde simples *smartphones* até satélites, ou mesmo no Google Street View e Google Earth. Por fim, existem ainda os

O Capitalismo de Vigilância e a Política da Desinformação

dados gerados por pesquisas no Google, músicas do Spotify, páginas no Facebook, blogs, redes e vídeos no YouTube (Zuboff, 2018).

Neste sentido, Zuboff (2020) conceitua o Capitalismo de Vigilância como uma nova lógica econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais, onde a produção de bens e serviços é subordinada a uma arquitetura global de modificação do comportamento humano. A autora ainda afirma que:

O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como inteligência de máquina e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de *mercados de comportamentos futuros*. (Zuboff, 2020, p.18,19).

A conceituação do Capitalismo de Vigilância feita por Zuboff, entretanto, não está isenta de críticas. Para Morozov (2019), a autora peca ao não considerar que o capitalismo de dados pode apresentar uma atuação assimétrica em diferentes partes do mundo. Assim, da mesma forma que o capitalismo industrial possuía um padrão específico de exploração para os centros de poder e consumo e outro para a periferia, o mesmo acontece com o capitalismo de vigilância. Ainda segundo Morozov (2019), Zuboff não define o que há de “capitalismo” no capitalismo de vigilância, uma vez que não aprofunda na sua relação com o desenvolvimento com o capitalismo neoliberal.

Apesar das críticas sofridas por Zuboff, não resta dúvida de que a extração dos dados pessoais além do que seria necessário para a melhoria dos serviços que justificaram a sua coleta, torna-se um negócio lucrativo que se retroalimenta indefinidamente. A economia movida a dados e o capitalismo de vigilância encontram-se umbilicalmente ligados, uma vez que a extração de dados, devido à sua importância econômica, é diretamente proporcional ao aumento da vigilância (Frazão, 2019).

CAPITALISMO DE VIGILÂNCIA, DESINFORMAÇÃO E A CORROSÃO DA DEMOCRACIA

O fenômeno da desinformação não é algo novo, trata-se de um conceito antigo que nasce ligado principalmente a projetos militares de contrainformação e espionagem (Brisola & Bezerra, 2018). Segundo Serrano (2010), a desinformação é fruto de mecanismos muito mais complexos do que uma mentira grosseira. São ações que buscam construir um cenário intencionalmente determinado, mediante a divulgação de informações manipuladas, fragmentadas e retiradas de sua historicidade. O objetivo é distorcer a realidade e confundir. Nem sempre se trata de uma informação falsa, mas também de uma informação que manipula fatos (Serrano, 2010).

Para Brisola e Bezerra (2018), uma das características da desinformação é a oferta de uma visão maniqueísta de mundo, com oposições bem claras entre bem/mal, certo/errado, branco/preto, nós/eles. Além disso, utiliza-se também a bandeira da opinião pública para incluir em suas informações a opinião que se quer propagar. É comum, por exemplo, o uso de expressões como “o povo brasileiro clama por justiça!”. A linguagem utilizada valoriza a emoção antes da crítica e embora possa sugerir distanciamento e neutralidade, na verdade carrega envolvimento e parcialidade. Outra característica da desinformação é a prática de impor etiquetas positivas ou negativas a determinados grupos com o objetivo de formar ou manipular a opinião pública (guerrilheiros esquerdistas, terroristas islâmicos, manifestantes vândalos, por exemplo). Neste sentido, as pessoas tendem a se acostumar com tais etiquetas e perdem a sua capacidade de avaliar situações de forma crítica (Brisola & Bezerra, 2018). No entanto, não se pode desgarrar a desinformação também do seu aspecto enquanto disputa narrativa – entre grupos, entre políticas, entre culturas – em que essas palavras ganham conotações distintas, podem ser informação para uns e desinformação para outros.

A política da desinformação é fruto de uma crise identitária onde as pessoas são tragadas pelo pensamento hegemônico em razão de estarem imersos em uma avalanche de informações. Trata-se, portanto, de um sistema informacional que molda a opinião pública de acordo com seus interesses, que podem ser políticos, ideológicos ou econômicos, utilizando uma série de artifícios e mecanismos, dentre os quais se encontra a divulgação das *fake news*. A desinformação nem sempre é ilegal, mas a sua abrangência pode afetar a democracia, os processos políticos e as políticas públicas (Brisola & Bezerra, 2018).

O Capitalismo de Vigilância e a Política da Desinformação

Serrano (2010) define a política da desinformação como um complexo de ações que tem como objetivo construir um cenário intencionalmente determinado, podendo estar presente em livros de história, jornais de ampla circulação ou em discursos políticos. Nos dias de hoje, devemos mencionar também a forte presença da política da desinformação em redes sociais e aplicativos de mensagens instantâneas.

Para Brisola e Bezerra (2018), a fim de atingir os seus objetivos que podem ser econômicos, políticos e/ou ideológicos, a política da desinformação utiliza diversas estratégias, tais como:

- a) O alinhamento aos interesses do poder econômico e do poder político nos meios de informação e comunicação;
- b) Dificuldade do leitor ou usuário de identificar as origens, contextos e motivações dos fatos e informações;
- c) Elaboração de notícias de forma resumida, sem visão crítica, baseadas em fontes cujo interesse não é claro;
- d) Excesso de informações, a fim de que haja uma dificuldade de selecioná-las;
- e) Aderência a sentimentos e a comoção, ao invés da razão;
- f) Adesão a uma visão de mundo que já vem pronta;
- g) A utilização da emoção como foco maior da informação;
- h) A utilização de uma linguagem que sugere uma neutralidade, a fim de dar a uma opinião com o aspecto de informação isenta.

A política da desinformação preenche um vácuo deixado num momento em que a informação profissional produzida por jornalistas enfrenta uma crise sem precedentes, tanto no Brasil quanto no mundo. Segundo o pesquisador e professor Bruno Souza Leal, do Departamento de Comunicação Social da Universidade Federal de Minas Gerais (UFMG), a perda de credibilidade do jornalismo profissional tem sido recorrente em democracias no mundo inteiro. No Brasil, tal fenômeno pode ser explicado por dois cenários distintos. O primeiro cenário trata-se de uma característica mundial onde o advento da internet fez com que a informação circulasse por outros canais e também por uma grande diversidade de mecanismos e processos que vão muito além dos veículos tradicionais de jornalismo (PRAE, 2020).

O segundo cenário apontado pelo Professor Bruno Leal (PRAE, 2020), diz respeito à estrutura de comunicação em massa herdada da ditadura militar no Brasil, com base numa produção centrada nas cidades do Rio de Janeiro e São Paulo,

distante, portanto, dos aspectos regionais do país, bem como em razão das empresas jornalísticas brasileiras estarem concentradas nas mãos de poucos agentes, ou seja, são controladas por algumas famílias e grupos empresariais muito específicos. É preciso observar também que as polarizações em torno das ideologias políticas, bastante acirrada nos últimos anos, também proporcionam um terreno fértil para o crescimento da política da desinformação, especialmente com a divulgação de *fake news* (Brisola & Bezerra, 2018).

Embora o termo *fake news* tem sido utilizado de forma abrangente, se confundindo com o significado da desinformação, é certo que esta vai muito além das notícias falsas e pode ter objetivos econômicos, políticos e ideológicos. Segundo Brisola e Bezerra (2018), as *fakes news* constituem apenas uma das faces da política da desinformação, uma vez que se tratam de artigos e informações travestidos de notícias, intencionalmente e verificadamente falsos com a intenção deliberada de enganar o leitor.

O fenômeno da propagação das notícias falsas, umas das faces da desinformação, é também fruto do alcance global da internet, dos aparelhos celulares inteligentes e das plataformas digitais que ampliaram a capacidade de comunicação do ser humano. Uma notícia espalhada através de um aplicativo de mensagens, por exemplo, pode alcançar milhões de pessoas sem que sua origem ou veracidade sejam identificadas (Galhardi, Freire, Minayo, & Fagundes, 2020).

A política da desinformação também encontra campo fértil nas plataformas reguladas por algoritmos pertencentes a grandes corporações como Facebook e Google. E neste ponto, o capitalismo de vigilância e a desinformação possuem estreita relação com a economia política da comunicação (EPC). A EPC, de uma forma crítica, aborda os interesses comerciais das empresas de comunicação na produção de conteúdo, entendendo que os meios de comunicação de massa são também indústrias que fabricam produtos culturais. Neste sentido, a produção de bens culturais e artísticos são apenas formas de produzir audiência que será trocada por faturamento publicitário gerando lucro os seus produtores (Rêgo & Dourado, 2013). E as plataformas digitais possuem um papel de destaque neste contexto.

Bolaño (1996) afirma que o desenvolvimento de mega sistemas de informação, criados para fomentar o processo de acumulação de capital é a base de uma grande internacionalização da indústria cultural, razão pela qual o setor das telecomunicações se transformou em elemento central para a rearticulação do padrão de desenvolvimento capitalista. A economia política da comunicação possui como um dos seus elementos

O Capitalismo de Vigilância e a Política da Desinformação

centrais o fato de que todas as formas mediadas de comunicação envolvem o uso de recursos materiais escassos. Assim, a nossa compreensão de mundo, bem como a nossa possibilidade de transformá-lo, são determinados pelo modo em que o acesso e o controle sobre esses recursos escassos são estruturados (Bolaño, 1996).

Bolaño (1996) considera correta a ideia frankfurtiana de que os meios de comunicação de massa são entidades econômicas que cumprem uma função econômica direta, através da produção e distribuição de mercadorias, e também uma função indireta, através da publicidade. A estruturação das redes telemáticas globais por grandes empresas tem início com a internacionalização produtiva e financeira ocorrida na economia mundial a partir dos anos 1990. Logo, há uma forte correlação entre a globalização da economia e a mudança estrutural dos sistemas de comunicação. Neste sentido, a indústria cultural é o ponto de partida para a constituição de uma cultura capitalista mundial, onde a globalização produtiva conduz à globalização da publicidade e com ela, da cultura industrializada que lhe serve de suporte (Bolaño, 1996).

Como dito, as plataformas digitais algorítmicas contribuem de forma importante neste contexto, uma vez que se guiam, principalmente, por interesses comerciais. Trata-se de meios de comunicação de massa que são uma excelente ferramenta para os negócios do capitalismo de dados. Como consequência, a desinformação prospera de forma acentuada nesse ambiente. Embora os conteúdos encontrados nessas plataformas sejam em sua maioria, de teor pessoal ou familiar, existem também conteúdos noticiosos que são postados por jornalistas, especialistas, políticos e celebridades. Neste cenário, a produção de notícias é transferida das empresas jornalísticas tradicionais para os usuários de tais plataformas, de forma que a imprecisão do que é notícia ou não, alimenta a desinformação (Castro, 2020).

Não podemos esquecer que os veículos jornalísticos tradicionais nem sempre são sinônimos de confiabilidade. Entretanto, nas plataformas o usuário muitas vezes assume a produção e distribuição de informações, ao lado ou no lugar de um jornalista, que seria o mediador a definir o que é notícia e de que forma a divulgar. Castro (2020) denomina tal fenômeno como “onimediação desigual”, ou seja, todos exercem alguma mediação ainda que em graus díspares. Ocorre que nas plataformas algorítmicas o critério de avaliação aplicado aos conteúdos, na maioria das vezes, é de ordem pecuniária, ou seja, a prioridade será dada ao que pode trazer um maior retorno financeiro. O chamado valor-algoritmo é a pedra de toque de uma economia da informação, baseada em conteúdos que não são necessariamente

notícias na concepção tradicional. Esse modelo de negócios praticado pelas plataformas transforma essa economia da informação em uma verdadeira economia da desinformação (Castro, 2020).

Na onimedição desigual defendida por Castro (2020), o valor-algoritmo não está ligado à qualidade da informação mediada em termos de reputação e credibilidade, mas sim na capacidade de captar a atenção dos usuários das plataformas. Para tanto tão importante quanto aquilo que é exibido ao usuário, é o conteúdo que ele divulga para chamar a atenção de outros usuários. O sucesso das viralizações depende do encadeamento desses dois processos.

Ocorre que o esquema de publicidade da internet enseja que a desinformação se transforme facilmente em um filão de negócios, uma vez que as notícias falsas viralizam muito mais rapidamente do que uma informação verdadeira, fato que gera uma receita considerável via publicidade. É muito mais fácil conseguir cliques em anúncios de publicidade quando se compartilha uma notícia sensacionalista, usualmente falsa (Castro, 2020). Um artigo embasado em um levantamento feito no Twitter por pesquisadores do MIT, concluiu que naquela plataforma digital, os boatos se alastram mais depressa e para um universo maior de pessoas do que notícias verdadeiras (Vosoughi, Roy, & Atal, 2018).

Em um trabalho publicado recentemente, o professor de psicologia e ciência neural da Universidade de Nova York, Jay Van Bavel, afirmou que as pessoas tendem a acreditar em notícias falsas em razão de um fenômeno chamado de viés de confirmação, ou seja, a tendência dos indivíduos de buscarem informações que reafirmem suas próprias convicções e crenças, seja por meio de memórias seletivas, seja por meio de fontes que reafirmem o seu modo de ver a vida. Os seres humanos, em geral, têm uma tendência de aceitar e compartilhar evidências que reafirmem a sua visão de mundo, bem como de rejeitar tudo aquilo que a contradiz (Galhardi et al., 2020).

Também neste sentido, em entrevista à BBC News Brasil, o psiquiatra e diretor da Associação Brasileira de Psiquiatria, Cláudio Martins, apontou que pessoas que compartilham notícias falsas, experimentam uma sensação de bem-estar semelhante à que sentem aquelas que suam drogas, uma vez que são estimulados no cérebro mecanismos de recompensa e prazer imediatos. Tais sentimentos, além de impulsionar a transmissão compulsiva da mesma informação, também impedem o desenvolvimento de senso crítico sobre a questão (Galhardi et al., 2020).

Assim, o modelo de negócios das plataformas algorítmicas funciona da seguinte

O Capitalismo de Vigilância e a Política da Desinformação

forma: os algoritmos estimulam a disseminação de desinformação tendo em vista que uma notícia falsa gera muito mais retorno em termos de visualização de publicidade do que uma informação verdadeira. Quando mais cliques, maior o valor-algoritmo e maior é a divulgação da informação. Seja ela verdadeira ou não. As plataformas digitais algorítmicas, na visão de Castro (2020), se expandiram juntamente com a hegemonia do neoliberalismo e o seu funcionamento guarda muita afinidade com a lógica de mercado neoliberal, ou seja, os conteúdos são avaliados pelo prisma da sua circulação e capacidade de gerar publicidade, predominando aqueles que conseguem maior repercussão. São meios de comunicação de massa que estimulam a produção de conteúdos, nem sempre verdadeiros, para a venda de publicidade.

Como dissemos, não há nada de novo no fenômeno da desinformação. O que é novo é a velocidade que ela se propaga no meio digital. E tal fato se dá, principalmente, em razão do capitalismo digital fazer da desinformação um produto altamente rentável, uma vez que produzir e compartilhar narrativas falsas atraem muitos cliques. (Morozov, 2018). E é neste ponto que o capitalismo de vigilância atua como meio facilitador para a divulgação da desinformação.

O capitalismo de dados, ao contribuir para a política da desinformação, viola os direitos dos cidadãos em diversas esferas. Para Marshall (1967), a cidadania se divide em direitos civis, políticos e sociais. Os direitos civis se traduzem nos direitos necessários à liberdade individual, tais como liberdade de imprensa, pensamento, direito à privacidade, à igualdade perante a lei e também o direito à justiça. Os direitos políticos consistem no direito do cidadão de participar do exercício do poder político, ou seja, de organizar partidos políticos, votar e ser votado. Já os direitos sociais significam os direitos de participação na riqueza coletiva, reduzindo as desigualdades e garantindo um mínimo de bem-estar coletivo.

Para o exercício de uma cidadania plena, é necessária observância desses três elementos de forma concomitante. A violação a um deles importa em violação aos demais. Pode até ser possível haver direitos civis sem direitos políticos. Entretanto, o contrário não é viável. Na ausência de liberdade de pensamento, por exemplo, os direitos políticos podem servir muito mais para justificar governos do que para representar cidadãos. Por outro lado, sem direitos civis e políticos, os direitos sociais tendem a ser arbitrários e não alcançam a sua verdadeira função (Carvalho, 2002).

Assim, a corrosão da democracia por parte da desinformação estimulada pelo capitalismo de vigilância começa com o desrespeito aos direitos à privacidade e liberdade de expressão e termina com a violação ao direito de participar do governo

da sociedade tendo como fundamento os valores democráticos. Para se ter uma ideia, em julho de 2015 foram divulgados conteúdos de *e-mails*, documentos internos e faturas da empresa italiana *Hacking Team*, que demonstram que países da América Latina como Brasil, Colômbia, Equador, Honduras, México e Panamá compraram licenças para o uso de um *software* chamado *Remote Control System* (RCS). Este *software* espião é capaz de acessar qualquer tipo de informação contida num telefone celular ou mesmo em um computador, tais como contatos, chamadas de áudio e vídeo, *e-mails*, geolocalização em tempo real, senhas, microfone e *webcam* (Acha, 2016).

Segundo um informe da ONG *Derechos Digitales*, o vazamento de informações da *Hacking Team* revelou que, no Equador, o RCS foi utilizado pelo governo de Rafael Correa para vigiar o seu opositor Carlos Figueroa. No México, a grande maioria das autoridades que adquiriu o *software* espião não estava autorizada a exercer atividades de vigilância. Além disso, os documentos divulgados indicaram que a *Drug Enforcement Agency* (DEA) norte-americana intercepta todas as comunicações de todos os cidadãos colombianos. Segundo os mesmos dados, o Brasil gastou cerca de 67.900 euros para aparelhar a sua Polícia Federal com o RCS (Acha, 2016).

Os sete países que compraram o RCS possuem legislações que preveem sanções que visam impedir esse tipo de invasão em computadores e *smartphones*. A tecnologia utilizada pela *Hacking Team* é muito mais invasiva que uma mera interceptação telefônica determinada por uma ordem judicial. Desta forma, exemplo acima demonstra como o capitalismo de dados também pode violar o direito ao devido processo legal e o princípio da legalidade.

Em 2013, o ex-analista da Agência de Segurança Nacional (NSA) dos EUA, Edward Snowden, divulgou documentos secretos da NSA comprovando que a inteligência americana monitorava de forma ilegal mensagens de e-mail, Skype, bem como todo tipo de informação trocada em redes sociais e na internet, ferindo as liberdades individuais e invadindo a privacidade de cidadãos e autoridades em todo o mundo. Dentre as autoridades espionadas estavam a ex-presidente brasileira Dilma Rousseff e seus principais assessores, e também o então presidente do México, Enrique Peña Nieto. Além de pessoas, Snowden revelou que a NSA e a CIA teriam espionado também empresas como a Petrobrás, o Google e a rede Swift, que reúne vários bancos privados, além do Ministério das Relações Exteriores da França (BBC, 2013).

Na época o governo dos EUA sofreu severas críticas da comunidade internacional e também da sociedade civil americana, por ter espionado indivíduos e empresas que

O Capitalismo de Vigilância e a Política da Desinformação

não possuíam qualquer envolvimento com o terrorismo e, por isso, não representavam qualquer risco para segurando dos EUA.

O documentário “Privacidade Hackeada” (Karin & Noujaim, 2019) relata como a empresa de marketing político britânica denominada *Cambridge Analytica* manipulou os dados pessoais de cerca de 87 milhões de usuários do Facebook, quando trabalhava na campanha eleitoral de Donald Trump à presidência dos Estados Unidos da América e também do *Brexit*, plebiscito que decidiu pela saída do Reino Unido da União Europeia. No caso da eleição norte-americana, a *Cambridge Analytica* utilizou dados captados por um aplicativo instalado dentro da plataforma Facebook para influenciar a eleição presidencial em favor do então candidato Donald Trump. A estratégia era identificar eleitores que ainda não tinham definido o seu voto ou que podiam mudar de ideia, a fim de influenciar o seu comportamento para que votassem no candidato republicano.

Segundo Karin e Noujain (2019), através da análise dos dados extraídos do Facebook, foi criado um modelo capaz de prever a personalidade de cada adulto nos Estados Unidos. A partir daí, conteúdos personalizados foram enviados a cada eleitor pertencente ao público alvo através de blogs, vídeos, anúncios e notícias falsas, para que este enxergasse o mundo da forma que a *Cambridge Analytica* queria e votasse em seu candidato. A campanha de desinformação nas redes ligou a candidata republicana Hillary Clinton à velha e corrupta política, definindo-a como “perigosa”, “psicopata” e “mentirosa”, além de convocar os eleitores indecisos a “derrotar a desonesta Hillary”. Para enviar mensagens personalizadas era preciso ter acesso a dados pessoais. Ocorre que esses dados foram extraídos sem o conhecimento de seus proprietários.

Ao investigar a atuação da *Cambridge Analytica* na campanha do *Brexit*, o parlamento britânico concluiu que as leis britânicas não estão adequadas a essa nova realidade, razão pela qual não é possível uma eleição livre e justa naquele país. Além do Reino Unido e dos Estados Unidos da América, a *Cambridge Analytica* também atuou comprovadamente em eleições na Malásia, Trinidad e Tobago, Lituânia, Romênia, Quênia e Gana. Em todos esses países o modo de operação foi sempre o mesmo. Extrair dados das pessoas sem o seu conhecimento e utilizar esses dados para descobrir qual é a melhor forma de manipular suas ações, notadamente nos processos eleitorais (Karin & Noujaim, 2019).

Assim como nos exemplos da eleição de Trump nos EUA e da campanha do *Brexit* no Reino Unido, a disseminação de notícias falsas também foi sentida nas eleições

presidenciais brasileiras de 2018, onde a extrema direita supostamente conseguiu sua vitória graças ao poder viral de conteúdo de desinformação amplamente divulgado em redes sociais (Galhardi et al., 2020). Tanto que foi criada no Brasil uma CPMI (Comissão Parlamentar Mista de Inquérito) com o objetivo de investigar os ataques cibernéticos que atentam contra a democracia e o debate público, além da utilização de perfis falsos para influenciar os resultados das eleições brasileiras de 2018 (SENADO FEDERAL, 2021).

Os exemplos citados demonstram de forma inequívoca como o Capitalismo de Dados viola um dos elementos mais importantes da cidadania, a democracia. E o caminho utilizado passa pela política da desinformação.

UMA PREOCUPAÇÃO MUNDIAL

Nos últimos tempos, a segurança de dados tornou-se uma preocupação mundial. Na União Europeia já vigora, desde 2018, a Regulação Geral de Proteção de Dados (GDPR, na sigla em inglês), uma norma que amplia a proteção de dados dos cidadãos daquele bloco econômico. Os Estados Unidos da América também são uma referência neste aspecto, possuindo uma farta legislação sobre o tema, tais como a Lei de Privacidade da Comunicação Eletrônica (ECPA), de 1986, que proíbe a interceptação de mensagens telefônicas e eletrônicas (incluindo e-mails) e garante a segurança de informações tanto durante a transmissão, quanto no seu armazenamento e a Lei de Proteção da Privacidade de Crianças (COPPA), que institui regras para websites e serviços *on line*, visando a proteção à privacidade de crianças e adolescentes de até 13 anos na internet. Existem também normas setoriais de proteção como a Lei de Portabilidade e Transparência de Seguros de Saúde (HIPAA) e a Lei de Privacidade (*Privacy Act*) que fixa diretrizes para a coleta, armazenamento e disseminação de dados por agências federais (Valente, 2018).

Na América Latina, diversos países também já possuem legislações relativas à proteção de dados, como por exemplo, Chile, Argentina, Uruguai e Colômbia (Valente, 2018). O Brasil passou a fazer parte do rol de países que possuem uma legislação específica para a proteção de dados pessoais a partir da criação da Lei 13.709 de 2018, já em vigor (Brasil, 2018).

O Poder Judiciário Brasileiro também tem se posicionado sobre o tema. Em uma decisão recente, o Supremo Tribunal Federal suspendeu a eficácia da Medida

O Capitalismo de Vigilância e a Política da Desinformação

Provisória 954/2020 (Brasil, 2020) que previa o compartilhamento de dados de usuários de telecomunicações com o IBGE, para fins de produção de estatísticas relacionadas à Pandemia do Covid-19. As ações foram propostas pelo Conselho Federal da Ordem dos Advogados do Brasil e por partidos políticos como o Partido da Social Democracia Brasileira – PSDB, o Partido Socialista Brasileiro – PSB, o Partido Socialismo de Liberdade – PSOL e o Partido Comunista do Brasil (STF, 2020).

Dentre outros argumentos, - alegou-se que a Medida Provisória violou a Constituição Federal no que se refere à dignidade da pessoa humana, à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e ao sigilo dos dados, uma vez que obrigava as empresas de telefonia fixa e móvel a disponibilizar ao IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, mesmo sendo para a produção de estatística oficial durante a pandemia do novo coronavírus. A Suprema Corte Brasileira decidiu que tal compartilhamento violaria o direito constitucional à privacidade, à intimidade e ao sigilo de dados, uma vez que a relativização de tais direitos pela Medida Provisória 954/2020 deveria observar os princípios da razoabilidade e da proporcionalidade, o que não ocorreu na prática (STF, 2020).

Ainda na esfera jurídica, também tramita no Congresso Nacional a Proposta de Emenda à Constituição (PEC) n. 17/2019 (Senado, 2019), que visa incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão. Neste caso, a proteção dos dados pessoais deixaria de ser um corolário do direito à privacidade para se tornar um direito fundamental autônomo.

Também no âmbito da sociedade civil existe uma séria preocupação com relação à extração de dados pessoais sem o conhecimento de seus proprietários.

Uma matéria publicada em um portal de notícias *on line* (Tilt, 2020), relata o caso de um afro-americano que foi preso na cidade de Detroit, porque um programa de computador concluiu de forma errônea que a foto constante de sua carteira de motorista era idêntica à imagem de um ladrão de relógios capturada por câmeras de vigilância. A mesma reportagem informa ainda que diante da imagem de várias pessoas segurando um termômetro, o programa de análise de imagens denominado “Google Vision” reconhece um binóculo nas mãos de uma pessoa de cor branca e uma arma na mão de uma pessoa negra. O caso citado demonstra que a interpretação de dados de forma enviesada pode gerar sérios prejuízos para a honra e imagem das pessoas.

Em 2019 foi descoberto que o sistema de segurança residencial da Google, *Nest Secure*, trazia um microfone embutido em seus dispositivos sem que a empresa tivesse

informado aos seus usuários sobre o fato. Em resposta, a empresa Google afirmou que houve um erro ao não informar nas especificações do produto a existência do microfone (Duong, 2019). Na China, até o final de 2020 o governo pretende concluir o seu novo Sistema de Crédito Social (SCS), uma espécie de ranking de confiança do governo no cidadão onde o comportamento de toda a população chinesa será monitorado e pontuado. Através de tecnologia de reconhecimento facial e inteligência artificial, as atitudes dos chineses passam a valer créditos positivos ou negativos. Assim, esse sistema de controle social irá definir, com base na pontuação de cada indivíduo, se este terá direito a comprar passagens aéreas, conseguir um novo emprego ou matricular seu filho em uma escola de qualidade, por exemplo (Braun, 2018).

Os exemplos citados demonstram que as práticas do capitalismo de vigilância (devendo ser incluída também neste rol, a política da desinformação), seja por empresas privadas ou por governos, constitui uma preocupação mundial por ser uma séria ameaça não somente à democracia, mas também aos direitos civis tais como privacidade, igualdade e liberdade. E que são práticas inerentes e intrínsecas da Economia da Desinformação e que, como tal, devem-se ser estudadas e combatidas, em consonância.

CONSIDERAÇÕES FINAIS

Diante da evidência de que o capitalismo de vigilância também utiliza de suas práticas pouco ortodoxas, para dizer o mínimo, para alimentar a política da desinformação, surge a seguinte questão: como as pessoas podem se proteger da manipulação no mundo digital?

Segundo Morozov (2018), alguns países europeus propuseram diversas soluções equivocadas nos últimos anos, tais como abrir centros de combate à desinformação, como as *fake news*, e multar quem as espalhar pelas redes sociais (como sugerido por autoridades alemãs); o banimento de todos os memes da internet (proposta do partido governante da Espanha), ou mesmo criar comissões de especialistas para averiguar a veracidade ou não das notícias (conforme solução proposta pelo chefe antitruste da Itália).

Viu-se que soluções que pensem o problema como uma questão de mercado, apenas sugerem soluções mercadológicas, as quais, portanto, não têm, necessariamente,

O Capitalismo de Vigilância e a Política da Desinformação

compromisso com o interesse público, a manutenção da democracia e a defesa dos direitos humanos. Assim, caminha-se para o inevitável e necessário estabelecimento de políticas públicas que, de alguma forma, deverá prever e impor algum tipo de regulação pública. Como já acontece na Europa e nos EUA, e timidamente no Brasil, o sistema judiciário já demanda dos poderes executivos e legislativos referenciais para julgar os já inúmeros casos, e, enquanto isso, legisla por conta própria, estabelecendo multas milionárias e obrigações às empresas, em um recado claro que a auto regulação não funcionou e que o Estado democrático precisa fazer sua parte. E que a sociedade civil deve acompanhar esses movimentos e, através de suas organizações públicas e privadas, os órgãos de comunicação social, os sistemas educacionais, as instituições representativas das diversas dimensões da sociedade, entre outros e outras, tomem os dados pessoais como algo tão importante a ser defendido como os demais direitos humanos.

Não há dúvida de que o capitalismo de vigilância e a política da desinformação constituem uma das maiores preocupações da sociedade nos tempos atuais. O grande desafio é enfrentar tais fenômenos, seja com leis específicas, seja com políticas públicas, sem cercear o direito dos cidadãos à liberdade de pensamento e de opinião. A censura não resolverá o problema, uma vez que não se protege um direito violando outro. A solução também seria investir em educação para que se formem cidadãos dotados de senso crítico para saber diferenciar uma informação confiável de outra manipulada.

Nenhuma é uma solução de fácil aplicabilidade. No entanto, todas elas se iniciam no debate, na pesquisa e na análise que esse trabalho se propôs, um entre muitos de já existem e que, obrigatoriamente, ainda devem acontecer neste período de atribuições informacionais que a Humanidade transpassa. Só pela ciência, pelo conhecimento e pelo respeito aos direitos humanos se encontrará uma esperança do uso das tecnologias modernas de informação e segurança para uma verdadeira comunicação social.

REFERÊNCIAS

- Acha, V. G. (2016). Hacking Team: malware para la vigilancia en américa latina. Derechos Digitales. <https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf>
- BBC News Brasil. (2013). EUA espionaram Petrobrás, dizem papéis vazados por Snowden. 08 set. https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilma_mm
- Bioni, B. R. (2020). *Proteção de Dados Pessoais: a função e os limites do conhecimento*. 2a. ed.. Rio de Janeiro: Forense.
- Bolão, C. R. (1996). Economia política, globalização e comunicação. *Novos Rumos*, 25(11), 15-23. Marília - SP. <https://doi.org/10.36311/0102-5864.11.v0n25.2047>
- Brasil. (2018). Lei Geral de Proteção de Dados (LGPD). Lei.13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei no.12.965, de 23 de abril de 2014 (Marco Civil da Internet). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm
- Brasil. (2020). Medida Provisória. 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações [...]. Diário Oficial da União, Brasília, DF, 17 abr. <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-954-de-17-de-abril-de-2020-253004955>
- Braun, J. (2018). Na China, atos dos cidadãos valerão pontos e limitarão seus projetos. *Veja*, Ed. 15 nov. <https://veja.abril.com.br/mundo/na-china-atos-dos-cidadaos-valerao-pontos-e-limitarao-seus-projetos/>
- Brisola, A., & Bezerra, A. C. (2018). Desinformação e circulação de “Fake News”: distinções, diagnóstico e reação. Anais do XIX Encontro Nacional de Pesquisa em Ciência da Informação – Enancib 2018. Londrina - PR.
- Carvalho, J. M. (2002). *Cidadania no Brasil: o longo caminho*. 3a. ed. Rio de Janeiro: Civilização Brasileira.
- Castro, J. C. L. (2020). A economia da desinformação em plataformas algorítmicas. São Paulo. Anais do 43º Congresso Brasileiro de Ciências da Comunicação – Intercom 2020.

O Capitalismo de Vigilância e a Política da Desinformação

- Duong, R. (2019). Shoshana Zuboff em Capitalismo de Vigilância. [Video]. Canal VPRO Documentary. 20 dez.. 50 min. <https://www.youtube.com/watch?v=hIXhnWUmMvw&t=37s>
- Frazão, A. (2019). Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: G. Tepedino, A. Frazão, & M. D. Oliva, *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*, 1a. ed., pp. 23-52. São Paulo: Thomson Reuters Brasil.
- Galhardi, C. P., Freire, N. P., Minayo, M. C., & Fagundes M. C. (2020). Fato ou Fake? Uma análise da desinformação frente à pandemia da Covid-19 no Brasil. <https://www.scielo.br/j/csc/a/XnfpYRR45Z4nXskC3PTnp8z/abstract/?lang=pt>
- Karim, A., & Noujaim, J. (Diretores) (2019). Korin, J., Kos, P., Dreyfous, G. & Amer, K. (Produtores). Privacidade Hackeada [Filme Cinematográfico]. Estados Unidos da América: Netflix. 1h50min.
- Marshall, T. H. (1967). *Cidadania, classe social e status*. Rio de Janeiro: Zahar.
- Morozov, E. (2018). *Big Tech: a ascensão dos dados e a morte da política*. São Paulo: Ubu.
- Morozov, E. (2019). Capitalism new clothes. The Baffler. February 4. <https://thebaffler.com/latest/capitalisms-new-clothes-morozov>
- Orlowski, J. (Diretor). (2019). O Dilema das Redes [Filme Cinematográfico]. Estados Unidos da América: Netflix. 1h34min.
- PRAE. (2020). Cenários explicam perda de confiança no jornalismo. 3 de Abr. <https://www.ufmg.br/prae/noticias/cenario-explicam-perda-de-confianca-no-jornalismo/>
- Rêgo, I. N. B. & Dourado, J. L. (2013). Economia Política da Comunicação e uma Reflexão Teórica sobre a Mídia nas Sociedades Capitalistas. Anais do XIV Congresso de Ciências da Comunicação na Região Nordeste – Mossoró – RN – Intercom.

- Senado Federal. (2019). Proposta de Emenda à Constituição n.17 de 2019. 03 jul. <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>
- Senado Federal. (2021). CPMI – Fake News. Comissão Parlamentar Mista de Inquérito – Fake News. Mai. <https://legis.senado.leg.br/comissoes/comissao?codcol=2292>
- Serrano, P. (2010). *Desinformação: como os meios de comunicação ocultam o mundo*. Rio de Janeiro: Espalhafato.
- STF – Supremo Tribunal Federal. (2020). STF suspende compartilhamento de dados de usuários de telefônicas com o IBGE. 7 mai. <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>
- TILT.(2020). Ativistas abrem queixa contra algoritmo após negro ser preso por IA racista. 25 jul. <https://www.uol.com.br/tilt/noticias/afp/2020/07/25/ativistas-abrem-queixa-contr-a-algoritmo-apos-negro-ser-preso-por-ia-racista.htm>
- Valente, J. (2018). Legislação de proteção de dados já é realidade em outros países. Agência Brasil. 5 mai. <https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359 (6380), 1146-1151.
- Zuboff, S. (2018). Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In F. Bruno, B. Cardoso, M. Kanachiro, L. Guilhon, & L. Melgaço, *Tecnopolíticas da vigilância: perspectivas da margem*, 1a. ed, pp. 17-68. São Paulo: Boitempo.
- Zuboff, S. (2020). *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*, 1ª ed. Rio de Janeiro: Intrínseca.